Essi Koivula

Yritysturvallisuuden hallinta

PK-yritysten tarpeet ja käsitykset

Opinnäytetyö
Syksy 2013
Liiketalouden ja kulttuurin yksikkö
Liiketalouden koulutusohjelma

Seinäjoen ammattikorkeakoulu
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

SISÄLTÖ

Kuvio- ja taulukkoluettelo

SEINÄJOEN AMMATTIKORKEAKOULU

Opinnäytetyön tiivistelmä

Koulutusyksikkö: Liiketoiminta ja kulttuuri

Koulutusohjelma: Liiketalouden koulutusohjelma

Tekijä: Essi Koivula

Työn nimi: Yritysturvallisuuden hallinta: PK-yritysten tarpeet ja käsitykset

Ohjaaja: Anmari Viljamaa

Vuosi: 2013 Sivumäärä: 65 Liitteiden lukumäärä: 2

Suomi on muuttunut tietoyhteiskunnaksi, jonka menestymisen edellytykset kansainvälisessä ympäristössä liittyvät yritysten kykyyn suojata tärkeintä pääomaansa, tietoa. PK-yritykset muodostavat Suomen yrityskannasta valtaosan ja niiden vaikutus maakuntien elinvoimaisuuteen, kuntien verotulojen kautta, on huomattava. PK-yrityksissä työskentelee enemmistö Suomen kaikista yrityksissä työskentelevistä henkilöistä. PK-yritysten haavoittuvuutta tietoturvallisuuden suhteen ei vältämättä tunnisteta riittävän hyvin.

Opinnäytetyössä selvitettiin PK-yritysten yritysturvallisuuden hallintaan liittyviä tarpeita ja käsityksiä. Selvityksessä painotettiin erityisesti tietoturvallisuutta. Tutkimus on osa Opsec Oy:n turvallisuuspalvelujen kehitystyötä. Tutkimuksen tavoitteena oli muodostaa PK-yritysten turvallisuuden hallintaan liittyvien tarpeiden ja käsitteiden profiili. Tarkoitus oli kartoittaa PK-yrityksien asiakkuuspotentiaalia turvallisuusalan näkökulmasta, jotta heidän turvallisuustarpeisiinsa voitaisiin entistä paremmin vastata. Tutkimusmenetelmänä käytettiin teemahaastattelumenetelmää. Haastateltavien määräksi muodostui seitsemän PK-yrityksen edustajaa Etelä-Pohjanmaan alueelta.

Tulokset osoittavat selkeästi, että suuriksi luokiteltavien yritysten ja PK-yritysten yritysturvallisuuden hallintaan liittyvät tarpeet eroavat toisistaan huomattavasti. PK-yritykset kaipaavat asiakaslähtöisiä ja kokonaisvaltaisia turvallisuuspalvelumalleja. PK-yrityksille tarjottavien turvallisuusratkaisujen tulee olla helppoja ja edullisia. Tarvitaan myös koottua tietoa yritysturvallisuudesta ja sen ajankohtaisista piirteistä. Yritysturvallisuusasioissa ohjaavalle toiminnalle ja koulutuksille nähtiin olevan selkeää tarvetta PK-yrityksissä. Älypuhelimien tietoturvallisuusasiat koettiin myös ajankohtaiseksi ja niihin liittyvää tietoisuutta tulisi lisätä.

Avainsanat: turvallisuus, yritysturvallisuus, tietoturva, kyberturvallisuus

SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Thesis abstract

Faculty: School of Business and Culture

Degree programme: Business Management

Author: Essi Koivula

Title of thesis: Corporate security management: needs and conceptions of SMEs

Supervisor: Anmari Viljamaa

Year: 2013 Number of pages: 65 Number of appendices: 2

Finland has turned into an information society whose key success factor is companies' ability to protect their prime capital, information. In Finland, small and medium-sized enterprises form the majority of the corporate base in Finland. SMEs have a significant positive impact also on the economy of regions via tax revenues. Also, the majority of all employees working for enterprises in Finland are employed by SMEs. Vulnerability in information security is not necessarily recognized well enough by SMEs.

The goal of this thesis is to find out the needs and conceptions of SMEs related to corporate security management. The survey focuses on information security. The thesis is also part of security service development work done at Opsec Ltd. The objective of this thesis was to form a customer profile of the needs and conceptions SMEs in corporate security management. The goal was to survey SMEs' customership from the point of view of the security service sector, in order that their needs can be met better than before. The data was collected by means of interactive semi-structured interviews carried through in an individual conversational mode. The target interviews were implemented with a total of seven SME representatives from South Ostrobothnia.

The results show that there are clear differences in the needs for corporate security between larger companies and SMEs. SMEs need customer-oriented and comprehensive security service models. Security solutions for SMEs need to be easy and affordable. There is also a need for concise information about corporate security and its current features. According to the interviews, there is also a significant need for guiding operations and training at the SMEs. What comes to smartphones and their information security, the interviewees find those to be topical issue and the awareness of security risks of smartphones should be increased.

Keywords: security, corporate security, information security, cyber security

1 Johdanto

Tausta. Europol kartoittaa kansainvälisesti Euroopan Unionin rikollisuuden kehittymispiirteitä (2013). Viimeisimmässä raportissa kerrotaan kansainvälisten rikollisryhmien keskinäisestä, kasvavasta yhteistoiminnasta, suuremmasta liikkuvuudesta EU:n sisällä ja rikollisten toimintojen laajentumisesta useammille osa-alueille, sekä internetin avulla tehtävien rikosten yleistymisestä. Enää ei pärjätä rakentamalla vain korkeita suojamuureja tiedon ympärille, vaan on eristäytymisen sijaan rakennettava kumppanuuksia yritysten ja yhteiskunnan välille (Mueller 2013). Yhteistyön avulla voidaan lisätä tiedonvaihtoa tietoturvallisuutta vaarantavasta rikollisuudesta ja muodostaa ajantasaista tilannekuvaa eri osapuolten kesken.

Käytännössä yhteiskunnan kasvava tietointensiivisyys, ulkomaisen yritysomistuksen lisääntyminen, eri toimintojen ulkoistaminen, tieto- ja viestintäjärjestelmien keskinäinen yhteensulautuminen, avoimien tietoverkkojen käyttö ja riippuvuus sähköstä on sysännyt yhteiskunnan elintärkeiden toimintojen turvaamisen ihan uudenlaisten vaatimusten äärelle (Maanpuolustuskorkeakoulu 2013, 1). Yhteiskunnan elintärkeisiin toimintoihin kuuluvat esimerkiksi kansantalouden ja infrastruktuurin toimivuus.

Kasvuhakuinen yrittäjyys on Suomessa todella vähäistä (GEM 2009). PK-yritykset muodostavat Suomen yrityskannasta valtaosan ja niiden henkilöstömäärä on reilusti yli puolet kaikkien yritysten henkilöstöstä (Tilastokeskus 2012). PK-yritysten merkitys niin kansantalouden kuin kunnallistalouden tukipilarina on huomattava (Elinkeinokeskus 2013 & Routamaa 2012, 9-11). PK-yritysten turvallisuuden takaaminen ja kilpailukyvyn vahvistaminen kansainvälistyvässä ympäristössä ei siis ole mikään vähäpätöinen asia.

Erityisesti suhteessa tietoturvallisuuteen PK-yritysten haavoittuvuus tulee tunnistaa. Osaamis- ja tietopääoma tulevat tulevaisuudessakin olemaan suomalaisyritysten tärkeimpiä kilpailuvaltteja (Hollmen, EK 2012). Alati muuttuvissa liikeelämän tilanteissa on liiketoiminnallisen kannattavuuden ehtona, että oikeaa tietoa menee oikeaan paikkaan ja näin pystytään tukemaan yritysten oikeanlaista reagoimista muutoksiin (Rantala & Virta 2006, 77).

Toimeksiantaja. Opsec Oy on vuonna 2009 perustettu yritys, joka tarjoaa tietohallinnon ja tietoturvallisuuden johtamis- ja asiantuntijapalveluita (Opsec Oy 2013). Opsec Oy:n palveluvalikoimaan kuuluvat IT-päällikköpalvelut, tietoturvapalvelut ja IT-tutkinta. Yrityksen toimialueena on koko Suomi. Toteutimme Seinäjoen Ammattikorkeakoulussa, FramiPro -monialaisten projektiopintojen aikana, projektin Opsec Oy:lle. Tämä aihe oli luonteva jatkoaihe opinnäytetyönä tehtävään tutkimukseen.

Tavoite. Opinnäytetyön tavoitteena oli muodostaa PK-yritysten koottujen, turvallisuuden hallintaan liittyvien, tarpeiden ja käsitteiden profiili. Tarkoitus oli kartoittaa PK-yritysten asiakkuuspotentiaalia turvallisuusalan näkökulmasta, jotta heidän turvallisuustarpeisiinsa voitaisiin entistä paremmin vastata. Opinnäytetyö on osa Opsec Oy:n turvallisuuspalveluiden kehitystyötä.

Toteutus. Tutkimus toteutettiin teemahaastattelututkimuksena. Teema-alueita oli kolme. Tutkimushaastattelun ensimmäinen teema-alue muodostui tutkimuksen aiheen kannalta keskeisten käsitteiden määrittelystä. Toisessa teema-alueessa tarkoituksena oli hahmottaa yritysturvallisuuden käytäntöä haastateltavien yrityksissä. Kolmannessa teema-alueessa tarkoitus oli vielä fokusoida turvallisuuden hallinnan tarpeita PK-yrityksissä.

Työn rakenne. Luvuissa 2 ja 3 käsitellään opinnäytetyön teoreettinen tausta. Opinnäytetyön teoriatausta rakentuu kahdesta osa-alueesta. Ensimmäisessä osa-alueessa käsitellään yritysturvallisuuteen liittyviä yleisiä asioita, kuten turvallisuuden olemusta, yritysturvallisuuden merkitystä liiketoiminnan kannalta, yrityksen turvallisuuspolitiikkaa ja rikostorjuntastrategiaa, turvallisuuskulttuuria ja turvallisuusviestintää. Toisessa osa-alueessa käsitellään yritysturvallisuuden osa-alueita tarkemmin, pääosin Suomen elinkeinokeskuksen (Yritysturvallisuus EK 2009) mukaisen jaottelun kautta.

Luvussa 4 käydään läpi tutkimustavan valinta ja valitun toteutustavan vaiheet. Luku 5 muodostuu tulosten läpikäynnistä ja lukuun 6 on koottu tuloksien perusteella tehdyt keskeiset johtopäätökset. Luvussa 7 pohditaan sitä, saavutettiinko opinnäytetyölle asetetut tavoitteet ja arvioidaan tutkimustulosten hyödynnettävyyttä suhteessa opinnäytetyölle asetettuihin tavoitteisiin.

2 Yritysturvallisuus

2.1 Turvallisuus

Turva on turvallisuuden kantasana, jolla tarkoitetaan sitä, mikä suojaa, varjelee tai turvaa (Suomisanakirja.fi 2013). *Turvaa* on se, mihin jokin turvautuu tai voi turvautua. Turvaa on myös tunne turvallisuudesta, turvattuna olosta tai suojasta. *Turva* on myös tekemisen merkityksessä, jonkin avulla tai tukemana jotain tekemistä, esimerkiksi ”hän pakeni pimeyden turvin”.

Turvallinen on jonkun asian ominaisuutena vaaraa aiheuttamaton tai suojainen (Suomisanakirja.fi 2013). Turvallinen on siis jotain, mikä luo tunteen turvallisuudesta tai luotettavuudesta. *Turvallisuus* on varmuutta tai tunnetta siitä, että onnettomuutta tai muuta pahaa ei tapahdu.

Englannin kielessä turvallisuutta kuvaavat kaksi sanaa *security* ja *safety*, joista ensimmäisellä tarkoitetaan kovaa turvallisuutta ja jälkimmäisellä pehmeää turvallisuutta (Mäkinen 2007, 56–57). Security ymmärretään perinteisenä suojautumisena se voi olla esimerkiksi vartiointia tai toimitilaturvallisuutta. Safety on käsitetty esimerkiksi kykynä tehdä joku tai jokin turvalliseksi, se ymmärretään enemmän palo- ja pelastustoimintana tai työturvallisuutena.

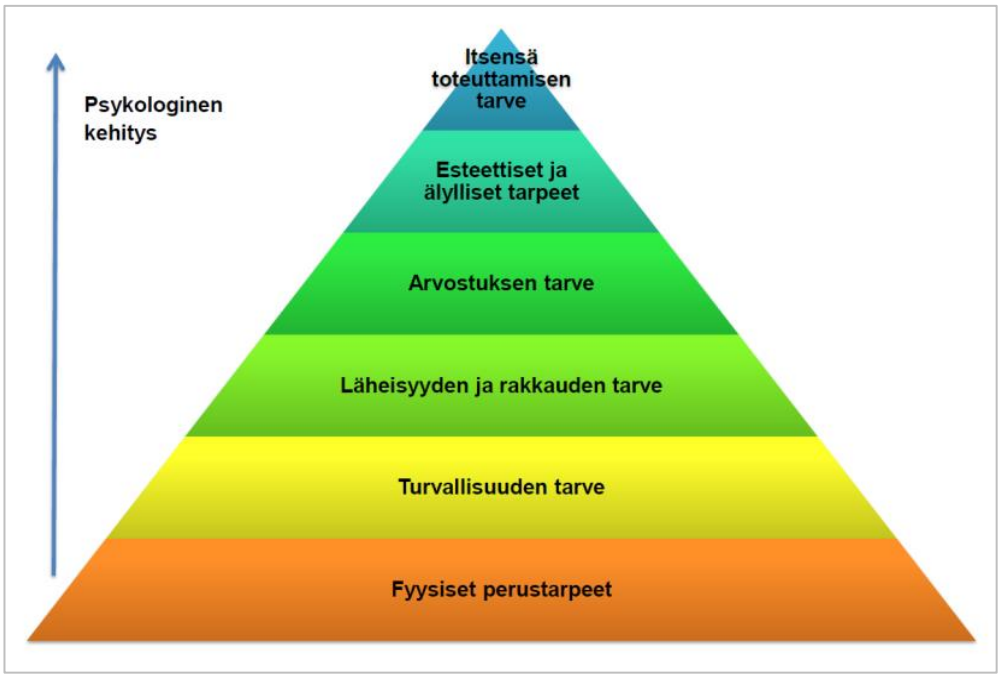
Turvallisuus voidaan jaotella kahteen osa-alueeseen, subjektiiviseen ja objektiiviseen turvallisuuteen (Leppänen 2006, 43–44). Nämä kaksi osa-aluetta eroavat siinä, miten ne määrittelevät riskin olemassaolon. Riskillä tarkoitetaan jonkin epäedullisen tapahtuman uhkaa, vaaraa tai mahdollisuutta tulevaisuudessa (Suomisanakirja.fi 2013). Objektiiviset riskit ovat olemassa siitä huolimatta, tiedostetaanko ne vai ei (Leppänen 2006, 43–44). Subjektiivisilla riskeillä tarkoitetaan niitä riskejä, jotka ovat riippuvaisia ihmisen omasta päätöksenteosta, uskomuksista ja arvostuksista.

Turvallisuus voidaan myös jaotella kahteen toisistaan eriävään ulottuvuuteen, sen perusteella tarkoitetaanko henkilökohtaista vai poliittista turvallisuutta (Rantala & Virta 2005, 112). Henkilökohtaisella turvallisuudella tarkoitetaan materiaalista tur-

vallisuutta ja ontologista, yksilön hyvinvointia kuvaavaa turvallisuutta. Poliittisella turvallisuudella tarkoitetaan tässä yhteydessä kansallista, yhteiskunnallista tai sosiaalista turvallisuutta.

Turvallisuus on käsitteenä paljon monimutkaisempi kuin aluksi luullaan (Mäkinen 2007, 63–66). Kokemukset turvallisuudesta ja turvattomuudesta luovat pohjan minän eli identiteetin suhteuttamiselle maailmaan. Oma olemassaolo ja lähiympäristön kokeminen riittävän turvalliseksi ovat perustekijöitä, joiden perusteella ihminen hahmottaa itsensä ja maailman.

Maslowin tarvehierarkiassa todetaan turvallisuuden olevan fyysisten perustarpeiden jälkeen se porras, johon kaikki muu ihmisen toiminta rakentuu (Maslow 1987). Mikäli fyysiset tarpeet ja turvallisuuden tarpeet ovat täyttyneet, ihmistä alkavat useimmiten motivoida kehittyneemmät tarpeet (Kuvio 1). Kaksi alimmaista porrasta toimivat ns. puutemotiivin idealla, ne tulevat voimakkaan pakottaviksi, mutta täyttyessään ne eivät enää vaikuta toimintaan. Ylimmät portaat ovat ns. kasvumotiiveja; ne eivät laiminlyötynä muutu pakottaviksi. Itsensä toteuttamisen tarvetta voidaan kuvata tilana, jossa ihminen on vapaa toteuttamaan omia mahdollisuuksiaan ja kykyjään.



Kuvio 1. Maslowin tarvehierarkia (Maslow 1987, Mäkisen 2007, 61 mukaan).

2.2 Yritysturvallisuus ja sen liiketoiminnallinen merkitys

Yritysturvallisuuden roolina on taata yrityksen häiriötön toiminta, liiketoiminnan jatkuvuus, sekä mahdollisuus ja vapaus toimia (Leppänen 2006, 21–28). Riskienhallinnalla ja turvallisuuden ylläpitämisellä pyritään vähentämään yrityksen toiminnan jatkuvuuteen vaikuttavia riskejä, liittyen esimerkiksi yritysstrategiaan, operatiivisiin toimintoihin, talouteen ja vahinkotapahtumiin.

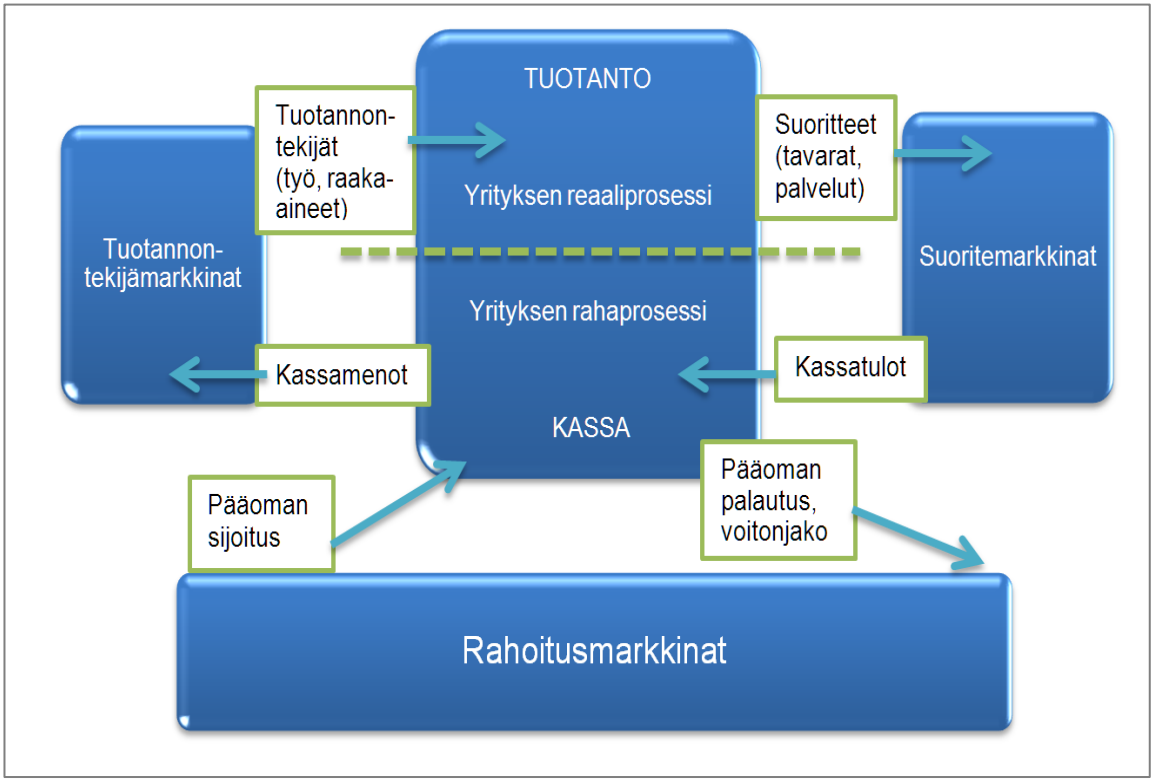
Yrityksen turvallisuustoimenpiteillä pyritään ennaltaehkäisemään ja torjumaan rikollisuutta yrityksessä. Rikollisuus aiheuttaa liiketoiminnalle suoria aineellisia menetyksiä ja ajallisia menetyksiä, rikostapahtumiin käytettynä aikana (Yritysuhritutkimuksen tuloksia 2010, 136). Kaikkien yritysten toimintojen on johdettava yrityksen tavoitteiden saavuttamiseen (Leppänen 2006, 24). Turvallisuustoimintojen avulla organisaation tavoitteiden saavuttamista pyritään mahdollistamaan ja varmistamaan.

Yritysturvallisuustoiminnan pohjana tulee olla se, että ollaan tietoisia yrityksen turvallisuusympäristöstä (Sisäasiainministeriö 2012, 12). Yritysten turvallisuusympäristö muodostuu yritysten rikosturvallisuuden kokonaiskuvasta ja yritysten turvallisuustilannekuvasta. Keskusrikospoliisi (2012, 3) kartoittaa vuosittain yritysten rikosturvallisuuden tilannekuvassa tapahtuvia muutoksia ja julkaisee yleisesti saatavilla olevaa Yrityksiin kohdistuva ja niitä hyödyntävän rikollisuuden kokonaiskuva -raporttia.

Yrityksen turvallisuusjohtamisen ja turvallisuustoiminnan tavoitteena on yksinkertaisimmillaan suojata yrityksen reaali- ja rahaprosesseja, yritysjohtamista sekä arvoketjua (Leppänen 2006, 22–23). Reaaliprosesseilla tarkoitetaan yritystoiminnan tuotannontekijöitä eli esimerkiksi työtä ja raaka-aineita (Kuvio 2). Rahaprosessit koostuvat pääoman sijoituksista ja palautuksista, sekä yrityksen menoista ja tuloista.

Yrityksen strategisen johtamisen turvaaminen on jatkuvuuden kannalta olennaista, sillä se määrittelee yrityksen mission eli olemassaolon tarkoituksen ja vision eli tavoitetilan (Leppänen 2006, 22–23). Operatiiviseen johtamiseen, sekä ihmisten ja

asioiden johtamiseen liittyy myös monia riskejä. Yrityksen eri johtamisalueiden riskit tulee tunnistaa turvallisuusjohtamisen näkökulmasta.



Kuvio 2. Reaali- ja rahaprosessit (Leppänen 2006, 22).

Arvoketjulla tarkoitetaan sitä, miten tuotteet ja palvelut tuottavat lisäarvoa asiakkaalle ja sitä kautta voittoa yrityksen omistajille (Leppänen 2006, 23–24). Asiakkaan kokema laatu on yrityksen tuotteelle tai palvelulle asettama arvo. Arvoketjun toteutumiseen liittyviä riskejä pyritään minimoimaan yritysturvallisuuden toimintojen avulla, sillä arvoketjun toteutuminen vaikuttaa suoraan yrityksen tulokseen ja kannattavuuteen.

2.3 Turvallisuuspolitiikka ja rikostorjuntastrategia

Turvallisuuspolitiikassa yritysjohto määrittelee sen, mitkä asiat painottuvat yrityksen turvallisuustoiminnassa (Yritysturvallisuus EK 2009). Siinä määritetään suojattavien kohteiden merkitys ja asema yrityksen toiminnan jatkuvuuden varmistamisessa (Leppänen 2006, 177–179). Turvallisuuspolitiikalla määritellään turvallisuustoimenpiteiden kohteet, keinovalikoimat ja vastuiden jakaantuminen. Turvallisuu-

teen liittyvät arvot, ohjeistukset ja toimintasuunnitelmat ovat osa turvallisuuspolitiikkaa. Tarkoitus on edellä mainittujen avulla asettaa yrityksen turvallisuustoiminnan strategia ja tavoitteet.

Turvallisuuspolitiikka muodostuu kahdesta ulottuvuudesta, sisäisestä ja ulkoisesta turvallisuuspolitiikasta (Leppänen 2006, 177–179). Ulkoisella turvallisuuspolitiikalla tarkoitetaan asioita, jotka vaikuttavat ulkopuolisiin toimijoihin, kuten esimerkiksi turvallisuustoiminnan periaatteet ja linjaukset. Sisäisen turvallisuuspolitiikan merkitys on turvallisuuskulttuurin luomisessa ja muokkaamisessa.

Yrityksen rikostorjunnan tavoitteena on ennaltaehkäistä ja selvittää jo tapahtuneita rikoksia, sekä seurata rikostilannetta (Yritysturvallisuus EK 2009). Keskusrikospoliisin mukaan (2012, 6–8) yrityksen henkilökuntaa pitää suojata rikosriskeiltä. Rikoksen uhka voi kuitenkin tulla myös yrityksen sisältä, työntekijä voi myös osallistua väärinkäytöksiin tai rikoksiin. Yrityksillä on huomattavasti suurempi todennäköisyys joutua rikoksen teon kohteeksi kuin yksittäisillä henkilöillä (Yritysuhritutkimus 2011, 137).

Liiketoiminnassa on tärkeätä suojata myös omaisuutta, johon materiaaliturvallisuus lukeutuu ja ehkäistä siihen liittyvää rikollisuusuhkaa. Materiaaliturvallisuudella tarkoitetaan esimerkiksi materiaalin ja sen käyttäjien sekä ympäristön suojaamista (Puolustusministeriö 2007, 7). Lisäksi se pitää sisällään erilaisten materiaalin käytettävyyden, toimivuuden ja turvallisuuden varmistuksen koko elinkaaren ajan. Asianmukaisesti suunniteltu ja toteutettu tuotesuojaus myös vähentää siihen kohdistuvaa varkauden uhkaa (Keskusrikospoliisi 2012, 10).

Pohdittaessa rikostorjuntaa minkä tahansa yrityksen suojattavan kohteen kannalta, tärkeintä on pyrkiä ennaltaehkäisemään rikollisuutta (Leppänen 2006, 257). Olennaista on nimenomaisesti rikostorjuntastrategian suunnittelu, joka painottuu mahdollisimman kattavaan ennaltaehkäisevään suunnitteluun. Tyypillisiä riskienarvioinnin työkaluja ovat esimerkiksi erilaiset turvallisuusanalyysit ja haavoittuvuusanalyysit, joiden avulla pyritään löytämään todennäköisimmät turvallisuusuhat, arvioimaan niiden vaikutukset yritystoiminnalle ja rajoittamaan niiden seurauksia (Yritysturvallisuus EK 2009).

Leppäsen mukaan (2006, 257) kriminologiassa yritysturvallisuuteen liittyvä rikostorjunta muodostuu seuraavista:

- Rikostorjuntastrategia
- Ennaltaehkäisevät taktiikat
- Tekniset torjuntakeinot

Rikostorjuntastrategia voi esimerkiksi pitää sisällään erilaisia teoreettisia malleja, joiden kohteena voivat olla rikoksen tekijä, rikoksen kohde (uhri) tai rikostapahtuma (Leppänen 2006, 257). Tilannekuva-analyysillä pyritään ennakoimaan todennäköisimmät rikoskohteet, toteutuspaikat, tilanteet ja ajankohdat. Rikoksen kohdetta ennakoidessa pyritään analysoimaan potentiaalista rikoksen teon kohdetta ja estämään rikoksen todennäköisimmät toteutumismahdollisuudet.

Tilanteen ennaltaehkäiseviä keinoja voivat olla kiinnijäämisriskin lisääminen, rikoksentorjuntamahdollisuuksien lisääminen, rikoksentekomahdollisuuksien vähentäminen, sekä rikoksesta saatavan hyödyn minimoiminen (Leppänen 2006, 258). Rikoksen hyödyn vähentämistä voivat olla materiaaliturvallisuuden näkökulmasta käteisvarojen minimointi, rahahuollon siirto vartiointiliikkeelle ja arvo-omaisuuden merkintä. Teknisillä torjuntakeinoilla pyritään ennaltaehkäisemään rikostapahtumat ja niiden toteutus.

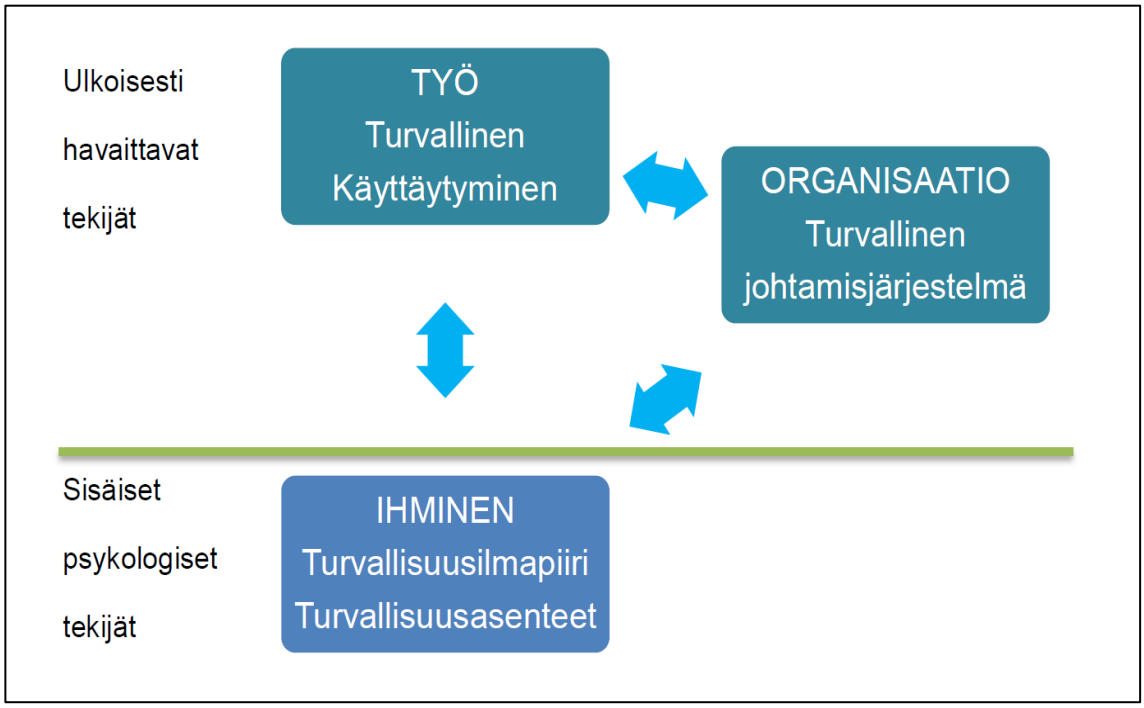
2.4 Turvallisuuskulttuuri

Turvallisuuskulttuurin käsite sai alkunsa Tšernobylin ja British Railway’n Clapham Junctonin onnettomuustapausten aikoihin, 1980 - luvun lopuilla. Niihin aikoihin alettiin tutkia, mitä kulttuurilla tarkoitetaan erityisesti turvallisuuden näkökulmasta. Turvallisuuskulttuuri muodostuu organisaation toimintatavoista ja yksittäisen ihmisen asenteista (Leppänen 2006,195).

Turvallisuuskulttuuri on osa organisaatiokulttuuria, samoin kuin turvallisuusilmapiirikin (Leppänen 2006, 185–187). Turvallisuusilmapiiri pitää sisällään myös havainnot ja asenteet turvallisuusasioista, henkilöstön sisäiset arvot ja asenteet, sekä ne asiat mihin asenteet kohdistuvat. Turvallisuusasenne on henkilökohtainen ja riski-

käsitys on sosiaalinen kokonaisuus. Asenteiden ja riskikäsityksen lisäksi tulee huomioida muu kyseessä olevaa ryhmää koskeva tieto turvallisuuskulttuuria kehitettäessä.

Cooper (1998, 17–18) jäsentelee turvallisuuskulttuurin mallissaan turvallisuuskulttuurin osa-järjestelmät (Kuvio 3) turvallisuuden johtamisjärjestelmään, turvallisuusilmapiiriin ja -asenteisiin, sekä käyttäytymiseen. Cooperin turvallisuuskulttuurimallin avulla voidaan myös mitata yrityksen turvallisuuskulttuuria.



Kuvio 3. Turvallisuuskulttuurin osa-järjestelmät (Cooper 1998).

Turvallisuusilmapiiriin ja turvallisuuskulttuuriin vaikuttamisella pyritään vaikuttamaan yrityksessä työskentelevien ihmisten käyttäytymiseen, jotta turvallisuuden ylläpitäminen on mahdollista ja turvallisuuteen vaikuttavat keskeiset asiat huomioidaan asianmukaisella tavalla (Leppänen 2006, 179–195). Turvallisuuskulttuuriin voidaan vaikuttaa turvallisuusjohtamisen avulla ja turvallisuuspolitiikan, toimintatapojen ja ohjeistuksien määrittelyllä ja toteutuksella.

Turvallisuuskulttuurin kehittäminen, erilaiset koulutukset, tiedonkulun kehittäminen ja eri osapuolten kanssakäymisen parantaminen lisäävät yrityksen aineetonta tieto- ja osaamispääomaa (Simola 2005, 118–120). Yrityksen aineettoman pääoman liiketoiminnallinen merkitys on selkeä ja kartoittaa pitkällä tähtäimellä yrityksen

aineellistakin pääomaa. Osaamispääoma muodostuu henkilöpääomasta, rakenteellista pääomasta ja suhdepääomasta (Otala 2008). Tieto- ja osaamispääoman todellinen hyöty tulee näkyväksi siinä vaiheessa, kun sitä osataan johtaa.

2.5 Turvallisuusviestintä

Viestintä tulee sanasta kommunikointi ja sen alkuperä on latinankielisessä termissä communicare, jolla tarkoitetaan jonkun tekemistä yhdessä. Turvallisuusviestintä on keskeisessä asemassa, turvallisuuskulttuurin luomisessa, vaikkei se yksistään takaa yrityksen turvallisuutta (Hjelt-Putin 2005, 8–10). Sen merkitys työpaikkojen turvallisuuteen on kuitenkin merkittävämpi kuin usein ajatellaan (140).

Wiion (1994) mukaan viestintä jaetaan kahteen osaan, sanattomaan eli nonverbaaliseen viestintään ja kielelliseen eli sanalliseen viestintään. Nonverbaalinen viestintä voidaan jakaa edelleen, kinestiikkaan (eleet, ilmeet, liikkeet ja kosketuskäyttäytyminen), parakieleen (äänen sävyt, painotus, rytmi ja tauotukset) ja proksemiikkaan (paikan valinta, tilan käyttö ja etäisyys). Viestin vastaanottamiseen vaikuttavat myös erilaiset sisäiset ja ulkoiset häiriötekijät.

Yrityksen turvallisuusviestinnän avulla voidaan lisätä turvallisuutta, sekä ehkäistä ja hallita mahdollisia konfliktitilanteita (Hjelt-Putin 2005, 8–15). Etenkin palvelualojen turvallisuudessa viestintä on keskeinen osa yritysturvallisuutta, sitä tarvitaan aina ongelmien havainnoinnissa, niiden järjestelmällisessä kartoituksessa, turvallisuus- ja varautumissuunnittelussa ja -johtamisessa, suunnitelmien toteutuksessa ja vakiinnuttamisessa käytäntöön.

Vuorovaikutusvalmiuksien kolme eri osa-aluetta liittyvät yksilön tietoihin, taitoihin ja asenteisiin (Hjelt-Putin 2005, 31–56). Vuorovaikutusvalmiudet vaikuttavat havainnoinnin tasoon ja tehokkuuteen. Havainnoinnin tehokkuutta turvallisuusasioissa voidaan lisätä lisäämällä tietoisuutta siitä, mihin tulee konkreettisesti ja käytännön tasolla kiinnittää huomiota. Toimintamallit eri tilanteissa on hyvä myös tiedostaa ja turvallisuuden kannalta epäsuotavista toimintamalleista tulisi oppia pois.

Toimintamalleihin liittyvä hiljainen tieto tulisi, tietoturvallisuuden puitteissa, tuoda eksplisiittiseksi eli tallennetuksi johonkin muotoon (Otala 2008). Kun tieto on eksplisiittistä liittyen turvallisuusasioihin ja toimintamalleihin, on se helpommin tunnistettavaa ja hallittavaa, sekä tarkoituksenmukaisempaa. Hyvään viestintäilmastoon liitetään myös avoimuus, luottamus, sosiaalinen tuki ja välittäminen, joiden on todettu olevan hyvän viestintäilmaston kivijalka (Hjelt-Putin 2005, 74).

Viestinnällä on aina joku päämäärä, johon pyritään erilaisilla viestintätaktiikoilla ja -strategioilla (Hjelt-Putin 2005, 85–86). Toiset ovat tarkoituksenmukaisempia turvallisuuden näkökulmasta kuin toiset. Tämä näkökulma tulisi tiedostaa, etenkin palvelualalla työskenneltäessä.

Turvallisuutta tukevia viestintätyylejä palvelutyössä ovat assertiiviset viestintästrategiat ja -taktiikat (Hjelt-Putin 2005, 94). Assertiiviselle viestintätyylille on ominaista, että se on maltillista ja päämäärätietoista viestintää. Silloin pidetään omista oikeuksista kiinni, mutta toisten oikeuksia kunnioittaen ja aggressiivisuutta välttäen. Pyritään siis pääsemään päämäärään lievimpiä mahdollisia keinoja käyttäen.

Yritystoiminnassa viestinnän kannalta on myös olennaista kriisiviestintäsuunnitelman- tai ohjeen laatiminen (Yritysten rikosturvallisuus 2012, 62). Sen tavoitteena on selkeyttää ja tehostaa yrityksen sisäistä ja ulkoista viestintää kriisien aikana. Kriisiviestintäsuunnitelman laatimisella voi olla pelastava vaikutus yrityksen mainetta ajatellen mahdollisissa kriisitilanteissa.

3 Yritysturvallisuuden osa-alueet

Yritysturvallisuuden osa-alueet jakaantuvat yritysturvallisuusneuvottelukunnan mukaan 10 eri osa-alueeseen (Kuvio 4), jotka suojaavat yrityksen henkilöitä, mainetta, tietoa, omaisuutta ja ympäristöä (Yritysturvallisuus EK 2009). Tavoitteena on siis ennakoida, ehkäistä ja torjua yritystoiminnan keskeisiin, suojeltaviin asioihin kohdistuvia riskejä. Yritysjohdon tulee määritellä yrityksen turvallisuuspolitiikka, jonka mukaan kyseessä olevassa yrityksessä toimitaan ja miten turvallisuusasioita hoidetaan. Turvallisuusjohtamisella tarkoitetaan turvallisuusnäkökohtien huomioonottamista yrityksen päivittäisessä toiminnassa, ja siten sen avulla hallitaan turvallisuusosa-alueista muodostuvaa kokonaisuutta.

Kuvio 4. Yritysturvallisuuden osa-alueet (Yritysturvallisuus EK 2009).

Tässä opinnäytetyössä käsitellään pääosin yritysturvallisuuden osa-alueita yritysturvallisuusneuvottelukunnan mukaisen jaottelun kautta (Yritysturvallisuus EK 2009). Rikosturvallisuutta on käsitelty luvussa 2, yrityksen rikostorjuntastrategian muodostamisen kannalta, joten sitä ei tässä käsitellä muiden turvallisuuden osa-alueiden ohessa. Yritysturvallisuusneuvottelukunnan (2009) mukaan turvallisuuden osa-alueet jakaantuvat henkilöturvallisuuteen, työturvallisuuteen, kiinteistö- ja

toimitilaturvallisuuteen, tuotannon ja toiminnan turvallisuuteen, pelastustoimintaan, ympäristöturvallisuuteen, ulkomaantoimintojen turvallisuuteen, valmiussuunnitteluun, tietoturvallisuuteen ja rikosturvallisuuteen.

3.1 Henkilöturvallisuus

Henkilöturvallisuudessa pyritään suojaamaan ihmistä henkilötasolla (Leppänen 2006, 204–217). Yritysturvallisuusneuvottelukunnan (Yritysturvallisuus EK 2009) mukaan henkilöturvallisuudella tarkoitetaan ihmisten turvallisuuden takaamista suhteessa rikollisuuteen ja onnettomuuksiin. Henkilöiden, yrityksille aiheuttamien uhkien pienentäminen katsotaan myös kuuluvaksi henkilöturvallisuuteen. Tavoitteena on siis turvata henkilöt ja toiminta (Leppänen 2006, 204). Henkilöturvallisuuteen kuuluvat seuraavat osa-alueet:

- Asiakkaiden ja vierailijoiden turvallisuus
- Avainhenkilöiden turvallisuus ja sijaisjärjestelyt
- Kodin ja perheen turvallisuus
- Matkustusturvallisuus
- Henkilösuojaus erikoistapauksissa
- Tavoitettavuus- ja hälytysjärjestelmät
- Varamiesjärjestelyt
- Luotettavuusmenettelyt
- Salassapitosopimukset
- Verkoston hallinta

Henkilöturvallisuus on Suomen Keskusrikospoliisin mukaan koko yritysturvallisuuden kivajalka, koska vasta työntekijän osaaminen ja asenne määrittävät sen, onko turvallisuuteen liittyvistä menettelytavoista ja järjestelmistä hyötyä yritykselle (Keskusrikospoliisi 2012, 6). On työnantajan velvollisuus kouluttaa ja perehdyttää työntekijät erilaisten turvallisuusjärjestelmien käyttöön ja varmistaa, että riittävä ohjeistus on saatavilla.

3.2 Työturvallisuus

Työturvallisuustoimintojen avulla pyritään tekemään työntekijöiden työnteko mahdollisimman turvalliseksi (Leppänen 2006, 218). Työturvallisuuteen liittyy myös keskeisesti sitä säätelevä lainsäädäntö, jonka tulisi olla niiden vähimmäistason määrittäjä (Työturvallisuuslaki 2002/738). Työturvallisuuteen liittyvä lainsäädäntö on kehittynyttä ja se määrittelee työpaikoilla tehtävää työturvallisuustoimintaa.

Työturvallisuustoiminnan tavoitteena on edistää työntekijän työskentelyn turvallisuutta ja terveellisyyttä (Työturvallisuuslaki 2002/738). Työturvallisuustoiminta jakautuu työturvallisuussuojeluun eli tapaturmien ennaltaehkäisyyn, työterveyssuojeluun eli terveyshaittojen ja ammattitautien ehkäisyyn, sekä henkiseen työsuojeluun. Uusitun työturvallisuuslain painopisteeksi on otettu työnantajan velvollisuus selvittää ja arvioida työnteon vaarat ja haitat työntekijälle (Työturvallisuuslaki 738/2002 10§).

Työnantaja on vastuussa työpaikan ja työympäristön turvallisuudesta; käytännössä vastuu jakaantuu kuitenkin useammille organisaatiotasoille ja työntekijällä on velvollisuus noudattaa työnantajan työnteon turvallisuutta koskevia määräyksiä (Työturvallisuuskeskus 2013). Työpaikkakohtaisia työsuojeluelimiä ovat työsuojeluvastaava, jonka tulee olla työnantajan nimittämä, ellei työnantaja ole itse. Työsuojeluvaltuutettu valitaan työntekijöiden toimesta, mikäli yrityksessä on yli kymmenen työntekijää. Työsuojelutoimikunta sisältää työnantajan- ja työntekijöiden edustajat työpaikoissa, joissa työskentelee yli 30 henkilöä. Sosiaali- ja terveysministeriö sekä työsuojelupiirit valvovat työsuojelulain noudattamista kansallisesti.

Yritysturvallisuustoimikunnan mukaan työturvallisuuden tulee koostua tavoitteellisesta toimintaohjelmasta, johon on sisällytetty kehittämistarpeet työoloista työpaikalla ja arviointi työympäristöön liittyvien tekijöiden vaikutuksista, sekä tietoisuuden lisääminen työturvallisuusasioissa (Yritysturvallisuus EK 2009). Työntekijälle on myös annettava perehdytystä työtehtäviinsä, sekä koulutettava ja ohjattava työhön liittyvissä haitta- ja vaaratekijöissä sekä niiden vähentämisessä (Työturvallisuuslaki 738/2002 14§).

Käytännön työturvallisuustoimintaan liittyy myös keskeisesti kyseessä olevaa alaa säätelevät työehtosopimukset, joilla tarkoitetaan alan työnantaja- ja työntekijäliittojen tekemiä sopimuksia, joilla säädetään muutoin työsopimuksessa tai työsuhteessa noudatettavista ehdoista (Työehtosopimuslaki1946/436). Työehtosopimukset varmistavat työntekijän turvallisuutta ja työetuja, sekä pyrkivät takaamaan työrauhan työpaikoilla. Työehtosopimus sitoo niitä työnantajia, yrityksiä ja yhdistyksiä, jotka ovat työehtosopimuksen tehneet tai ovat työehtosopimuksen tehneen yhdistyksen alayhdistyksiä.

3.3 Kiinteistö- ja toimitilaturvallisuus

Kiinteistö- ja toimitilaturvallisuus on merkittävimpiä yritysturvallisuuden osa-alueita, sillä se muodostaa melkein kaikkien toimintojen suojaamiselle perustan (Miettinen 2002, 90). Kiinteistön ja toimitilojen asianmukaisella suojauksella varmistetaan, että pääsy on vain oikeilla henkilöillä, sisällä oleva omaisuus on turvassa, ja että tilojen sisällä on turvallista olla. Kiinteistö- ja toimitilaturvallisuus muodostuu kiinteistöstä, toimitiloista ja niissä olevista suojeltavista kohteista (Leppänen 2006, 333).

Yritysturvallisuusneuvottelukunnan mukaan toimitilaturvallisuuteen liittyy myös turvallisuusvalvonta, jolla tarkoitetaan teknistä valvontaa (Yritysturvallisuus EK 2009). Teknisiä turvallisuusjärjestelmiä voivat olla yrityksissä esimerkiksi rikosilmoitin-, kulunvalvonta-, videovalvonta-, paloilmoitinjärjestelmät ja sammutus- ja savunpoistolaitteet sekä muut tekniset järjestelmät (Leppänen 2006, 333). Turvallisuusvalvontaa voidaan myös toteuttaa omatoimisella vartioinnilla tai ostamalla vartiointipalveluja.

Kiinteistö- ja toimitilaturvallisuudessa on myös ensiarvoisen tärkeää, että yrityksen toimitilat asetetaan tärkeysjärjestykseen ja riskiluokitellaan (Leppänen 2006, 343–346). Näin saadaan jokaiselle tilalle oikea suojaustaso ja säästetään kustannuksia (Miettinen 2002, 92). Tilat voidaan jakaa erilaisiin suojaustasoihin niiden tärkeyden perusteella (Leppänen 2006, 343–346). Suojaustasoja ovat perussuojaus, tehostettu perussuojaus, erityissuojaus ja täyssuojaus.

Yrityksen kiinteistö- ja toimitilaturvallisuudessa on myös olennaista pyrkiä estämään luvattomat tunkeutumisyritykset ja havaita mahdolliset tunkeutumisyritykset mahdollisimman pienellä viiveellä. Tunkeutumissuojausta voidaan toteuttaa esimerkiksi erilaisilla tiedustelullisilla, fyysisillä, teknisillä ja henkilövalvonnan menetelmillä (Leppänen 2006, 346–348).

Lukitus- ja avainhallinnan keskeinen merkitys on siinä, että pystytään estämään luvattomat kulkemiset ja tiedetään tarkalleen, kenellä on pääsy yrityksen tiloihin (Leppänen 2006, 357). Olennaista on myös sopimushallinta ja ulkoistettujen palveluiden suunnitelmallisuus myös kiinteistö- ja toimitilaturvallisuuden näkökulmasta (Yritysturvallisuus EK 2009). Kiinteistön ja toimitilojen ylläpito- ja huoltosopimukset, sekä tarkastukset liittyvät myös keskeisesti kiinteistö- ja toimitilaturvallisuuteen.

Tunkeutumissuojauksen keskeisin asia on kerroksittain suojaus eli kehäsuojaus, joka perustuu tilojen suojaustasoluokituksiin (Yritysturvallisuus EK 2009). Kun kehäsuojaus on toteutettu asianmukaisesti, voidaan saavuttaa hyvin korkea turvallisuustaso (Miettinen 2002, 96). Leppäsen mukaan (2009, 346–348) kehäsuojaus jakaantuu viiteen vyöhykkeeseen, jossa tunkeutuja voidaan tunnistaa. Kehäsuojauksen vyöhykkeitä ovat, uloimmasta aloittaen seuraavat:

1. Kiinteistön aluevalvonta
- Rakenteelliset hidasteet, aidat, portit ja valaistus
- Tekniset tunnistimet, liiketunnistimet, induktiosilmukat
- Kameravalvonta

2. Alueelta lähtevän ja tulevan liikenteen valvonta
- Ajoneuvojen tunnistus
- Punnitus saapuessa ja lähtiessä

3. Rakennuksen ulkokuori
- Ulkokuoren rakennusmateriaali
- Oviympäristö ja sen lukitukset
- Ikkunoiden vahvuus, kalterit
- Ilmastointikanavien ja muiden aukkojen suojaus rakenteellisesti

4. Rakennuksen sisätilojen osastointi
- Sisäinen eristys lukituksien ja kulun- ja kameravalvonnan avulla
- Hissien ja muiden kuljettimien suojaus valvomattomilta reiteiltä
- Tilojen rakennus siten, ettei niihin voi päiväsaikaan piiloutua

5. Erityistila tai tärkeä kohde
- Esimerkiksi atk- ja teletilat, arkistot ja arvo-omaisuuden säilytys
- Kaikki tiloissa kävijät tunnistetaan
- Kassakaapit, arvosäilytysyksiköt, lukitut kaapit ja palosuojakaapit

3.4 Tuotannon ja toiminnan turvallisuus

Yritysturvallisuusneuvottelukunnan mukaan tuotannon ja toiminnan turvallisuuden tavoitteena on varmistaa yrityksen häiriötön tuotanto ja toiminta (Yritysturvallisuus EK 2009). Tuotannon ja toiminnan turvallisuudessa pyritään myös edesauttamaan nopeaa toipumista mahdollisten häiriöiden jälkeen. Tuotteiden turvallisuus kuuluu myös tuotannon ja toiminnan turvallisuuteen.

Yritysturvallisuusneuvottelukunnan mukaan tuotannon ja toiminnan turvallisuus muodostuu yrityksen riskien arviointiin pohjautuvasta jatkuvuussuunnittelusta, liiketoiminnan riskien arvioinnista ja vaihtoehtosuunnittelusta, tuotevastuusta ja -turvallisuudesta, palvelujen turvallisuudesta, varastoinnista ja kuljetuksista, logistiikkaturvallisuudesta, maksuliikenteen turvallisuudesta, arvo-omaisuuden säilytyksestä, sopimusten turvallisuudesta sekä alihankkija- ja palveluverkoston turvallisuusriskien hallinnasta (Yritysturvallisuus EK 2009). Tuotannon ja toiminnan turvallisuuden tulee perustua yrityksen toimintapolitiikkaan, ja se on osa yrityksen liiketoimintajohtamista sekä turvallisuus- ja vahinkoriskien hallintaa (Leppänen 2006, 319). Keskeisessä asemassa ovat myös erilaiset vakuutukset (Yritysturvallisuus EK 2009).

Tuotannon ja toiminnan turvallisuuteen liittyviä yleisempiä riskejä ovat yhteistyökumppanin epäluotettavuus, tahallisen perättömän tiedon levittäminen, tuotteiden tai tuotemerkkien plagiointi, pimeän työvoiman käyttö ja epätavallinen hävikki, taloushallintoon liittyvät väärinkäytökset, vahingollisella tiedolla kiristäminen ja lah-

jonta (Yritysten rikosturvallisuus 2012, 46). Erityisen tärkeätä on Keskusrikospoliisin mukaan (2012, 9) suojata huolellisesti maksutietoja sisältävä välineistö. Tuotannon ja toiminnan turvallisuudessa voidaan vähentää riskejä muun muassa sillä, että pyritään aina tekemään kirjalliset sopimukset yhteistyötahojen kanssa, asiantuntijat tarkistavat ja laativat sopimustekstit ja -pohjat, yrityksen johto tarkistaa merkitykseltään keskeiset liiketoimintasopimukset, taloushallintoon liittyviä mahdollisia väärinkäytöksiä torjutaan ja auditoidaan (Yritysten rikosturvallisuus 2012, 52–54).

3.5 Pelastustoiminta

Yritysten keskeiset, pelastustoimintaan liittyvät velvoitteet määräytyvät pelastuslaissa (2011/379). Sen keskeisenä sisältönä on ehkäistä tulipaloja ja muita onnettomuuksia, varautuminen niihin ja seurauksien rajoittaminen. Lisäksi väestönsuojavelvoitteet ja velvoitteet pelastustoimintaan osallistumisesta määritellään pelastuslaissa.

Pelastuslaissa määritellään myös tulipaloihin ja muihin onnettomuuksiin liittyvästä uhkien ennakoinnista ja varautumisesta eli riskienhallinnasta. Tavoitteena on ennakoida, poistaa, minimoida ja vakuuttaa palo- ja onnettomuusriskejä (Yritysturvallisuus EK 2009). Pelastuslaissa (2011/379) säädetään myös pelastussuunnitelman laatimisvelvoitteesta ja muista kiinteistön- ja toimitilojen vaadittavista rakenteellisista ominaisuuksista. Pelastautumisharjoituksilla harjoitellaan yrityksen toimitiloista pelastautumista, jotta se olisi todellisessa tilanteessa helpompaa. Vakuutusyhtiöt asettavat myös omat vaatimuksena palo- ja pelastustoimintaan liittyen. Yritysturvallisuusneuvottelukunnan mukaan rakennuksen paloturvallisuutta tulisi edistää esimerkiksi kiinteistön osien paloluokittelulla, rakennuksen kantavilla rakenteilla, palo-osastoimalla kiinteistö, pelastus- ja sammutusjärjestelyillä, tuhopolttojen torjunnalla, alkusammutuskalustolla, automaattisella sammutuslaitteistolla ja paloilmoitinjärjestelmällä, savunpoistolla, turva- ja merkkivalaistuksella sekä turvallisuusopasteilla (Yritysturvallisuus EK 2009).

Työntekijöiden alkusammutusosaamisen ja ensiapukoulutuksen kehittäminen edistää myös yrityksen pelastustoimintaan liittyvää turvallisuutta (Yritysturvallisuus EK

2009). Pelastusviranomaiset tekevät tarkistuksia yritysten tiloihin selvittääkseen, ovatko pelastuslain mukaiset velvoitteet täytetty. Pelastusviranomaisten velvoitteista ja toiminnasta on myös säädetty pelastuslain (2011/379) luvussa neljä.

3.6 Ulkomaantoimintojen turvallisuus

Yritysturvallisuusneuvottelukunnan mukaan ulkomaantoimintojen turvallisuudella varmistetaan henkilöstön turvallisuustaso heidän työskennellessään ulkomailla (Yritysturvallisuus EK 2009). Ulkomailla työskenneltäessä kohdemaan palvelut ovat erilaisia ja voivat poiketa kotimaan palvelutasoista huomattavasti. On myös hyvä ottaa selvää kohdemaan turvallisuustilanteesta ja tunnistaa erityisen konfliktiherkät maat (Keskusrikospoliisi 2012, 19). Joissain konfliktiherkissä maissa voi esimerkiksi olla yleinen uhka länsimaalaisten sieppauksille ja väkivallanteoille, kuten esimerkiksi Afganistanissa, Jemenissä tai Pakistanissa. Lisäksi suomalaiset työmatkustajat voivat joutua muita maita vastaan suunnatuissa iskuissa vaaraan.

Kuitenkin suomalaisiin kohdistuva varsinainen terroriuhka ulkomailla on varsin vähäinen tällä hetkellä Suojelupoliisin mukaan (Keskusrikospoliisi 2012, 19). Suomen ulkoasiainministeriö julkaisee matkustustiedotteita maakohtaisesti, joissa kerrotaan maiden turvallisuustilanteiden aiheuttamista mahdollisista riskeistä ja Suomen edustoista maittain (Suomen ulkoasiainministeriö 2013).

Matkustusohjeilla yritys voi ennaltaehkäistä ja pyrkiä ennakoimaan henkilöstön ulkomailla työskentelyn turvallisuutta (Yritysten rikosturvallisuus 2012, 18). Matkustusvalmistelut tulisi hoitaa asianmukaisesti, aina matkasuunnitelman laatimisesta, passien ja muiden matkustusasiakirjojen hankkimisesta, rokotuksiin ja matkustamisjärjestelyihin (hotellien ja muiden varaaminen, matkaliput) (Leppänen 2006, 210). Matkan yksityiskohdista tulee myös informoida työpaikkaa ja kotiväkeä, sekä tarvittaessa jättää kopiot matka-aikatauluista, hotellien yhteystiedoista, paikallisesta yhteyshenkilöstä ja ohje toiminnasta poikkeustilanteessa.

Kun toimitaan työtehtävissä ulkomailla, tulee kohdemaatietoisuuden lisäksi selvittää yhteistyökumppaneiden taustat ja toimintatavat (Leppänen 2006, 211). Työnantajan antamiin matkustusohjeisiin ulkomailla tulee myös sisällyttää ohje tiedon

käsittelystä ulkomailla (Yritysten rikosturvallisuus 2012,18). Lisäksi tulee selvittää, yritysturvallisuusneuvottelukunnan mukaan työntekijän ulkomailla olon aikaiset terveydenhuoltoasiat ja raha-asiat, verotus, sekä yleiset matkustus-, liikenne- ja majoitus- turvallisuusnäkökohdat (Yritysturvallisuus EK 2009).

3.7 Ympäristöturvallisuus

Yritysturvallisuusneuvottelukunnan mukaan ympäristöturvallisuuden tavoitteena on ekologinen kestävyys ja ympäristöodotusten ennakointi suhteessa yhteistyökumppaneihin, yhteiskuntaan ja asiakkaisiin, sekä ympäristöystävällisten prosessien ja käytäntöjen kehittäminen yritystoiminnassa (Yritysturvallisuus EK 2009). Yritysten tulisi siis kantaa vastuunsa ympäristöstä, sekä lisätä tietoisuutta ympäristöystävällisistä toimintatavoista. Ympäristöturvallisuuden velvoitteita liiketoiminnalle säätelevät kansallinen ja kansainvälinen ympäristölainsäädäntö, sekä erilaiset standardit ja laatujärjestelmät. Ympäristöturvallisuuteen liittyvät myös yritystoiminnassa kestävän kehityksen periaatteet, ympäristövaikutusten arviointi, ilmoitus- ja lupamenettelyt, vaarallisten aineiden käsittely ja varastointi, ympäristönsuojelun hallintajärjestelmä ja toimintaohjelma, ilmasuojelu ja päästökauppa, vesien ja maaperän suojelu (erityisesti pohjavesialueilla sijaitsevat yritykset), melutorjunta ja maisemansuojelu, kemikaalivalvonta ja jätehuolto.

3.8 Valmiussuunnittelu

Yritysturvallisuusneuvottelukunnan mukaan valmiussuunnittelu liittyy Suomen puolustustaloudelliseen suunnitteluun ja yhteiskunnan huoltovarmuuden varmistamiseen kriisitilanteiden aikana (Yritysturvallisuus EK 2009). Kriisitilanteita voivat olla erilaiset yhteiskuntaa uhkaavat häiriötilanteet tai poikkeusolot, kuten esimerkiksi tulvat, myrskyt, maanjäristykset, sodat tai konfliktialueen lähialueilla oleminen (Leppänen 2006, 305). Lisäksi järjestäytynyt rikollisuus voi kohdistua myös yhteiskunnan kriittisiin toimintoihin.

Yritysten, jotka ylläpitävät yhteiskunnan kriittisiä infrastruktuureja on valmistauduttava häiriötilanteisiin ja poikkeusoloihin (2011/1552). Yritysturvallisuusneuvottelu-

kunnan mukaan valmiussuunnitteluun kuuluvat varautuminen poikkeusoloihin, tuotannon ja toiminnan suunnittelu, riskiarvioinnin tarkistaminen poikkeusoloihin soveltuvina, energiahuolto, raaka-aineet, koneet ja laitteet, korjaus- ja huoltotoiminta, varaosat, materiaalivarastointi, alihankinta- ja muut palvelutyöt, sekä henkilövaraukset (Yritysturvallisuus EK 2009).

3.9 Tietoturvallisuus

Tietosuoja ja tietoturva tulee määritelminä erottaa toisistaan, sillä ne kuvaavat käytännössä aivan eri asioita (Laaksonen, Nevansalo & Tomula 2006, 17–33). Tietosuoja on ihmisen tiedollista itsemääräämisoikeutta ja yksityisyyttä, sitä säätelevät perustuslain 10§ määritelmä yksityisyyden suojasta, laki yksityisyyden suojasta työelämässä (2004/759) ja sähköisen viestinnän tietosuojalaki (2004/516). Tietoturva taas on valikoima keinoja ja toimintamalleja, joiden tarkoitus on tietosuojan ylläpitäminen. Tietoturvallisuudesta ei ole olemassa yksittäistä lakia, sen keskeisin määrittäjä on henkilötietolaki (1999/523), jossa asetetaan ohjeet muun muassa henkilörekisterin ylläpitämiseen ja suojaamiseen.

Suomi on valtiona muuttunut tietoyhteiskunnaksi, minkä vuoksi on elintärkeätä tiedostaa tietoverkkojen ja -järjestelmien toimintojen keskeinen asema (Valtioneuvoston periaatepäätös 2013, 1). On alettu puhua kybertoimintaympäristöstä, jolla tarkoitetaan yhteiskunnan haavoittuvuutta ja riippuvuutta suhteessa sähköiseen tiedonkäsittely-ympäristöön. Kyberturvallisuuden tavoitteena on sähköinen tiedonkäsittely-ympäristön turvallisuus. Tässä opinnäytetyössä käsitellään tietoturvallisuutta kuitenkin perinteisten lähestymistapojen mukaan.

Tietoturvallisuus on yksi yritysturvallisuuden osa-alue, jonka merkitys on keskeinen liiketoiminnallisen jatkuvuuden ja kilpailukyvyn turvaamisessa (Yritysturvallisuus EK 2009). Jokaisesta yrityksestä löytyy taloudellisesti arvokasta tietoa, jonka menetys ulkopuoliselle aiheuttaa vahinkoa (Yritysten rikosturvallisuus 2012, 23). Siitä syystä on tärkeää arvioida erilaisten tietokokonaisuuksien merkitys yritystoiminnalle ja sen asiakkaille. Tiivistettynä olennaista on, että oikeaa tietoa menee oikeaan paikkaan ja näin pystytään tukemaan yrityksen nopeaa reagoimista alati muuttuvissa liike-elämän tilanteissa (Rantala & Virta 2006, 77).

Tietoturvallisuuden klassiseen määritelmään kuuluu kolme osa-aluetta, joita ovat tiedon eheyden, käytettävyyden ja luottamuksellisuuden suojaus (Leppänen 2006, 260). Tiedon eheydellä tarkoitetaan tiedon sisällöllistä vahingoittumattomuutta, oikeellisuutta ja muuttumattomuutta. Kun tieto on eheää, se on kokonaisuudessaan saatavilla. Tieto on käytettävää silloin, kun sen oikeutetulla käsittelijällä on mahdollisuus synnyttää, käsitellä, muuttaa, hyödyntää, siirtää, sekä niin halutessaan tuhota tieto. Tiedon luottamuksellisuuteen kuuluu tietojen luokittelu, käyttäjien hallinta, suojaamistoimenpiteet, sekä yksityisyyden suojan varmennus. Yritysturvallisuusneuvottelukunta ottaa edellä mainittujen, kolmen osa-alueen lisäksi mukaan myös tiedon todistettavuuden, kiistämättömyyden ja varmenteet (Yritysturvallisuus EK 2009).

Tietämättömyys tai välinpitämättömyys on yleensä syynä toteutuneisiin tietoriskeihin, niitä voidaan välttää esimerkiksi kriittisen tiedon tunnistamisella, tiedon luokittelulla, henkilökunnan koulutuksella ja tietoon liittyvillä ohjeistuksilla (Yritysten rikosturvallisuus 2012, 28–30). Tietoturvallisuuden osa-alueita ovat Valtiohallinnon tietoturvallisuuden johtoryhmän mukaan seuraavat (Valtiovarainministeriö 2003, 6):

- hallinnollinen tietoturvallisuus
- fyysinen tietoturvallisuus
- henkilöturvallisuus
- tietoaineistoturvallisuus
- ohjelmistoturvallisuus
- laitteistoturvallisuus
- tietoliikenneturvallisuus
- käyttöturvallisuus

Hallinnollinen tietoturvallisuus. Hallinnollinen tietoturvallisuus on turvallisuusjohtamisen keskeinen osa-alue, joka rakentuu erilaisista tietoturvallisuuden johtamisen hallintamenettelyistä (Leppänen, 2006, 285). Hallinnollinen tietoturvallisuus on tietoturvallisuuden toimintapolitiikkaa ja ohjeistoa, toiminnan linjauksia, organisointia, resursointia ja vastuunjakoa (Kauppa- ja teollisuusministeriö 2006, 6).

Fyysinen tietoturvallisuus. Fyysisellä tietoturvallisuudella tarkoitetaan tietoaineistojen, -välineiden ja -laitteistojen, sekä niiden sijoituspaikkojen rakenteellista ja toiminnallista suojaamista (Leppänen 2006, 287). Tavoitteena on suojata tieto, erilaisissa olomuodoissaan. Tietoa siis pyritään suojaamaan vahingoittumiselta esimerkiksi tulipaloissa, vesi- ja kosteusvaurioilta, sähkökatkoilta tai -pulsseilta, pölyltä ja muilta ilmastointiriskeiltä, varkauksilta, kavalluksilta, tuhotöiltä, luvattomalta kopioinnilta, salakatselulta tai -kuuntelulta tai laittomalta tiedonhankinnalta.

Henkilöturvallisuus. Henkilöturvallisuus tarkoittaa tietoturvallisuudessa sitä, että varmistetaan tietojärjestelmään oikeutetusti pääsevien käyttäjien toimintakykyisyys ja rajataan käyttöoikeuksia (Hakala, Vainio & Vuorinen 2006, 11). Käytännössä se tarkoittaa vastuiden ja oikeuksien määrittelyä, koulutuksia ja perehdyttämisiä. Tietyillä toimialoilla on myös tarpeen selvittää tarkemmin työntekijän taustatietoja. Lisäksi henkilöstön soveltuvuuden, toimenkuvien, sijaisuuksien, tiedonsaanti- ja käyttöoikeuksien, suojaamisen turvallisuuskoulutuksen ja valvonnan voidaan katsoa kuuluvan henkilöstöön liittyvään tietoturvallisuuteen (Valtiovarainministeriö 2003,13).

Ohjelmistoturvallisuus. Ohjelmistoturvallisuudella tarkoitetaan käyttöjärjestelmiä ja sovellusohjelmistoja, jotka ovat osana organisaation päivittäistä arkea (Leppänen 2006, 302). Käyttöjärjestelmien ja sovellusohjelmistojen tietoturvallisuutta voidaan parantaa päivityksillä, henkilöstön ohjeistuksella ja turvallisen käytön opastuksella. Ohjelmistoturvallisuuteen kuuluu myös sovellusten sopivuus käyttötarkoitukseen, ohjelmistojen yhteensopivuus (integraatio), lisenssihallinta, asennusohjeet ja toiminnan luotettavuus sekä virheettömyys (Hakala ym. 2006, 11).

Laitteistoturvallisuus. Laitteistoturvallisuus liittyy laitteiden hankintapolitiikkaan, jonka tulee pohjautua käyttötarpeisiin ja vaatimuksiin (Leppänen 2006, 301). Laitteistoturvallisuus sisältää laitekannan ylläpidollisia asioita, kuten laitteistokirjanpitoa, laitekaappien lukitusta ja valvontaa, laitetiloihin pääsy, laitteiden sijoittelu, huoltosopimukset, laitteistojen muistien tyhjennystä asianmukaisesti (päällekirjoitus tai tuhoaminen).

Tietoliikenneturvallisuus. Tietoliikenneturvallisuus muodostuu tietoliikenteen ja viestintäverkkojen turvallisuuden varmistamisesta (Leppänen 2006, 292). Tietolii-

kenne rakentuu useista eri osista, joissa tieto tulisi välittää eheänä ja muuttumattomana perille. Lähi- ja laajakaistaverkkoyhteyksien sekä muiden viestintäyhteyksien turvallisuus kuuluu tietoliikenneturvallisuuteen (Hakala ym. 2006, 12). Lisäksi siihen kuuluu matkapuhelin-, data- ja videoliikenneyhteydet (Leppänen 2006, 292). Päätelaitteet, reitittimet, palvelimet, siirtotiet ja erilaiset ohjelmistot ovat sisäisen viestintäverkon osia.

Käyttöturvallisuus. Käyttöturvallisuuden tavoitteena on pitää huolta siitä, että henkilöstössä kaikki ovat sisäistäneet tietoturvallisuuteen liittyvät toimintaohjeet (Leppänen 2006, 303). Valtiovarainministeriön mukaan käyttöturvallisuus käsittää tietotekniikan käyttöön, käyttöympäristöön, tietojenkäsittelyyn ja sen jatkuvuuteen sekä tuki-, ylläpito-, kehittämis- ja huoltotoimintoihin liittyvät keinot tietoturvallisuuden parantamiseksi (Valtiovarainministeriö 2003, 22).

Tietoaineistoturvallisuus. Tietoaineistoturvallisuus on sitä, että pyritään hallitsemaan tietojen kokoamista, käyttöä, säilyttämistä, siirtämistä ja tuhoamista (Leppänen 2006, 262). Luokiteltaessa tietoa eri luokkiin sen esiintulon kriittisyyden perusteella, voidaan määritellä eri suojaustasoja, tietojen omistajan asettamien perusteiden mukaisesti (Valtiovarainministeriö 2008, 48). Tieto voidaan luokitella Valtiovarainministeriön mukaan (2009) viiteen eri luokkaan (Kuvio 5):

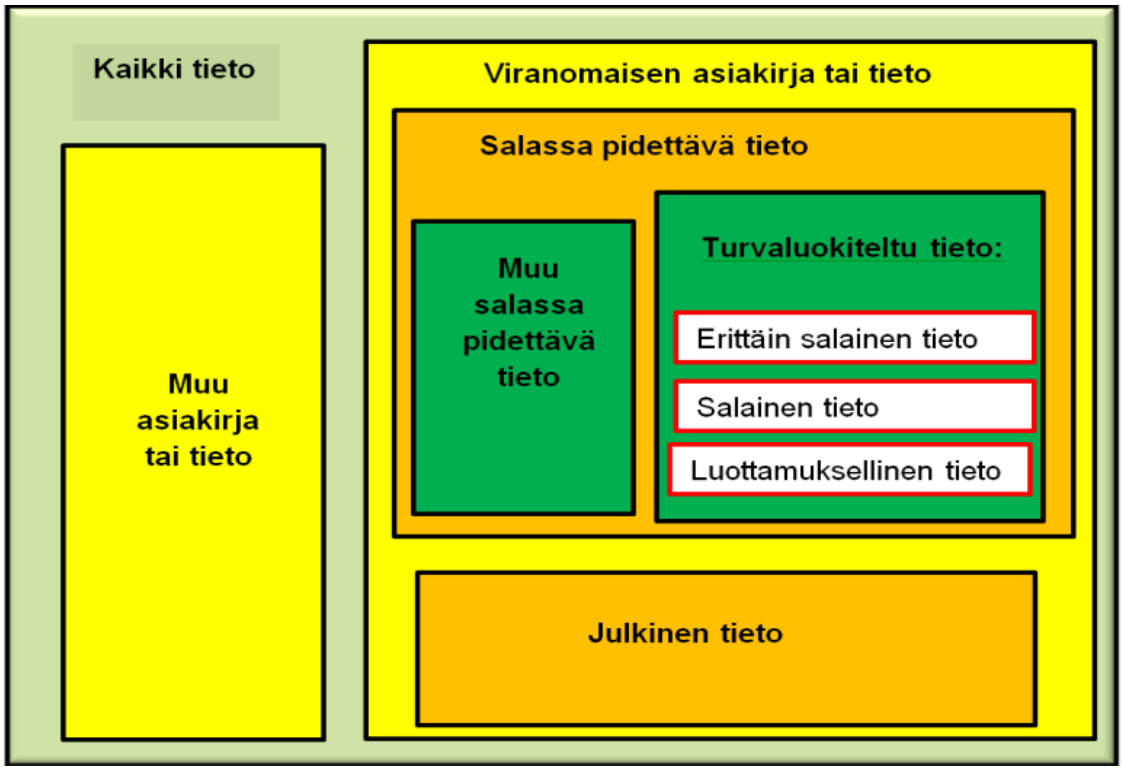
1. Julkinen tieto
2. Sisäinen tieto, myös viranomaiskäytössä olevat tiedot ja ei tietoa sivullisille tiedot
3. Luottamuksellinen tieto
4. Salainen tieto
5. Erittäin salainen tieto

Julkinen tieto on esimerkiksi yrityksen nettisivuilla tai muissa julkisissa lähteissä oleva tieto, joka on kaikkien saatavilla, jaettavissa ja käytettävissä (Leppänen 2006, 269). Kaikki julkinen tieto ei kuitenkaan ole kaupallisesti hyödynnettävää; esimerkiksi tekijänoikeuksien, tavaramerkki- ja patenttioikeuksien ynnä muiden immateriaalioikeuksien avulla suojataan julkisesti saatavilla olevia tuotteita ja teoksia. Yrityksen sisäisen tiedon ominaisuuksia ovat laaja käsittelytarve, korkea käy-

tettävyys ja tarpeellisuus päivittäisessä työssä. Tavoitteena on, että sisäinen tieto ei leviä henkilöstön ulkopuolisille tahoille, vaikka se ei aina merkittävää haittaa aiheuttaisi organisaatiolle.

Luottamuksellinen tieto sen sijaan voi vahingoittaa organisaatiota, sen henkilöstöä tai jotain kolmatta osapuolta tullessaan ilmi (Leppänen 2006, 273–274). Salainen tieto on tietoa, joka vaarantaa oleellisesti tai pysyvästi yrityksen keskeisiä tavoitteita ja aiheuttaa merkittävää vahinkoa organisaatiolle, sopimuskumppanille tai kolmannelle osa-puolelle. Salaista on tieto, joka on laissa tai asetuksessa määrätty salassa pidettäväksi, esimerkiksi lakisääteinen vaitiolovelvollisuus tai salassa pidettävät viranomaisasiakirjat.

Erittäin salaiseksi luokiteltua tietoa harvoissa yrityksissä käsitellään ja sillä tarkoitetaan lähinnä tietoa, joka vahingoittaa valtion turvallisuutta ilmi tullessaan (Leppänen 2006, 274). Myös tieto, joka merkittävästi vaarantaa henkilön tai organisaation turvallisuuden voi joissain kohtaa olla erittäin salaiseksi luokiteltua. Erittäin salaista tietoa käsiteltäessä on jatkuvasti oltava varma, ettei missään olosuhteissa tietoa luovuteta muille kuin erikseen hyväksytyille henkilöille.



Kuvio 5. Tietoaineistojen turvaluokittelu (Valtiovarainministeriö 2009).

4 Teemahaastattelututkimus PK-yrityksille

4.1 Tutkimusmenetelmä

Toimeksiantona oli riippumattoman ja julkisen tutkimuksen tekeminen opinnäytetyön muodossa. Opinnäytetyön alkutaipaleella oli jo selkeästi suuntana kvalitatiivinen eli laadullinen tutkimus. Tavoitteena oli muodostaa PK-yritysten koottujen, yritysturvallisuuden hallintaan liittyvien tarpeiden ja käsitteiden profiili. Opinnäytetyö on osa Opsec Oy:n laajempaa turvallisuuspalveluiden kehitystyötä.

Palvelumuotoilulla tarkoitetaan Tuulaniemen (2011, 146) mukaan systemaattista tapaa lähestyä palveluiden suunnittelua ja kehittämistä, joka on samanaikaisesti analyyttistä ja intuitiivista. Analyyttinen lähestyminen tarkoittaa päättelyä loogisista tosiasioista, asiakastutkimuksista ja datasta. Intuitiivinen tarkoittaa taidon ja kokemuksen avulla näkemistä. Asiakasymmärryksen tiedonkeruumenetelmiä voivat olla palveluiden käyttäjätietoa hankittaessa esimerkiksi haastattelut ja eri menetelmillä toteutettavat kyselyt. Riippumatta tutkimustyypistä aineiston keräämisen perusmenetelminä käytetään havainnointia ja erilaisia dokumentteja, sekä haastatteluiden tekemistä (Hirsjärvi, Remes & Sajavaara 2009, 192).

Tiedonkeruutapana käytettiin haastattelumenetelmää, koska sillä tavoin pystyttiin myös kuvailemaan haastateltavien käyttämää sanastoa ja näkemään, millaisia sisältökokonaisuuksia he hahmottavat turvallisuudesta. Haastattelumenetelmää käyttäen oli mahdollista myös kuvailla ja tulkita monipuolisesti, abstraktiotason asioita ja ajatuksia liittyen tutkittavaan asiaan. Haastattelumenetelmässä aineiston keruun sääteleminen tilanteen mukaan mahdollistaa myös tutkimusaineiston laatuun ja määrään vaikuttamisen (Hirsjärvi ym. 2009, 205).

Tutkimushaastattelut jaetaan sillä perusteella eri ryhmiin, kuinka jäsennelty tai muodollinen haastattelutilanne on (Hirsjärvi ym. 2009, 208). Ne jaetaan kolmeen ryhmään: täysin strukturoituun eli lomakehaastatteluun, teemahaastatteluun ja avoimeen haastatteluun. Tässä kohtaa käytettiin teemahaastattelumenetelmää, sillä sen avulla oli parhaiten mahdollista saada tietoa tutkittavasta asiasta. Tarkoitus oli lisäksi saada ennalta määritellyistä aihekokonaisuuksista enemmän tietoa.

4.2 Teemahaastattelu

Teemahaastattelu on täysin strukturoidun ja avoimen haastattelun välimuoto, jossa aihealueisiin liittyvien kysymysten järjestys on vapaa (Hirsjärvi ym. 2009, 208). Teemahaastattelussa pystyy ohjailemaan keskustelua ennalta määriteltyjen teema-alueiden suuntaisesti ja tekemään tarvittaessa tarkennuksia (109). Teema-alueet määritellään ennalta ja ne ovat kaikille samat (66–67). Kuitenkin niiden on oltava väljästi määrittelyt, jotta saadaan hyvin esiin se todellisuuden monimuotoisuus ja rikkaus, mikä tutkittavaan ilmiöön ja sen osailmiöihin tosiasiallisesti liittyy.

Teemahaastattelut toteutettiin yksilöhaastatteluina. Useamman henkilön ryhmissä olisi voinut olla riski ns. sosiaalisesti suotavien vastausten antamisesta suurempi. Tutkimusongelma ja aihealue asettivat myös tiettyjä eettisiä edellytyksiä tutkimuksen toteutuksen suhteen. Haastatteluissa mukana olevia yritykset ja henkilöt eivät saaneet olla tunnistettavissa toisilleen tai tutkimuksen ulkopuolisille tahoille.

4.3 Teema-alueet

Teema-alueiden asettamisen määrittelevät tutkimusongelma, aihealueen luonne, tutkimusaiheen pääluokat ja analysoitavat kohteet (Hirsjärvi ja Hurme 2008, 65–68). Teemahaastattelumenetelmän käytössä keskeisin onnistumisen määrittäjä on teema-alueiden asettaminen. Teema-alueiden määrittämisen vuoksi on tärkeää perehtyä tutkimusaiheeseen liittyvään teoreettiseen tietoon ja tehtyihin tutkimuksiin aiheesta. Tässä opinnäytetyössä teemahaastattelututkimus jaettiin kolmeen teema-alueeseen:

1. Käsitteiden määrittely (turvallisuus, yritys- tai organisaatioturvallisuus, tietoturvallisuus ja riski)
2. Tilannekartoitusta ja kokemusta
3. Yrityskokoluokkien eroavaisuudet ja tulevaisuuden ideointia

Ensimmäisen teema-alueen keskeinen tarkoitus oli päästä selville siitä, miten haastateltava mieltää kyseiset asiat ja siten selventää niiden saamia merkityksiä haastattelun aikana. Tutkimushaastattelun ensimmäinen teema-alue muodostui

tutkimuksen aiheen kannalta keskeisten käsitteiden määrittelystä. Haastateltavia pyydettiin kertomaan, mitä kustakin käsitteestä tulee ensimmäisenä mieleen, ja mitä siihen liittyy ja sisältyy. Määriteltäviä käsitteitä olivat turvallisuus yleisesti, yritysturvallisuus, tietoturvallisuus ja riskit. Turvallisuuden, yritysturvallisuuden ja tietoturvallisuuden kohdalla kysyttiin lisäksi, miten yksittäinen henkilö tai työntekijä pystyy niiden toteutumista edistämään. Riskien kohdalla kysyttiin vastaavasti, miten niitä pystyy tunnistamaan ja hallitsemaan.

Tutkimushaastattelun toisessa teema-alueessa tarkoituksena oli hahmottaa yritysturvallisuuden käytäntöä, osa-alueiden jakaantumista ja vastuutusta haastateltavien yrityksissä. Tarkoitus oli myös selvittää, mikä painoarvo on suojattavien kohteiden suhteen haastateltavien yrityksissä. Toisen teema-alueen alussa jokaiselle haastateltavalle näytettiin paperille tulostettu kuva Suomen Elinkeinokeskuksen yritysturvallisuuden osa-alueista (Kuva 4, s.18). Kuvassa on koostettu ympyrän muotoon 10 yritysturvallisuuden osa-aluetta ja keskellä on viisi tyypillistä suojattavaa kohdetta yrityksissä.

Kuva otettiin haastattelun oheismateriaaliksi siitä syystä, että haastateltavilla olisi jotain konkreettista havaintomateriaalia tutkittavasta asiasta. Yritysturvallisuuden kokonaisuuden ja toisaalta eri osa-alueiden hahmottaminen helpottui kuvan avulla haastatteluissa. Sen avulla oli helpompi verrata turvallisuuden tarpeiden ja mahdollisten ongelmakohtien eroavaisuutta kahdessa eri yrityskokoluokassa, suuriksi luokiteltavissa yrityksissä ja PK-yrityksissä.

Tutkimushaastattelun kolmannen teema-alueen tarkoitus oli pyrkiä löytämään PK-yritysten keskeisiä tarpeita ja mahdollisia ongelmakohtia turvallisuuden hallinnassa. Haastateltavia pyydettiin myös miettimään, mistä asioista tavoiteltava turvallisuuden tila muodostuu PK-yrityksissä ja sitä kautta hahmottelemaan tavoitteita yritysturvallisuuden suhteen. Lisäksi pyrittiin kartoittamaan keskeisiä odotuksia ja kehittämisideoita turvallisuusalan tarjonnassa yleisesti.

4.4 Haastateltavat

Tavoitteena oli saada teemahaastatteluihin haastateltavia 5-9 PK-yrityksestä Etelä-Pohjanmaan alueelta. Haastateltavat poimittiin harkinnanvaraisesti toimeksiantajan toimesta. Tarkoituksena oli saada tutkimukseen haastateltavia pienistä ja keskikokoisista yrityksistä, sekä eri toimialoilta. Tällä tavoin pystyttiin varmistamaan tutkimusaineiston monipuolisuus ja osittain myös välttämään tutkimuksen painottumista liiaksi johonkin tiettyyn osa-alueeseen.

Kvalitatiivisten haastatteluiden kohdalla tutkimusaineiston heterogeenisyys sekä kokonaisuutena että tutkimusryhmien sisällä on rikkaus, olettaen tarkoituksen olevan ymmärryksen rakentaminen ja lisääminen tutkittavasta asiasta (Vilkka 2005, 127). Laadullisessa tutkimuksessa ei ole olennaista haastattelujen määrä, vaan niiden laatu (126). Siksi haastateltavien valinnassa on otettava huomioon haastateltavien kyky kertoa asioista, joita on tarkoitus tutkia (Hirsjärvi ym. 2008, 60). Haastateltavien valinnassa otettiin huomioon heidän kykynsä kuvata tutkittavaa asiaa, mikä tässä kohtaa tarkoitti haastateltavan työkokemusta alaltaan ja tekemisissä oloa yritysturvallisuuden kanssa.

Näytteen kooksi muodostui lopulta yhdeksän PK-yrityksen edustajaa, joista seitsemän osallistui tutkimushaastatteluun. Kaksi haastateltavaa kieltäytyi osallistumasta tutkimukseen, toinen ajanpuutteen vuoksi ja toinen ilmoitti asiasta viime hetkellä. Alun perin molemmat olivat lupautuneet haastateltaviksi. Tutkimuksen suunnitelluista osallistujista 78 %, eli seitsemän haastateltiin.

Haastatelluista neljä edustivat yksityisen sektorin teollisuusyrityksiä, kaksi edustivat useamman kunnan omistuksessa olevaa palveluorganisaatiota ja yksi edusti yksityisen sektorin palveluyritystä. 57 % eli neljä haastatellusta toimi teollisuusalalla ja kolme toimi palvelualan eri sektoreilla. Jokainen yritys, tai julkisessa omistuksessa oleva liikelaitos- tai kuntayhtymä täytti PK-yrityksen kokoluokkamääritelmän henkilöstön määrän ja rahaliikenteen määrien suhteen. Tässä opinnäytetyössä viitataan molempiin termillä PK-yritys (PK-yrityksiin- ja organisaatioihin).

Haastateltavilla oli kokemusta omalta alaltaan 8-27. Vähintään viidellä haastateltavalla oli omalta alaltaan yli 15 vuotta työkokemusta. Haastateltavilla oli kaupallisia,

tietoteknisiä ja muita teknisiä koulutuksia ja tutkintoja. Työkokemusta heillä oli paitsi nykyisestä työtehtävästään, yli puolella haastateltavista oli myös muista toimenkuvista ja yrityksistä. Ainakin yhdellä haastateltavalla oli myös työkokemusta ulkomaisesta yrityksestä.

Haastateltavien titteleitä olivat

- toimitusjohtaja
- yrityskehityspäällikkö
- talouspäällikkö
- tietohallintopäällikkö
- tietohuoltosihteeri
- teknologiapäällikkö
- atk -vastaava

4.5 Haastattelutilanteet

Haastatteluajankohdat sijoittuivat aikavälille 9.4.2013–29.5.2013. Ennen haastatteluja haastateltaville lähetettiin saatekirje, jossa kerrottiin tutkimuksen toteuttamisesta (Liite 1). Haastatteluajankohdat sovittiin puhelimitse, opinnäytetyöntekijän ja haastateltavien kesken. Haastattelut oli jaettu kolmeen osaan, toisessa osassa haastateltaville näytettiin Elinkeinokeskuksen kuva Yritysturvallisuuden osa-alueista (Kuva 4, s.18), jotta heillä olisi jotain konkreettista materiaalia, jolla hahmottaa yritysturvallisuuden osa-alueita.

Haastattelut kestivät 50 minuutista puoleentoista tuntiin. Haastattelut pidettiin haastateltavien yritysten tiloissa. Haastattelut tallennettiin MiniDisc -nauhurilla. Haastatteluiden jälkeen haastateltaville lähetettiin kiitoskirje (Liite 2) osallistumisesta tutkimukseen. Haastateltaville annettiin mahdollisuus tarkistaa oma osuutensa haastattelujen raportoinnista. Lopuksi haastateltaville kerrottiin, missä valmis opinnäytetyö on nähtävillä.

4.6 Haastattelujen analyysi

Opinnäytetyössä käytettiin aineistolähtöistä sisällönanalyysia. Aineiston analyysin vaiheet jaetaan kolmeen osaan, joita ovat aineiston luokittelu, analysointi ja tulkinta (Ruusuvuori, Nikander & Hyvärinen 2010, 11–20). Lähestymistapa aineistoon ja päätelmien tekemiseen oli induktiivinen, eli aineistolähtöinen. Käytännössä se tarkoittaa sitä, että päätelmät on tehty tutkimusaineiston avulla, eikä esimerkiksi pyritä todentamaan teoreettisia johtoideoita aineiston pohjalta (Hirsjärvi ja Hurme 2008, 136).

Haastattelut purettiin auki ja litteroitiin tekstinkäsittelyohjelmaan riittävällä tarkkuudella. Jokainen haastattelu purettiin omaksi tiedostokseen, jolloin oli mahdollista tarkastella jokaisen haastateltavan antamia vastauksia erillisenä kokonaisuutena. Aineistosta muodostettiin myös teema-alueittainen kuva kokoamalla haastateltavien antamat vastaukset yhteen teemoittain. Sen jälkeen aineistoon perehdyttiin ja sitä luettiin, sekä tarkasteltiin eri näkökulmista. Tämän jälkeen voitiin siirtyä varsinaiseen analyysivaiheeseen.

Aluksi aineisto koodattiin, luokiteltiin ja siitä laskettiin sisältöjä. Eroavaisuuksia ja yksityiskohtia tarkasteltiin, tekemällä arviota haastatteluaineiston yhdenmukaisuudesta. Seuraavaksi aineistoa kuvattiin sanallisesti ja merkityksiä tiivistettiin, muodostettiin kokonaiskuva haastatteluaineistosta. Merkityksiä siis tuotettiin toistuvuuksien etsinnällä ja vertailuja tekemällä. Tutkimusongelman kannalta keskeisistä sisällöistä tehtiin erittelyä ja yhteenvetoa. Haastatteluaineistoa tarkasteltiin ja tulkittiin myös teoreettisen viitekehyksen näkökulmasta. Lopuksi niistä koottiin PK-yritysten koottujen yritysturvallisuuden hallintaan liittyvä turvallisuuskäsitysten ja -tarpeiden profiili.

5 Tulokset

5.1 Turvallisuuskäsitykset

5.1.1 Turvallisuus

Ensimmäisiä ajatuksia haastateltavilla turvallisuudesta olivat sen monimuotoisuus ja kokonaisvaltaisuus, sanana sen todettiin olevan myös monikäyttöinen. Turvallisuuteen liittyivät niin henkilökohtainen materiaalinen turvallisuus kuin yksilöllinen kokemus turvallisuudesta. Osa haastateltavista pohti sen enempää miettimättä vain yritysturvallisuutta, toinen osa ajatteli edellä mainittujen lisäksi myös yhteiskunnallista turvallisuutta.

Henkilökohtaisesta turvallisuudesta tuli haastateltaville mieleen se, että turvallisuus on jotain, mikä on tunnetta ja tunnetilaa. Henkilön näkökulmasta, Haastateltava 2 näki turvallisuuden olotilana, joka lisää hyvinvointia, vähentää pelkoa ja asioiden jahkailua. Turvallisen olotilan Haastateltava 3 näki myös koskemattomuutena ja suojassaolona. Haastateltava 5 näki myös eri sukupuolilla olevan erilaisia perinteisiä rooleja turvaamisessa ja turvallisuuden ylläpitämisessä. Lisäksi työ- ja perusterveydenhuollon laadun Haastateltava 7 kertoi olevan keskeinen asia ihmisen turvallisuuden lisääjänä.

Henkilökohtaisessa materiaalisessa turvallisuudessa haastateltavat näkivät tärkeäksi, että henkilökohtainen omaisuus niin vapaa-ajalla kuin työpaikalla säilyy asianmukaisesti ja paikallaan. Haastateltavat tarkoittivat sillä juuri esimerkiksi tavaroiden ja kulkuvälineiden turvallista säilymistä, ettei niihin kohdistu esimerkiksi ilkivallan tai varastamisen uhkaa.

5.1.2 Yritysturvallisuus

Tavoiteltava turvallisuuden tila on Haastateltavan 2 mielestä sitä: ”että kaikki turvallisuuteen liittyvät asiat ovat kunnossa siinä määrin kuin sen kokoisessa organi-

saatiossa on tarpeen”. Tavoitteisiin liittyi haastatteluissa henkilöiden, talouden ja tiedon turvallisuus. Talouden turvallisuudesta Haastateltava 7 totesi, että: ”yrityksen hyvinvointi kuitenkin muodostuu sen kautta, silloin on varaa panostaa turvallisuuteen, kehittämiseen ja yrityslainojen takaisin maksuihin”. Turvallisuuden Haastateltava 7 kertoi olevan uskoa tulevaisuuteen, esimerkiksi liiketoiminnan jatkuvuuteen ja siihen, että töitä on vielä huomennakin. Taloudellisen vakauden ja taloudellisen turvallisuuden Haastateltava 5 näki myös olevan perustana yritysturvallisuudelle. Ilman taloudellista menestystä yritys ei selviä useiden haastateltavien mukaan kuin maksimissaan viisi vuotta.

Yrityksen konkreettisten rakennusten ja tilojen merkitys turvallisuudelle tuli myös monissa haastatteluissa ilmi. Infrastruktuuriin nähtiin kuuluvaksi muun muassa kulunvalvonta, lukitukset, kamerat, rikosilmoitinjärjestelmät, sähköjen saatavuus, kulkemistiet ja poistumistiet. Olennaisena Haastateltava 1 näki esimerkiksi sen, että: ”rakennuksen ja yritystilojen käyttö on suunniteltua turvallisuuden näkökulmasta”. Pelastussuunnitelmista todettiin lainkin jo niitä vaativan. Työskentelylaitteiden huoltamisen, työntekijän fyysisten ominaisuuksien huomioonottamisen ja työympäristön muun turvallisuuden (esimerkiksi ilmanvaihto ja valaistus) nähtiin olevan keskeinen osa työn tekemiseen liittyvässä turvallisuudessa.

Haastateltavat pohtivat myös sitä, että yksittäisen henkilön kokemaan turvallisuuteen työpaikalla vaikuttavat työturvallisuusasiat ja työympäristön laatu. Monet haastateltavat painottivat paitsi työympäristön fyysiseen puoleen liittyviä asioita, myös keskinäisen luottamuksen, sosiaalisen tuen, viestinnän ja toisten huomioonottamisen merkitystä työyhteisön turvallisuuden lisääjinä.

Yrityskulttuurin todettiin myös olevan keskeisessä asemassa suhteessa siihen, miten turvallisuuteen liittyvät ohjeet ja uudet käytänteet viedään jokapäiväisessä työssä arkeen. Haastateltavan 7 mukaan työporukassa ei kuulemma tarvitse olla kuin 1-2 henkilöä, jotka eivät välitä turvallisista työtavoista ja sen jälkeen se voi levitä koko työyhteisöön. Haastateltava 7 oli sitä mieltä, että yrityskulttuuriin voi vaikuttaa omalla esimerkillä, perehdyttämisillä, koulutuksilla ja sitouttamalla.

Yrityksen turvallisuuspolitiikan eli sen, miten on määritelty yrityksen tavoitteet suhteessa turvallisuuteen, haastateltavat kokivat myös tärkeäksi. Haastateltava 2 to-

tesi: ”että kun on selvät sävelet siitä, miten toimitaan, ei tarvitse kuluttaa energiaa sen jahkailuun, mitä voi tehdä ja mitä ei”. Turvallisuuspolitiikassa voidaan esimerkiksi määritellä haastateltavien mielestä säännöt ja ohjeistukset, sekä niiden valvonta. Uuden työntekijän perehdytyksessä läpikäytävät turvallisuusasiat ja sosiaalisen median ohjeet suhteessa yrityksen tietoon nähtiin myös kuuluvan yrityksen turvallisuuspolitiikkaan.

Haastatteluissa pyydettiin haastateltavia myös pohtimaan sitä, miten yksittäinen ihminen voi omalta osaltaan vaikuttaa positiivisesti yrityksen turvallisuuteen. Haastateltavien vastauksia tähän kohtaan olivat esimerkiksi toimintatapojen huolellisuudella, noudattamalla konkreettisia pieniä johdonmukaisia käytänteitä, aktiivisuudella turvallisuuspuutteista viestittäessä ja ottamalla toiset työntekijät huomioon. Tärkeimpänä asiana Haastateltava 3 totesi, että: ”Työntekijän pitää ymmärtää oma roolinsa yrityksen menestymisen takaajana.”

5.1.3 Tietoturvallisuus

Haastatteluissa pyydettiin haastateltavia määrittelemään tietoturvallisuutta ja siihen liittyviä asioita. Salasanakäytännöt ja salasanojen vaihtaminen nähtiin neljässä haastattelussa yrityksen tietoturvallisuuteen liittyväksi keskeiseksi asiaksi. Myös virustorjunnat, palomuurit ja käyttöoikeudet, sekä niiden ajantasaisuus liitettiin tietoturvallisuuteen haastatteluissa. Yrityksen tietoturvapolitiikka mainittiin kahdessa haastattelussa ja joissain haastatteluissa tuli esille epäsuorasti siihen liittyviä asioita. Koulutukset, perehdytykset, käytännöt ja ohjeistukset liitettiin tietoturvallisuuteen kolmessa haastattelussa.

Seuraavat, tärkeäksi koetut asiat saivat jokainen yhden maininnan haastatteluissa:

- samat järjestelmät ja ohjelmat
- ohjelmavalinnat
- päivitykset keskitetysti
- nauhavarmenteet
- sähköiset allekirjoitukset
- pääsynesto ja etätuhous
- selkeät, määritellyt rajat puhuttaessa ulkopuolisille

- tiedon saatavuuden varmistus tallentamalla palvelimelle ja toimivilla yhteyksillä
- sisäisen verkon rajaus
- sopimuksilla suojaaminen ja tuotesuojaus
- ulkoyhteyksien hoitaminen ja vastuutus

Edellä mainittujen lisäksi tietoturvallisuuden inhimillinen puoli tuli mainituksi neljässä haastattelussa ja sen lisäksi yhdessä epäsuorasti yleisen huolellisuuden kautta. Haastateltava 3 totesi tietoturvallisuuteen liittyvistä työntekijäkohtaisista automaatioista ja toimintatavoista seuraavaa: ” Niihin ei tarvitse kiinnittää edes huomiota kovin paljon, kun ottaa tavaksi sulkea työ-ja asiakaskansiot ja laittaa paperit naama alaspäin, kun menee työpisteeltä pois.”

Haastateltava 1 kuvasi tietoturvallisuutta asiana, jonka suhteen keskeiset säännöt tulee olla sovittuna kaikilla ja tietoturvallisuuteen liittyviä asioita hoidetaan keskitetysti yrityksessä, jolloin: ”yksittäisen työntekijän ei niistä määräänsä enempää tarvitse huolehtia”. Haastateltava 2 myös kertoo, että: ”yritysten pitäisi sillä tavoin olla ajanhermoilla, sillä maailma muuttuu teknologian suhteen valtavalla vauhdilla ja sitä kautta myös tietoturvallisuuteen liittyvät uhat”.

5.1.4 Riskit

Haastatteluissa suurimpina riskeinä nähtiin yrityksen tietopääomaan liittyvät riskit. Yrityksen toimintaa koettiin haittaavan tiedon osittainen tai kokonaisvaltainen häviäminen. Tietovälineiden, kuten tietokoneiden tai sähköpostien toimimattomuus nähtiin myös asiana, joka aiheuttaisi toimintaan riittävästi häiriötä. Lisäksi haastatteluissa mainittiin myös tietojen suojaamiseen liittyviä riskejä, kuten tiedon leviäminen ei-toivotuille tahoille ja siten esimerkiksi tuotekehityksen tai tuotesuojauksen vaarantuminen.

Haastateltavat mainitsivat myös muita riskejä, jotka liittyvät yrityksen toimintaan tai toiminta-alaan. Riskeiksi nähtiin tulipalot, ilkivalta, laitteiden tai koneiden varastaminen, vahingonteot, ympäristöriskit, työturvallisuusriskit ja avainhenkilöriskit. Riskeistä Haastateltava 3 totesi, että: ”se on ei-toivotun asian tapahtuminen, joka pa-

lautuu loppupeleissä aina yrityksen kustannuksiin”. Liiketoiminnan jatkuvuuteen liittyvät riskit ja henkilöstöriskit nousivat myös haastatteluissa esille.

Haastateltavat puhuivat liiketoiminnallisten riskien merkityksestä ja siitä, kuinka niitä pyritään minimoimaan erilaisilla kartoituksilla, auditoinneilla, laatujärjestelmillä, poikkeama-analyyseilla. Johtoryhmien kerrottiin kokoontuvan myös siitä syystä, että he juuri tarttuvat niihin asioihin ja pyrkivät luotsaamaan yritystoimintaa kohti turvallisia vesiä. Haastateltava 5 myös toteaa, ”että aina löytyy riskejä ja tärkeintä on tiedostaa ne, vaikka aina ei olisi resursseja heti niihin varautua”.

5.2 Turvallisuusasioiden organisointi

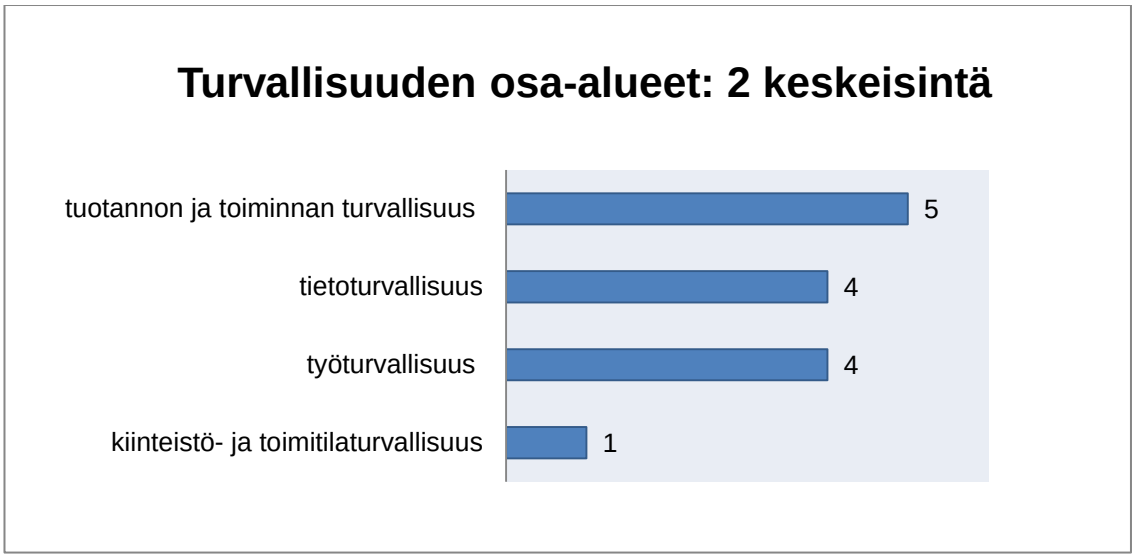
5.2.1 Yritysturvallisuuden osa-alueiden painoarvot

Haastateltavia pyydettiin valitsemaan Suomen elinkeinokeskuksen kuvasta (Kuva 4) kaksi eniten huomiota saavaa turvallisuuden osa-aluetta yrityksessään. Viiden haastateltavan mukaan kahden eniten huomiota saavan joukossa oli tuotannon ja toiminnan turvallisuus (Kuvio 6). Tuotannon- ja toiminnan turvallisuuden nähtiin olevan myös työturvallisuuden kanssa samaa asiaa, sekä vaikuttavan henkilöturvallisuuteen. Yksi haastateltava valitsi tuotannon- ja toiminnan turvallisuuden sekä työturvallisuuden yhtenä osa-alueena, koska katsoi niiden olevan samaa asiaa. Tuotannon ja toiminnan sekä työturvallisuuden korostuminen nähtiin olevan myös toimialasta riippuvaista.

Toiseksi eniten mainintoja turvallisuuden osa-alueista kahden eniten huomiota saavan joukossa oli työturvallisuus. Jaetulla toisella sijalla oli työturvallisuuden lisäksi tietoturvallisuus. Tieto- ja työturvallisuus saivat molemmat neljä mainintaa.

Tuotannon- ja toiminnan turvallisuuden sekä työturvallisuuden näki Haastateltava 1 tärkeänä siksi, että ne vaikuttavat työympäristöön ja lisäävät yrityksen houkuttelevuutta ja mainetta työpaikkana. Tuotannon ja toiminnan turvallisuuteen sekä tietoturvallisuuteen sidotaan euromääräisesti eniten yrityksessä rahaa, yhden haastateltavan mukaan. Kolme haastateltavaa kertoi, että tietoturvallisuus nähtiin myös

keskeisenä asiana yrityksen toiminnan kannalta. Yksi haastateltava kertoi, ettei heidän yrityksessään pohdita muita turvallisuuden osa-alueita kuin tietoturvallisuutta. Kolmannelle sijalle tuli kiinteistö- ja toimitilaturvallisuus, yhdellä maininnalla.

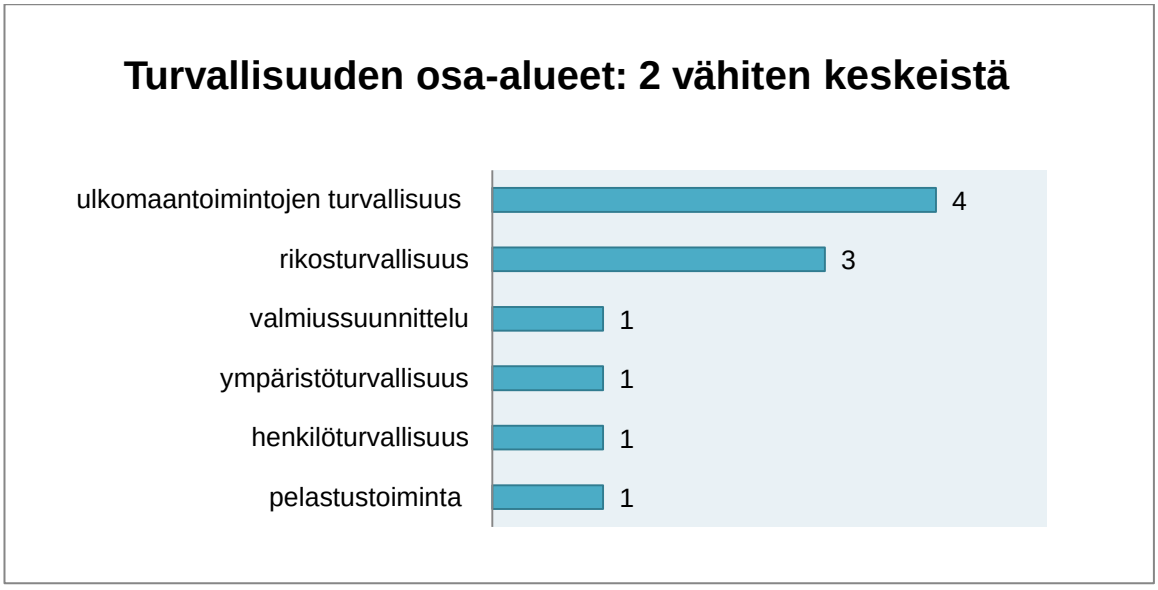


Kuvio 6. Turvallisuuden osa-alueet, 2 keskeisintä.

Suomen Elinkeinokeskuksen -kuvasta (Kuvio 4) haastateltavia pyydettiin myös mainitsemaan kaksi vähiten huomiota saavaa turvallisuuden osa-aluetta. Neljän haastateltavan mukaan ulkomaantoimintojen turvallisuus on kahden vähiten huomiota saavan osa-alueen joukossa (Kuvio 7). Haastateltavien yrityksistä yhdellä oli toimipiste ulkomailla. Viidessä yrityksessä mainittiin tehtävän ulkomaille suuntautuvia työmatkoja.

Rikosturvallisuuden nähtiin kolmessa haastattelussa olevan myös kahden vähiten huomiota saavan turvallisuuden osa-alueen joukossa, mietittäessä haastateltavan yrityksen painotusalueita. Haastateltavan 3 mukaan heidän yrityksessään pyritään vähentämään rikoksen mahdollisuutta sillä, että rikollisuutta houkuttelevat asiat pyritään pitämään minimissä. Hälytys- ja rikosilmoitinjärjestelmien käyttö nähtiin rikosturvallisuutta lisääväksi asiaksi vähintään kahden haastateltavan mielestä ja kaikissa haastateltavissa yrityksissä käytettiin yksityisiä turvallisuuspalveluja. Kahdessa haastattelussa todettiin, ettei yrityksessä ole ilmennyt vakavia rikoksia. Rikosturvallisuuden katsoivat kaksi haastateltavaa liittyvän kiinteistö- ja toimitilaturvallisuuteen, ja sen katsottiin olevan myös tietoturvallisuuden yksi osa.

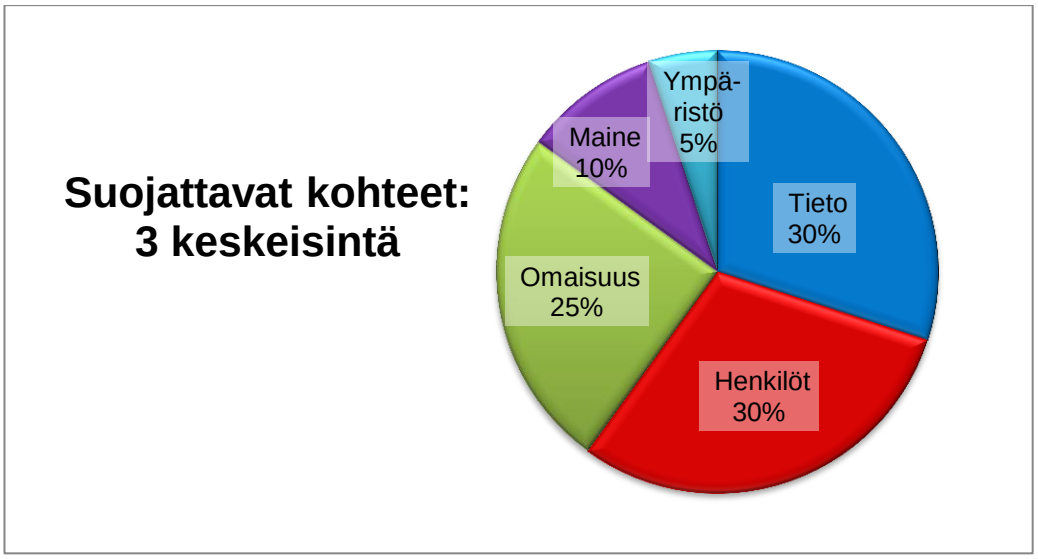
Valmiussuunnittelu (esim. sähkönsaanti), pelastustoiminta, perinteinen henkilöturvallisuus ja ympäristöturvallisuus nähtiin myös turvallisuuden osa-alueina, jotka saavat vähiten huomiota. Yhdessä yrityksessä ei pohdittu kuin yhtä turvallisuuden osa-aluetta, joten sieltä ei saatu vastauksia tähän kohtaan. Myös yhdessä yrityksessä ei mainittu kuin yksi vähiten huomiota saava turvallisuuden osa-alue.



Kuvio 7. Turvallisuuden osa-alueet, 2 vähiten keskeistä.

Haastateltavia pyydettiin myös valitsemaan kolme tärkeintä suojattavaa kohdetta yrityksessään Suomen Elinkeinokeskuksen kuvan keskellä olevista, tyypillisimmistä suojattavista kohteista. Suojeltavien asioiden joukossa olivat tieto, henkilöt, omaisuus, maine ja ympäristö. Tieto nähtiin kuudessa yrityksessä kolmen tärkeimmän suojattavan asian joukossa, samoin kuin henkilöidenkin suojaaminen (Kuvio 8).

Perusteluja valinnoille olivat esimerkiksi, kuinka vaikeaa jotain tiettyä suojeltavaa kohdetta olisi korvata, mihin kohteisiin pääoma on yrityksessä sidottu ja myös minkä vahingoittuminen vaikuttaisi eniten yritykseen maineeseen. Yhdessä haastattelussa mainittiin vain kaksi suojeltavaa kohdetta. Haastateltava 6 myös painotti, että kaikki suojattavat kohteet ovat tärkeitä, mutta sanoi kuitenkin oman mielipiteensä kolmesta tärkeimmästä suojattavasta kohteesta.



Kuvio 8. Suojattavat kohteet, 3 keskeisintä.

5.2.2 Yritysturvallisuuden osa-alueet ja niiden vastuutus

Turvallisuuden osa-alueista kokonaisvastuussa oli viiden haastateltavan mukaan toimitusjohtaja tai vastaavassa asemassa oleva henkilö. Konsernin johdon mainittiin olevan kokonaisvastuussa turvallisuuden osa-alueista yhdessä haastattelussa. Tiedettiin siis hyvin, kuka turvallisuuden osa-alueista on yrityksissä viime kädessä vastuussa.

Osa-alueiden vastaavien yksilöinti osoittautui kuitenkin PK-yrityksien kokoluokassa hankalaksi. Tyypillistä oli, että yksi henkilö vastaa useista eri osa-alueista tai jotkut osa-alueet on jätetty huomiotta. Perusteluja joidenkin osa-alueiden huomiotta jättämiselle olivat muun muassa, ettei joidenkin turvallisuuden osa-alueiden huomiointi ole heidän toiminnassaan, toimialallaan tai yrityskokoluokassaan olennaista. Tyypillistä PK-yritysten kokoluokassa oli myös se, että turvallisuusasioiden vastuut olivat oman pääasiallisen työn ohella hoidettavia, ns. ”OTO -luonteisia”.

Yksityisiä turvallisuuspalveluja käyttivät kaikki haastateltavien yritykset, esimerkiksi rikosturvallisuuden, kiinteistö- ja toimitilaturvallisuuden sekä tietoturvallisuuden hoitamiseen. Yhdessä yrityksessä oli käytetty myös pelastustoiminnan asiantuntijapalveluita. Lisäksi useissa haastateltavien yrityksissä oli käytössä laatujärjestelmiä, joiden käyttö vaatii tietyntasoista turvallisuutta joidenkin asioiden suhteen.

Pelastustoimintaa ja kiinteistö- ja toimitilaturvallisuutta kuvasivat kaikki haastateltavat, niistä tiedettiin parhaiten kertoa. Melkein kaikki osasivat kuvata ja nimetä vastuualueet myös työturvallisuudesta, tietoturvallisuudesta ja rikosturvallisuudesta.

Heikoiten pystyttiin kuvaamaan ulkomaantoimintojen-, ja henkilöturvallisuutta sekä valmiussuunnittelua, osa ei oikein edes yhtäkkiseltään tiennyt mitä niillä oikein tarkoitetaan. Valmiussuunnittelun kaltainen toiminta liitettiin joissain kohti pelastustoimintaan ja henkilöturvallisuus työturvallisuuteen. Ulkomaantoimintoja ja niiden turvallisuutta ei kuudessa yrityksessä mietitty, koska heillä ei ole toimipisteitä ulkomailla. Kuitenkin viidessä yrityksessä tehtiin ulkomaille suuntautuvia työmatkoja.

5.2.3 Ulkoistaen vai yrityksen sisäisesti?

Haastateltavilta kysyttiin myös ajatuksia siitä, minkä tyyppiset turvallisuuteen liittyvät asiat on lähdettävä organisaatiosta itsestään ja mitä voisi ajatella ulkoistettavan. Suurin osa, viisi haastateltavaa, näkee järkevänä kiinteistö- ja toimitilaturvallisuuden sekä rikosturvallisuuden ulkoistamisen yksityisen turvallisuusalan vartiointipalvelujen kautta. Toimijoita on haastateltavien mukaan paljon ja ne on helppo kilpailuttaa, heidän mielestään niitä kannattaa siis hyödyntää. Tietoturvallisuudesta oltiin myös sitä mieltä, viidessä haastattelussa, että sen ulkoistaminen on järkevää, jos organisaatiossa ei kyseen omaiseen asiaan ole asiantuntijatason osaamista.

Pelastustoimintaan todettiin voivan hakea tukea ulkoisilta viranomaisilta. Ulkomaantoimintojen ulkoistamista pohdittiin myös yhdessä haastattelussa ja tiedettiin jo valmius- ja tukiorganisaatioiden olemassaolosta, jos jotain ulkomailla sattuu. Haastateltavan 1 mielestä kaikki muut turvallisuuden osa-alueet pystyy ulkoistamaan paitsi tuotannon ja toiminnan turvallisuuden, sekä työ- ja ympäristöturvallisuuden. Haastateltava 7 toteaa, että pääsääntöisesti kaikki sellaiset turvallisuusasiat, joista ei organisaatiossa ole riittävästi osaamista tulisi hoitaa ulkoapäin. Haastattelussa 3 myös todettiin, että: ” juuri asiantuntijatoimenpiteitä vaativat asiat eli laitteiden suojaus, lukitukset ja erilaiset auditoinnit kannattaa yleensä hankkia ulkoapäin”.

Neljässä haastattelussa kuitenkin todettiin, ettei työturvallisuutta oikein pysty ulkoapäin hankkimaan, sillä se riippuu jokaisesta työntekijästä itsestäänkin. Pelastustoiminnasta kerrottiin myös neljässä haastattelussa, että siihen voi hakea tukea ulkoisilta tahoilta, mutta se on osaltaan myös yrityksen sisältäpäin tuleva asia. Tuotannon ja toiminnanturvallisuuden ulkoistamista ei pitänyt järkevänä kaksi haastateltavaa. Kahdessa haastattelussa mainittiin, ettei tosiaan ihan kaikkea voi ulkoistaa, muttei jokaiseen asiaan toisaalta kannata itsekään sekaantua. Myös henkilöturvallisuudesta ja tietoturvallisuudesta kerrottiin, että nekin ovat tietyiltä osin sisältäpäin tulevia asioita.

Yrityskulttuurin totesi Haastateltava 7 myös liittyvän siihen, miten hyvin mikä tahansa turvallisuuteen liittyvä asia toimii. Haastateltava 3 painotti myös sitä, että työntekijöiden tahtotilaan ja asenteisiin vaikuttamalla voidaan ehkäistä joidenkin turvallisuusuhkien toteutuminen. Ulkoistettavien palvelujen määritteleminen ja koordinoiminen tulisi myös lähteä yrityksen sisältä Haastateltavan 5 mukaan, jotta tiedetään, mitä osaamista hankitaan, mikä on mahdollista ja mikä ehkä ei.

5.3 Turvallisuusasioiden hallintaan liittyvät tarpeet

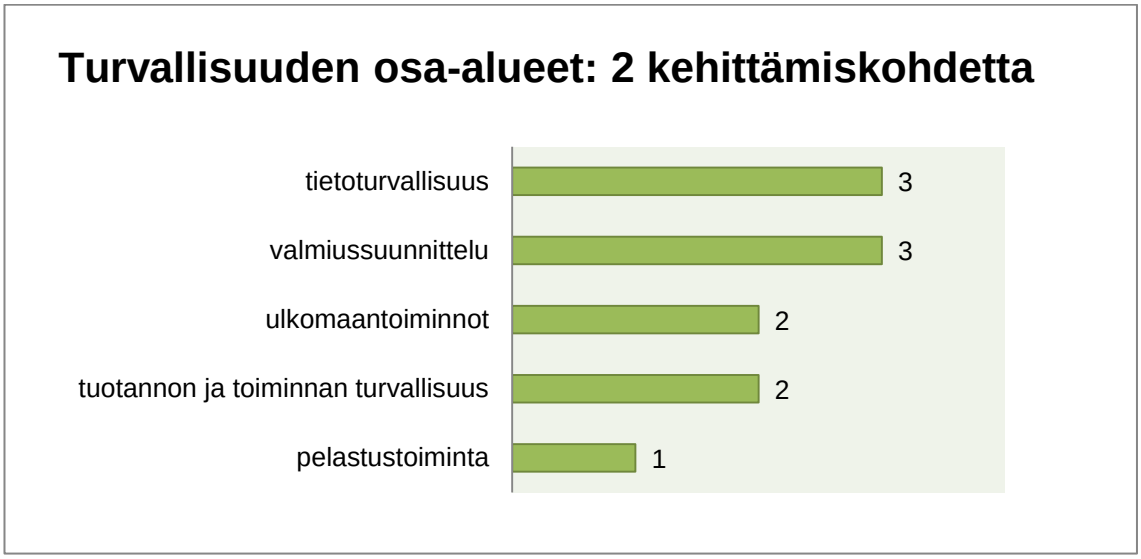
5.3.1 Kehittämiskohteet yritysturvallisuuden osa-alueista

Haastateltavia pyydettiin myös arvioimaan, mitkä Suomen Elinkeinokeskuksen kuvassa olevista turvallisuuden osa-alueista (Kuva 4) voisivat olla kaksi kehittämiskohdetta. Kolme haastateltavaa oli sitä mieltä, että tulevaisuudessa kehittämiskohteina voisivat olla tietoturvallisuus ja valmiussuunnittelu (uhkat, riskit, henkilöt) (Kuvio 9). Valmiussuunnittelun nähtiin tietoturvallisuuden ohella olevan asioita, joissa yritys ei voi koskaan tulla valmiiksi

Toiseksi suurimpana kehittämiskohteena kaksi haastateltavaa piti ulkomaantoimintojen turvallisuutta. Kaksi haastateltavista näki myös kehittämiskohteena tuotannon ja toiminnan turvallisuuden. Myös pelastustoiminnan todettiin olevan kehittämiskohteena yhdessä yrityksessä. Yhden haastateltavan mukaan kaikki turvalli-

suuden osa-alueet ovat kehittämiskohteita, niiden painoalueet vain kuulemma muuttuvat.

Haastateltava 7 näki kaikki turvallisuuden osa-alueet kehittämiskohteiksi, sillä maailma ei tule koskaan valmiiksi ja kaikissa riittää aina hiomista, mikään ei ole kuulemma niin pysyvää kuin muutos. Haastateltavalta 7 ei siis tähän kohtaan tullut tarkempia vastauksia. Yksi haastateltava mainitsi vain yhden kehittämiskohteen turvallisuuden osa-alueista.



Kuvio 9. Turvallisuuden osa-alueet, 2 kehittämiskohdetta.

5.3.2 PK-yrityksien ja suurien yrityksien tarpeiden erot

Osiossa kaksi kysyttiin haastateltavilta mielipidettä Elinkeinokeskuksen yritysturvallisuuden osa-alueita käsittelevästä kuvasta, sen selkeydestä ja hyödynnettävyydestä nimenomaan pienten ja keskisuurten yritysten näkökulmasta. Tarkoitus oli sillä tavoin selvittää, pienten ja keskisuurten yritysten turvallisuuden tarpeiden ja mahdollisten ongelmakohtien erilaisuutta, verrattaessa suuriin yrityksiin. Kyseessä ei siis ole kuvan arvostelu sinänsä, vaan sen kartoitus, eroavatko turvallisuuden tarpeet kahdessa eri kokoluokassa, suurissa yrityksissä ja PK-yrityksissä.

Kaiken kaikkiaan viiden haastateltavan mukaan kuvassa käsiteltävät asiat olivat kokonaisuutena hyvä, selkeä, siinä oli paljon asiaa, tyhjentävä, ymmärrettävä ja hyödynnettävä. Yksi haastateltava kuitenkin totesi, että: ”Siinä ammutaan yli PK-

yritysten näkökulmasta, ei välttämättä ole kovin hyödyllinen ja selkeä, koska vaatisi määrätyn kokoluokan toimiakseen”. Kolmessa haastattelussa myös todettiin, että PK-yrittäjät eivät välttämättä tunnista eri osa-alueita, he ajattelevat ne eri tavalla tai eivät pysty mieltämään niitä konkreettisesti omaan toimintaansa Haastateltava 1 mietti myös, että olisi järkevää miettiä ennemminkin, mikä milloinkin on olennaista ja asettamalla turvallisuuden osa-alueita tärkeysjärjestykseen.

Haastateltavan 5 mukaan turvallisuuden osa-alueissa myös monet asiat limittyvät liikaa toisiinsa ja silloin rajapinnat häilyvät, jolloin se ei välttämättä ole hyvä asia. Haastateltava 7 myös ideoi, että osa-alueista saisi vähemmän yksilöityjä, yhdistämällä osa-alueet 4-5 osa-alueeseen ja kuvaamalla niitä eri tavoin. Haastateltava 3 totesi, että kuvan mukaisessa kokonaisuudessa on niin paljon asiaa, että se ei herätä kiinnostusta PK-yrittäjän näkökulmasta ajateltuna.

Kahdessa yrityskokoluokassa, suurissa yrityksissä ja PK-yritysten kokoluokassa, oli siis haastateltavien mielestä eroavaisuutta suhteessa kuvan turvallisuuden osa-alueisiin ja suojattaviin kohteisiin. Se, miten eri turvallisuuden osa-alueet jakaantuvat eri vastuualueille ja mitä turvallisuuden osa-alueita painotetaan, vaikuttaa haastateltavien mukaan juuri yrityksen toimiala, toiminnan luonne ja yrityksen kokoluokka.

5.3.3 PK-yritysten turvallisuusasioiden hallinnan tarpeet

Keskeisenä ongelmakohtana PK-yrityksissä näki kolme haastateltavaa juuri henkilöstön määrän vähäisyyden jolloin esimerkiksi yhden henkilön poissaolo voi vaikuttaa liian paljon yrityksen toimintaan. Myös isoissa yrityksissä todettiin olevan haavoittuvuutta avainhenkilöiden suhteen. Varsinkin pienemmissä yrityksissä kerrottiin tavallaan jokaisen työntekijän olevan avainhenkilö, jolloin henkilöstöriskit korostuvat. Henkilöriskeistä Haastateltava 1 toteaa, että niitä voidaan vähentää henkilöstösuunnittelulla ja ennakoimalla ja jatkaakin osuvasti: ”..Kaikissa yrityksissä sitä ei vain ajatella etukäteen ja siksi hautausmaat ovat täynnä korvaamattomia työntekijöitä”.

Syventymisen tason, yritysturvallisuuteen liittyvissä asioissa, kerrottiin olevan myös suuria yrityksiä heikompaa PK-yrityksissä. Yritysturvallisuusasioiden toimintojen todettiin myös olevan suppeampia. Suurissa yrityksissä voidaan asettaa jokaiselle turvallisuuden osa-alueelle oma vastuuhenkilönsä tai yksi, joka vastaa päätoimisesti turvallisuuteen liittyvistä asioista yrityksessä. PK-yrityksissä vain yhdellä henkilöllä voi olla vain 20 % työajasta käytettävänään turvallisuusasioihin, haastateltavat kertovat.

Kyse on siis resurssien erilaisuudesta ja siitä seuraa kuulemma se, että yhden ihmisen pitää PK-yrityksessä tietää todella paljon yritysturvallisuudesta tai sitten turvallisuusasioista osa on jätetty huomiotta. Haastateltava 6 toteaa, että silloin ei yleensä paljon ole haavoittuvuuttakaan tai jos on, se on koettu hallituksi riskiksi.

Tiedon laatu ja saatavuus nousee haastateltavien mukaan kysymysmerkiksi, kun yhden ihmisen pitäisi hallita yritysturvallisuus kokonaisuudessaan, oman työnsä ohessa. Haastateltava 1 toteaa, ettei sellaista yksinkertaista kokonaispakettia ole saatavilla PK-yrittäjien tarpeisiin. Yrityksen toiminnan luonne, toimiala ja koko siis vaikuttavat haastatteluiden mukaan siihen, minkälainen tärkeysjärjestys on yritysturvallisuuden eri osa-alueiden kesken. Haastateltava 6 myös totesi osuvasti, että: ”On myös selvää, että joku osa-alue jää vähemmälle huomiolle ja niihin ne turvallisuusasiat sitten kulminoituvat”.

Ongelma on, Haastateltavan 7 mukaan se, että jo pelkästään yritysturvallisuuden lakisääteiset velvollisuudet, jotka ovat kaikille kokoluokille samat (lukuun ottamatta YT-lakia), ja niiden hoitaminen vie usein kaikki voimavarat PK-yrityksiltä. Haastateltava 7 myös pohti, että isommilla yrityksillä on palkkalistoillaan yleensä lakimies, eikä siellä tarvitse pelätä niin paljon viranomaistarkastuksia kuin PK-yrityksissä. Suomessa myös annetaan etumatkaa turvallisuusasioissa, sillä täällä niitä noudatetaan ihan eri tavalla kuin ulkomaisissa kilpailevissa yrityksissä.

Turvallisuuden kokonaisuuden hallinnan Haastateltava 3 toteaa olevan helpompaa pienemmissä yrityskokoluokissa. Tyypillisimpiä riskejä todettiin alkavan myös realisoitua enemmän, yrityksen kasvattaessa kokoluokkaansa ja niiden käsittely automatisoituu. Haastateltava 5 kertoo, että PK-yrityksissä päätöksenteko ja reagointi ovat yleensä kuitenkin ketterämpiä ja nopeampia kuin suurissa yrityksissä. ”Suu-

rissa yrityksissä on voitu tiedostaa joku ongelma ja tehty useita aloitteitakin, mutta silti päätöksenteko on voinut jäädä vaiheeseen", kertoo Haastateltava 5.

Haastateltavat 2 ja 5 toivat esille älypuhelinten käyttöön liittyviä tietoturvallisuusasioita ja -tarpeita. Haastateltava 5 totesi mm. "Älypuhelinten olevan kehittymättömiä tiedon ylläpidon suhteen ja käyttäjät ovat valveutumattomia" ja totesi lukeneensa niihin liittyvien hakkerointien ja haittaohjelmien lisääntymisestä. Myös muistitikkujen Haastateltava 3 kertoo olevan sinänsä riski, koska niistä ei kuulemma oikein pidetä lukua ja ne häviävät jopa huomaamatta, yrityksen kokoluokasta riippumatta.

5.3.4 PK-yritykset ja turvallisuusala

Lopuksi haastateltavia pyydettiin ideoimaan, miten PK-yritysten tarpeisiin voitaisiin turva-alalla paremmin vastata. Eniten haastateltavat kaipasivat kokonaisvaltaisia palvelupaketteja ja -palveluita yritysturvallisuudesta. Yhteensä kolmessa haastattelussa tuli esille koottujen turvapalveluiden tarve. Haastateltavien mukaan se helpottaisi PK-yritysten kokonaisuuden hallintaa yritysturvallisuudessa, palveluiden saatavuus olisi helpompaa ja kustannukset pienentyisivät asiakastasolla. Haastatteluissa ideoitiin, että turva-alan yritysten pitäisi verkostoitua paremmin, erilaistaa tarjontaansa ja kenties tehdä työyhteenliittymiä. Lisäksi näin haastatteluissa todettiin asiakaskohtaisesti räätälöityjen turvapalveluiden tarjoamisen helpottuvan PK-yrityksille.

Valmiiden, kokonaisten tietopakettien tarve on myös selkeä PK-yrityksillä, kolmen haastateltavan mukaan. Tietopaketteihin ideoitiin voivan sisältyä mm. tietoa suunnittelusta ja turvallisuuden hoitamisesta sekä erilaisia suunnitelmarunkoja ja tarkistuslistoja. Tietopaketteihin ideoitiin sisältyvän myös koulutuksellisia asioita ja tietoa yksinkertaisista konkreettisista turvallisuuskäytänteistä.

Haastateltavien 1 ja 2 mukaan tiedostavuutta lisäävien koulutuksien järjestämiselle yritysturvallisuusasioista olisi tarvetta PK-yrityksissä. Koulutusten pitäisi olla mahdollisimman käytännönläheisiä, tekemällä oppimista, Case-esimerkkejä ja ratkaisujen ideointia, helposti ymmärrettävää ja sovellettavaa. Keskusteleva luentomai-

suus nähtiin myös hyväksi ja alueellisten turvapalvelujen listaaminen, sekä niiden tarjonnasta kertominen. Näin ei haastateltavien mukaan tarvitsisi käyttää monta päivää tiedon etsintään ja seulomiseen, vaan saisi esimerkiksi yhden päivän aikana paljon käyttökelpoista tietoa turvallisuuden suunnitteluun.

Haastatteluissa todettiin myös, että tietoa yritysturvallisuudesta on, jos sitä tietää kaivata (Haastateltava 3). Tietoisuutta pitäisi siis lisätä yritysturvallisuuteen liittyen, varsinkin PK-yrityksissä, joissa resurssit ovat rajalliset. Pitäisi pystyä perustelemaan säästö ja hyöty, sekä kenties luoda joku euromääräinen järjestelmä, joka mittaa tiettyjen toimenpiteiden vaikutuksia yrityksen kannattavuuteen. Pitäisi siis Haastateltavan 6 mukaan parantaa vuorovaikutusta PK-yritysten ja turva-alan välillä.

Haastateltavan 7 mielestä tarve selkeästi ohjaavalle toiminnalle yritysturvallisuusasioissa on ilmeinen, koska viranomaisilla ei hänen mukaansa siihen ole aikaa. Hän miettii, mikseivät vakuutusyhtiöt järjestä ohjaavaa toimintaa, joka vähentäisi niitä realisoituneita riskejä yrityksissä. Pelastusviranomaisillakaan ei hänen mukaansa ole resursseja järjestää ohjaavaa toimintaa ja siksi on kuulemma syntynyt yrityksiä, jotka sitä tarjoavat.

6 Johtopäätökset

Tulokset osoittavat selkeästi, että suuriksi luokiteltavien yritysten ja PK-yritysten yritysturvallisuuden hallintaan liittyvät tarpeet eroavat toisistaan huomattavasti. PK-yritykset kaipaavat asiakaslähtöisiä ja kokonaisvaltaisia turvallisuuspalvelumalleja. PK-yrityksille tarjottavien turvallisuusratkaisujen tulee olla helppoja ja edullisia. Tarvitaan myös koottua tietoa yritysturvallisuudesta ja sen ajankohtaisista piirteistä. Yritysturvallisuusasioissa ohjaavalle toiminnalle ja koulutuksille nähtiin olevan selkeää tarvetta PK-yrityksissä. Älypuhelimien tietoturvallisuusasiat koettiin myös ajankohtaiseksi ja niihin liittyvää tietoisuutta tulisi lisätä.

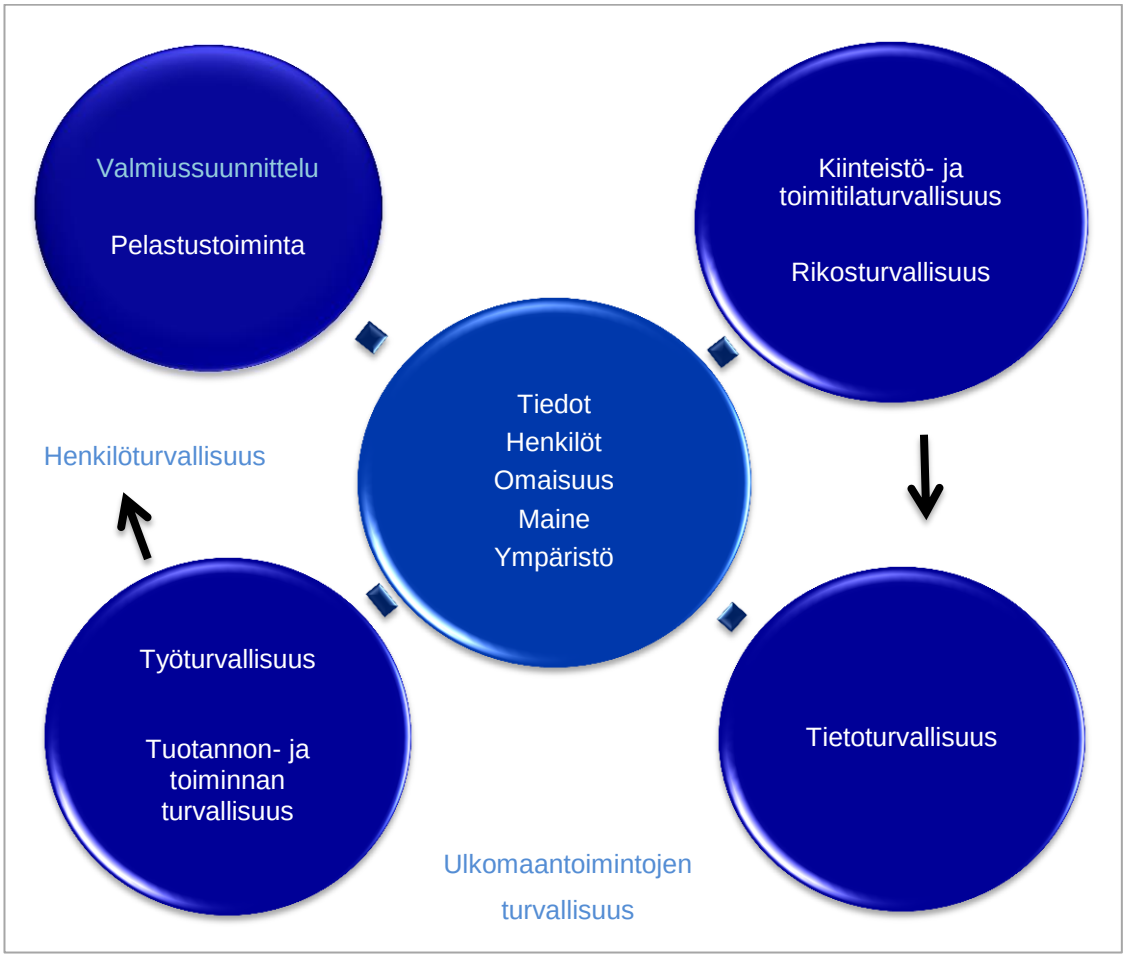
Teemahaastattelujen ensimmäisessä osassa tutkittiin aiheen kannalta keskeisten käsitteiden määrittelyä ja niiden saamia merkityksiä haastattelujen aikana. Kokonaisuudessaan haastateltavilla oli hyvin hallussaan turvallisuuskäsitteistö ja eri käsitteitä haastateltavat osasivat kuvata eri näkökulmista. Kuitenkin eri termien tarkka kuvaaminen osoittautui vaikeaksi ja erottelujen tekeminen eri turvallisuuden osa-alueiden välillä. Tietoturvallisuuteen liittyvien osa-alueiden tunnistaminen ja erottelu ei myöskään ollut kaikissa haastatteluissa kovin kattavaa. Kyberturvallisuudesta ei puhuttu yhdessäkään haastattelussa, mikä on toisaalta käsitteenä vasta 2012 - 2013 vuoden tulokas.

Toisessa teema-alueessa tutkittiin PK-yritysten ja suurien yritysten turvallisuuden hallinnan tarpeiden eroavaisuuksia ja sitä, millä tolalla turvallisuusasiat yrityksissä konkreettisesti ovat. Tulokset osoittivat selkeästi sen, että suuriksi luokiteltavien yritysten ja PK-yritysten turvallisuuden tarpeet eroavat toisistaan huomattavasti. Yritysturvallisuus EK:n (2009) kuvaa käytettiin havaintomateriaalina ja sen avulla kävi hyvin selväksi, että kuvan mukainen jaottelu kymmeneen turvallisuuden osa-alueeseen on kaukana PK-yritysten todellisuudesta.

Kuvan mukainen jaottelu vaatisi haastattelujen mukaan määrätyn kokoluokan toimiakseen. Yritysturvallisuus EK:n kuvasta todettiin kolmessa haastattelussa lisäksi, etteivät PK-yrittäjät välttämättä tunnista eri turvallisuuden osa-alueita, ajattelevat ne eri tavoin tai eivät pysty mieltämään sitä konkreettisesti omaan toimintaan-

sa. Haastatteluissa myös todettiin, että turvallisuuden osa-alueissa monet asiat limittyvät liikaa toisiinsa ja se aiheuttaa rajapintojen häilymistä.

Yritysturvallisuus EK:n (2009) kuviota (s.18) soveltaen, kuviossa 10 on esitetty PK-yritysten käsitys yritysturvallisuuden kokonaisuudesta. Kuviossa on esitetty keskeiset, haastatteluissa esiin tulleet liitännät eri turvallisuuden osa-alueiden välillä. Turvallisuuden osa-alueet, jotka on kuvattu kuviossa sinisellä fontilla, osoittautuvat kaikista hankalimmiksi määritellä ja ne useimmiten poissuljettiin.



Kuvio 10. PK-yritysten käsitys yritysturvallisuuden kokonaisuudesta.

Työturvallisuuden katsottiin kahdessa haastattelussa olevan tuotannon ja toiminnan turvallisuuden kanssa samaa asiaa, lisäksi niiden todettiin vaikuttavan henkilöturvallisuuteen. Kiinteistö- ja toimitilaturvallisuus sekä rikosturvallisuus nähtiin samana turvallisuuden osa-alueena, niiden myös katsottiin vaikuttavan tietoturvallisuuteen. Valmiussuunnittelun ja pelastustoiminnan myös nähtiin liittyvän toisiinsa. Ulkomaantoimintoja ja niiden turvallisuutta ei kuudessa yrityksessä mietitty, koska

heillä ei ollut toimipisteitä ulkomailla. Kuitenkin viidessä yrityksessä tehtiin ulkomaille suuntautuvia työmatkoja. Kaksi haastateltavista näki ulkomaantoimintojen turvallisuuden kehittämiskohteena.

Haastateltavien mukaan tärkeäksi koettiin tiedon, henkilöiden ja omaisuuden suojaaminen. Niitä pyrittiin suojaamaan kiinnittämällä huomiota esimerkiksi tuotannon- ja toiminnan turvallisuuteen, tietoturvallisuuteen ja työturvallisuuteen. Vähiten tärkeäksi koettiin ulkomaantoimintojen turvallisuus ja rikosturvallisuus.

PK-yrityksissä hyvin tyypillistä oli haastattelujen mukaan se, että resurssit ovat rajalliset turvallisuusasioiden hoitamisessa. Turvallisuusasioita hoitavat yrityksen sisällä henkilöt oman pääasiallisen työnsä ohessa, osa-aikaisesti ja monista eri turvallisuusasioiden osa-alueista vastaten. Siitä aiheutuu haastateltavien mukaan se, että syventymisen taso turvallisuusasioissa on heikkoa, turvallisuustoiminnot ovat suppeampia ja joitain osa-alueita joudutaan jättämään huomiotta.

Lainsäädännön vaatimuksien täyttäminen jo pelkästään tuntui vievän kaikki voimavarat PK-yrityksissä, yhdessä haastattelussa todettiin. Haastattelussa kerrottiin, kansainvälisesti olevan suuria eroja turvallisuuslainsäädännön suhteen. Suomessa turvallisuusasioita hoidetaan esimerkiksi ihan eri tavalla, kuin ulkomaisissa kilpailevissa yrityksissä. PK-yritysten turvallisuuden hallintatarpeiden ja turvallisuusalan tarjonnan pitäisi kohdata paremmin tulevaisuudessa haastateltavien mukaan, jotta voitaisiin varmistaa PK-yritysten kilpailukyky kansainvälistyvillä markkinoilla.

PK-yrityksissä koetaan haastattelujen mukaan yrityksen ulkoapäin ostettavien turvallisuuspalveluiden koordinoimisen olevan työlästä. PK-yrittäjä kaipaa helppoja ja edullisia ratkaisuja, koottua tietoa, ohjaavaa toimintaa ja kokonaisvaltaisia turvallisuuspalvelumalleja. Tämä on ymmärrettävää, sillä jo pelkän liiketoiminnan pyörittäminen kannattavasti kyseisessä yrityskokoluokassa on haaste sinänsä. PK-yritysten on vaikea pärjätä kansainvälisillä markkinoilla suuryrityksiä vastaan.

Ohjaavan toiminnan ympärille yritysturvallisuusasioissa on nyt jo muodostunut haastateltavien mukaan sitä tarjoavia yrityksiä. Haastatteluissa ajankohtaiseksi koettiin myös älypuhelimiin liittyvät tietoturvallisuusriskit. Älypuhelimiin on helppo murtautua, jos käyttäjä ei tiedosta niihin liittyviä riskejä (Smart, men farlig 2013).

Kuitenkin esimerkiksi tärkeimpiin turvallisuusalan kasvua ehkäiseviin tekijöihin lukeutuvat Suomen tilastokeskuksen mukaan asiakkaiden hajallaan olevat turvallisuuspalveluhankinnat (2007). Näyttäisi siltä, etteivät PK-yritysten tarpeet ja turvallisuusalan tarjonta kohtaa välttämättä toisiaan tarpeeksi hyvin. Turvallisuuspalveluita pitäisi haastateltavien mukaan muotoilla ja konseptoida paremmin.

Haastatteluissa yhteistyön parantamisen nähtiin olevan tärkeää PK-yritysten ja turva-alan välillä. Haastateltavien mukaan ratkaisuna voisivat esimerkiksi olla työyhteenliittymät turvallisuusalan yrityksien kesken, jolloin kustannukset PK-yrityksille pienentyisivät ja turvallisuuspalveluiden saatavuus helpottuisi. Kenties tämä mahdollistaisi pitkällä tähtäimellä myös kasvuyrittäjyyden edellytyksiä, kun PK-yrityksissä koettaisiin asioiden olevan helpommin hallittavissa ja turvattavissa.

Kolme haastateltavaa oli sitä mieltä, että tulevaisuudessa kehittämiskohteina voisivat olla tietoturvallisuus ja valmiussuunnittelu (uhkat, riskit, henkilöt). Tässä kohtaa valmiussuunnittelu kuitenkin liitettiin enemmän yrityksen riskiarviointien tarkistamiseen ja päivittämiseen, kuin valtion puolustustaloudelliseen suunnitteluun ja varautumiseen poikkeusoloissa. Riskiarviointien päivittämisen ja sen pohjalta tehtävien toimenpiteiden kohdennuksen näki kolme haastateltavaa ajankohtaiseksi kehittämiskohteeksi. Taulukkoon 1 (s.57) on kiteytetty teemahaastattelututkimuksessa esiin tulleet, eniten huomiota ja mainintoja saaneet, yritysturvallisuuden hallintaan liittyvät tarpeet PK-yrityksissä.

PK-yritysten tarpeet yritysturvallisuuden hallinnassa kootusti
Turvallisuuspalvelujen palvelumuotoilu asiakaslähtöisesti
Koordinoinnin helpottaminen ulkoistetuissa turvallisuuspalveluissa
Yhteistyön parantaminen turvallisuusalan ja PK-yritysten välillä
Ohjaava toiminta ja koulutukset henkilöstölle turvallisuusasioissa
Tietoisuuden lisääminen ajankohtaisista turvallisuusriskeistä • ajan tasalla pysyminen, etenkin tietoturvallisuusasioissa
Olemassa olevan turvallisuustiedon luotettavuuden arviointi • tiedon yksinkertaistaminen ja kokoaminen yhteen lähteeseen • toisaalta mahdollisesti ohjaus hyvien lähteiden äärelle
Älypuhelinten ja tablettien käyttöön liittyvät tietoturvallisuushaasteet
Tietoturvallisuus ja turvallisuusanalyysit (esim. riskit, uhkat ja henkilöt)

Taulukko 1. PK-yritysten tarpeet yritysturvallisuuden hallinnassa.

7 Pohdinta

Tässä luvussa pyritään arvioimaan sitä, saavutettiinko opinnäytetyölle asetetut tavoitteet. Tarkasteluun otetaan myös opinnäytetyöprosessi kokonaisuudessaan. Lopuksi arvioidaan myös tutkimustulosten sovellettavuutta ja hyödynnettävyyttä suhteessa opinnäytetyölle asetettuihin tavoitteisiin.

Opinnäytetyölle asetetut tavoitteet saavutettiin. Tulosten perusteella muodostettiin PK-yritysten turvallisuuskäsitteiden ja -tarpeiden profiili, joka oli asetettu tavoitteeksi. Teemahaastattelujen pohjalta muodostettu eteläpohjalaisten PK-yritysten turvallisuuden hallintatarpeet voidaan ottaa osaksi käytännön turvallisuuspalvelujen kehitystyötä. Teoreettisessa viitekehyksessä on myös läpikäyty monipuolisesti yritysturvallisuuden osa-alueita ja merkityksiä. Opinnäytetyön aihe on ajankohtainen ja tärkeä, kuten johdannossa todetaan.

Työprosessina opinnäytetyö oli aiheeltaan ja laajuudeltaan haastava. Tarkoitus oli kerätä nimenomaan kokemuksellista tietoa PK-yrityksistä turvallisuuspalvelujen asiakasryhmänä. Opinnäytetyönä tehdyn teemahaastattelututkimuksen tuloksena on näyte seitsemän, eteläpohjalaisen, PK-yrityksen edustajan näkemyksestä liittyen yritysturvallisuuden hallinnan tarpeisiin ja käsitteisiin.

Haastateltavat olivat pienistä ja keskisuurista yrityksistä, sekä edustivat eri teollisuus- ja palvelualoja, yksityiseltä ja julkiselta sektorilta. Haastateltavien asemat yrityksissä myös vaihtelivat, mikä on hyvä laadullisen tutkimuksen tavoitteiden täyttymisen kannalta, kun pyritään ymmärtämään ja käsitteellistämään tutkimuksen kohteena olevaa asiaa. Varmistuttiin siitä, etteivät tulokset painotu vain johonkin tiettyyn ryhmään ja vältettiin systemaattisen harhan mahdollisuutta. Haastateltavilla oli kokemusta omalta alaltaan ja he olivat olleet yritysturvallisuusasioiden kanssa tekemisissä.

Tutkimustulosten luotettavuus ja uskottavuus ovat siis hyviä, tulokset edustavat kohderyhmää ja todennäköisesti voitaisiin saada samanlaisia tuloksia, toistamalla tutkimus uudelleen kohtuullisessa ajassa. Tutkimuksessa esiin tulleen asiakasryhmän tarpeet eivät todennäköisesti muuttuisi mittakaavaa vaihtamalla, vaan alkaisivat toistaa itseään. Tutkimuksen voidaan sanoa olevan melko kattava läpileik-

kaus PK-yritysten turvallisuuden hallinnan tarpeista ja käsitteistä. Tuloksille asetetut tavoitteet siis saavutettiin, vaikka ajalliset tavoitteet niiden suhteen eivät ihan täyttyneetkään

Teemahaastattelu menetelmänä sopi hyvin aiheeseen, koska sillä oli mahdollista saada tietoa tutkittavasta asiasta. Teema-alueet oli myös muodostettu siten, että aihetta lähestyttiin ensin laajemmin ja sitten kavennettiin pohdintaa yksittäisillä, aiheeseen liittyvillä kysymyksillä. Näin saatiin haastattelut sujuvammaksi ja syvennettyä näkemyksiä niihin olennaisiin, tutkimuksen kannalta kiinnostaviin kohtiin. Haastattelujen analysoinnissa käytettiin aineistolähtöistä sisällönanalyysia, johon sisältyi kokonaiskuvan hahmottaminen kustakin teema-alueesta, aineiston sisältöjen laskeminen ja aineiston kiinnostavat yksityiskohdat. Haastatteluista koottiin keskeiset, tutkimuksen aiheeseen liittyvät näkökulmat, mielipiteet ja tulkinnat yritysturvallisuuden hallintatarpeiden ja käsitteiden profiiliin sekä johtopäätöksiin.

On kuitenkin otettava huomioon, että teemahaastatteluiden määrän pitäisi olla huomattavasti suurempi ja haastattelijoita täytyisi olla enemmän, jos haluttaisiin oikeasti muodostaa absoluuttisen todellisuuden näköinen kuva tutkittavasta asiasta. Samaa aihetta tulisi tutkia eri tutkimusmenetelmillä, jotta voitaisiin varmistua siitä, ettei tutkimusmenetelmä vaikuta tutkimusaiheen tuloksiin. Tässä kohtaa resurssit olivat kuitenkin rajalliset.

Lopuksi kuitenkin on todettava, että vaikka tutkimuksen tuloksia ei sinällään pysty suoraan yleistämään laajemmin tutkimuksen kohderyhmään, tutkimuksen tulokset ovat kuitenkin täyttäneet tarkoituksensa. Kvalitatiivisessa tutkimuksessa on kuitenkin tarkoitus pyrkiä ymmärtämään ja käsitteellistämään tutkittavaa asiaa, ja siinä tässä teemahaastattelututkimuksessa on onnistuttu. Tutkimuksen tuloksia voi toimeksiantaja, Opsec Oy, hyödyntää osana turvallisuuspalvelujen kehitystyötään.

LÄHTEET

Elinkeinoelämän keskusliitto. 2013. Yrittäjyys. [verkko-artikkeli]. [viitattu: 20.8.2013]. Saatavana: http://www.ek.fi/ek/fi/yrittajyys_ym/yrittajyys/tietoa_pk-yrityksista/index.php

Europol. 2013. EU Serious and organised crime threat assessment. [PDF -julkaisu]. [Viitattu: 15.6.2013]. Saatavana: https://www.europol.europa.eu/sites/default/files/publications/socta2013_0.pdf

Cooper. 1998. Improving Safety Culture. A Practical Guide. Chichester: John Wiley & Sons Ltd.

GEM - Finnish 2009 report. 2010. Stenholm, P., Heinonen, J., Kovalainen, A., Pukkinen, T., Turun kauppakorkeakoulu. Sarja A, tutkimusraportteja 2010. . [PDF -julkaisu]. [Viitattu: 15.6.2013]. Saatavana: http://www.gemconsortium.org/docs/download/492

Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Docendo. (Porvoo: WS Bookwell).

Hirsjärvi, S. & Hurme, H. 2008. Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö. Helsinki: Yliopistopaino.

Hirsjärvi, S.; Remes, P. & Sajavaara, P. 2009. Tutki ja kirjoita. 15., uudistettu painos. Helsinki: Tammi.

Hjelt-Putin, P. 2005. Turvallisuutta viestinnällä. Helsinki: Edita.

Hollmèn, J. 2012. Kansallinen yritysturvallisuusstrategia valmistui, tärkeintä on yritysten turvallisuusjohtamisen vahvistaminen. Elinkeinoelämän keskusliitto, yritysturvallisuus. [verkko-artikkeli]. [viitattu: 22.8.2013]. Saatavana: http://www.ek.fi/ek/fi/ajankohtaista/tiedotteet/kansallinen_yritysturvallisuusstrategia_valmistui-9563

Kauppa- ja teollisuusministeriö. 2007. Pk-yritysten tietoturvakysely 2006. [PDF -julkaisu]. Viitattu: 15.3.2013. Saatavana: http://www.ek.fi/ek/fi/yrittajyys_ym/yrittajyys/tietoa_pk-yrityksista/liitteet/Pk-yritystentietoturvakysely.pdf

Keskusrikospoliisi. 2012. Yrityksiin kohdistuvan ja niitä hyödyntävän rikollisuuden tilannekuva. [PDF -julkaisu]. Viitattu: 15.3.2013. Saatavana: http://www.poliisi.fi/poliisi/krp/home.nsf/files/221CFC445A036999C2257AAE0045CB35/$file/Yrityrikollisuuden%20tilannekuva%20syksy%202012.pdf

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

L. 22.4.1999/523. Henkilötietolaki.

L. 13.8.2004/759. Laki yksityisyyden suojasta työelämässä.

L. 29.4.2011/379. Pelastuslaki.

L. 11.6.1999/731. Suomen perustuslaki.

L. 16.6.2004/516. Sähköisen viestinnän tietosuojalaki.

L. 23.8.2002/738. Työturvallisuuslaki.

L. 7.6.1946/436. Työehtosopimuslaki.

L. 9.12.2011/1552. Valmiuslaki.

Leppänen, J. 2006. Yritysturvallisuus käytännössä. Helsinki: Talentum, 2006 (Jyväskylä: Gummerus Kirjapaino).

Maanpuolustuskorkeakoulu. 2013. 9.1 Kyberturvallisuuden kehittäminen osana yhteiskunnan kokonaisturvallisuutta. Tiivistelmä. [verkko-artikkeli]. [viitattu: 17.9.2013]. Saatavana: http://www.puolustusvoimat.fi/wcm/Erikoissivustot/kokonaisturvallisuus/Suomeksi/9/9.1/

Maslow, A. 1987. Motivation and personality. 3. Painos. New York: Harper & Row Publishers, Inc.

Miettinen, J. & Kauppakaari. 2002. Yritysturvallisuuden käsikirja. Helsinki: Kauppakaari, 2002 (Jyväskylä: Gummerus)

Mueller, R. 2013. RSA Cyber Security Conference. Puhe. Viitattu 25.8.2013. Saatavana: http://www.fbi.gov/news/speeches/working-together-to-defeat-cyber-threats

Mäkinen, K. 2007. Organisaation strateginen kokonaisturvallisuus. Helsinki: Edita.

Opsec Oy. 2013. [www-sivut]. [viitattu: 20.8.2013]. Saatavana: http://www.opsec.fi/index.html

Otala, L. 2008. Osaamispääoman johtamisesta kilpailuetu. Helsinki: Edita.

PK-yritysten tietoturvakysely 2006. 2007. Kauppa- ja teollisuusministeriö. [PDF-julkaisu]. [viitattu: 15.3.2013]. Saatavana: http://www.ek.fi/ek/fi/yrittajyys_ym/yrittajyys/tietoa_pk-yrityksista/liitteet/Pk-yritystentietoturvakysely.pdf

Puolustusministeriö. 2007. Puolustusministeriön turvallisuustoiminnan strategia. [PDF-julkaisu]. [viitattu: 20.8.2013]. Saatavana: http://www.defmin.fi/files/1093/turvallisuustoiminta-strategia.pdf

Rantala, K. & Virta, S. (toim.). 2006. Tieto - mahdollisuus, uhka vai turva? Espoo: Poliisiammattikorkeakoulu, 2006. Helsinki: Edita Prima.

Routamaa, V. 2012. Yritysten taloudellinen merkitys kuntataloudelle Etelä-Karjalassa. Etelä-karjalan Yrittäjät Ry. Tutkimusraportti. [PDF -julkaisu]. [viitattu: 2.8.2013]. Saatavana: http://www.yrittajat.fi/File/24abeacd-639e-4616-bcac-91998d977e0f/E-Kraportti.pdf

Ruuhilehto, K & Vilppola, K. 2000. Turvallisuuskulttuuri ja turvallisuuden edistäminen yrityksessä. Helsinki: Turvatekniikan keskus.

Ruusuvuori, J. & Nikander, P. & Hyvärinen, M. (toim.). 2010. Haastattelun analyysi. Tampere : Vastapaino, 2010.

Seinäjoen ammattikorkeakoulu. 2013. FramiPro – tekemällä oppimista. [www-sivut]. [viitattu: 20.8.2013]. Saatavana: http://www.seamk.fi/Suomeksi/Koulutus/Opiskelijana-SeAMKissa/FramiPro---tekemalla-oppimista

Simola, A. 2005. Turvallisuuden johtaminen esimiestyönä. Oulun yliopisto. Teknillinen tiedekunta. Väitöskirja.

Sisäasiainministeriö. 2012. Liiketoimintaa turvallisesti. Kansallinen strategia yritystoiminnan turvallisuuden parantamiseksi. Helsinki: Yritysturvallisuuden kansallinen yhteistyöryhmä. [PDF -julkaisu]. [viitattu: 20.8.2013]. Saatavana: http://www.intermin.fi/download/37996_SM_Yritysturvallisuusstrategia_web.pdf

Smart, men farlig. 2013. Spotlight: Avsnitt 18/35. [verkkojulkaisu]. Åbo Akademin viestinnän opiskelijat, 2013: Spotlight på svenska.yle.fi. [viitattu: 6.9.2013]. Saatavana: http://arenan.yle.fi/tv/1989475

Suomisanakirja.fi.2013. Sivistyssanakirja netissä. [www-sivut]. [viitattu: 20.8.2013]. Saatavana: http://www.suomisanakirja.fi/

Tilastokeskus. 2012. Suomen virallinen tilasto (SVT): Yritysrekisterin vuositilasto [verkkojulkaisu]. Helsinki: Tilastokeskus [viitattu: 19.3.2013]. Saatavana: http://tilastokeskus.fi/til/syr/index.html

Tilastokeskus. 2011. Suomen virallinen tilasto (SVT): Palvelualojen toimialakatsaus IV/2011 [verkkojulkaisu]. Helsinki: Tilastokeskus [viitattu: 19.8.2013]. Saatavana: http://www.stat.fi/artikkelit/2012/art_2012-03-22_004.html

Työturvallisuuskeskus. Työsuojelu. [www-sivut]. [viitattu: 20.8.2013]. Saatavana: http://www.tyoturva.fi/

Ulkoasianministeriö. 2013. Matkustustiedotteet. [www-sivut]. [viitattu: 20.8.2013]. Saatavana: http://formin.finland.fi/public/default.aspx?contentid=50463&contentlan=1&culture=fi-FI

Virta, S. Turvallisuuden tutkimus. Tieteenalat ja monitieteellisyyden lähtökohtia. Tampereen yliopisto. [PDF-julkaisu]. Viitattu: 25.8.2013.

Valtiovarainministeriö. Tietoturvallisuuden hallintajärjestelmän arviointisuositus. 2003. [PDF-julkaisu]. [viitattu: 23.8.2013]. Saatavana: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/53808/name.jsp

Valtiovarainministeriö. Toimitilojen tietoturvaohje. 2013. [PDF-julkaisu]. [viitattu: 23.8.2013]. Saatavana: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20130530Toimit/name.jsp

Valtiovarainministeriö. Valtiohallinnon tietoturvasanasto. 2008. [PDF -julkaisu]. [viitattu: 23.8.2013]. Saatavana: https://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20081211Valtio/name.jsp

Valtiovarainministeriö. 2009. Tietoaineistojen turvaluokittelu. [www-sivut]. [viitattu: 23.8.2013]. Saatavana: https://www.vahtiohje.fi/web/guest/275

Valtioneuvoston periaatepäätös 2013. Suomen kyberturvallisuusstrategia ja taustamuistio. Valtioneuvoston periaatepäätös 24.1.2013. . [PDF-julkaisu]. [viitattu: 17.9.2013]. Saatavana: http://www.yhteiskunnanturvallisuus.fi/fi/component/search/?searchword=kyber&ordering=&searchphrase=all

Vilkka, H. 2005. Tutki ja kehitä. Helsinki : Tammi, 2005.

Wiio, O.1994: Johdatus viestintään. Porvoo: Weilin+Göös, 1994.

Yrittäjäsanomat. 2013. Herätkää valtuutetut: Talous lepää PK-yritysten varassa. [verkko-artikkeli]. [viitattu: 20.8.2013]. Saatavana: http://www.yrittajat.fi/fi-FI/uutisarkisto/a/?groupId=fefe50b4-2878-4e00-a3c3-a040462d6561&announcementId=cfe76695-b116-473a-ba18-6d808722d161

Yritysten rikosturvallisuus 2012. Riskit ja niiden hallinta. 2012. Keskuskauppakamari ja Helsingin seudun kauppakamari. [PDF -julkaisu]. [viitattu: 14.1.2013]. Saatavana: http://kauppakamari.fi/wp-content/uploads/2012/01/Yritysten_rikosturvallisuus_2012-.pdf

Yritysturvallisuus EK. 2009. Yritysturvallisuuden osa-alueet. Elinkeinoelämän keskusliitto. [www-dokumentti]. [viitattu: 14.1.2013]. Saatavana: http://www.ek.fi/ek/fi/tyomarkkinat_ym/Yritysturvallisuus/osa-alueet/Osa-alueet.php

Yritysuhritutkimus. 2010. V. Salmi & M. Lehti & Keinänen A.. Kauppa ja teollisuus rikosten kohteena. Vuoden 2010 yritysuhritutkimuksen tuloksia. Helsinki: Oikeuspoliittisen tutkimuslaitoksen tuloksia 254.

LIITTEET

Liite 1 Kutsu tutkimushaastatteluun

Essi Koivula
Liiketalouden Ko. Opiskelija
SeAMK
Puh. 044 528 4221
essi.koivula@seamk.fi

Hyvä yrittäjä

Olen Essi Koivula ja etsin vapaaehtoisia tutkimushaastatteluun PK – yritysten turvallisuuskokemuksista. Kyseessä on Seinäjoen Ammattikorkeakoulun Liiketalouden korkeakoulututkintoon liittyvä opinnäytetyö, johon sisältyy haastattelututkimus. Tarkoitus on tutkia PK – yrittäjien kokemuksia ja käsityksiä liittyen yritysturvallisuuteen ja erityisesti tietoturvallisuuteen.

Haastattelu kestää noin tunnin. Haastattelut tallennetaan Minidisc – nauhurilla, kuten haastattelututkimuksissa hyvin usein on tapana. Haastattelussa esille tulleet asiat raportoidaan tutkimusjulkaisuissa tavalla, jossa tutkittavia tai muita haastattelussa mainittuja yksittäisiä henkilöitä ei voi välittömästi tunnistaa. Haastattelu kirjataan tekstitiedostoksi ja siinä yhteydessä henkilönimet muutetaan peitenimiksi ja haastateltavien nimi- ja osoitetiedot hävitetään. Äänitallenteet tuhotaan, kun haastattelujen kirjaaminen on tarkistettu (mikäli tutkittavat näin toivovat).

Tutkimus suoritetaan Opsec Oy:n toimeksiantona, yhteistyössä Seinäjoen Ammattikorkeakoulun kanssa. Haastattelututkimus on osa Opsec Oy:n turvallisuuspalveluiden kehitystyötä.

Vastaan mielelläni mahdollisiin lisäkysymyksiin. Puhelinnumeroni on 044 528 4221. Toivottavasti palaatte pian asiaan.

Parhain terveisin,

Essi Koivula

Essi Koivula

opsec

Seinäjoen ammattikorkeakoulu
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Liite 2 Kiitoskirje

opsec

Seinäjoen ammattikorkeakoulu
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Hyvä yrittäjä

Kiitos osallistumisestanne tutkimushaastatteluun PK – yritysten turvallisuuskokemuksista. Kyseessä oli Seinäjoen Ammattikorkeakoulun Liiketalouden korkeakoulututkintoon liittyvä opinnäytetyö, johon sisältyi haastattelututkimus. Tarkoitus oli tutkia PK – yrittäjien kokemuksia ja käsityksiä liittyen yritysturvallisuuteen ja erityisesti tietoturvallisuuteen. Haastattelut menivät hyvin ja tutkittavasta asiasta saatiin kattava kuva. Kokemuksena haastattelutilanteet olivat opinnäytetyöntekijälle positiivisia.

Haastattelussa esille tulleet asiat raportoidaan tutkimusjulkaisuissa tavalla, jossa tutkittavia tai muita haastattelussa mainittuja yksittäisiä henkilöitä ei voi välittömästi tunnistaa. Kesän 2013 aikana haastateltaville lähetetään tarkistettavaksi opinnäytetyössä kyseistä organisaatiota käsittelevät kohdat (esim. lainaukset keskusteluista) sähköpostin liitetiedostona. Mikäli niiden kohdalla ilmenee huomautettavaa tai lisäkysymyksiä, tulee niistä ilmoittaa sähköpostissa mainittuun määräaikaan mennessä allekirjoittaneille.

Tutkimus suoritettiin Opsec Oy:n toimeksiantona, yhteistyössä Seinäjoen Ammattikorkeakoulun kanssa. Haastattelututkimus on osa Opsec Oy:n turvallisuuspalveluiden kehitystyötä.

Vastaamme mielellämme mahdollisiin lisäkysymyksiin.

Parhain terveisin,

Jari Latvala

Jari Latvala

Toimitusjohtaja
Opsec Oy
Puh. 020 198 6699
jari.latvala@opsec.fi

Essi Koivula

Essi Koivula

Liiketalouden Ko. Opiskelija
SeAMK
Puh. 044 528 4221
essi.koivula@seamk.fi