Juhani Matilainen

PK-YRITYSTEN KYBERVALMIUS

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2018

TIIVISTELMÄ

Matilainen, Juhani
PK-yritysten kybervalmius
Jyväskylä: Jyväskylän yliopisto, 2018
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja: Makkonen, Pekka

Pienet ja keskisuuret yritykset joutuvat yhä enenemissä määrin kyberhyökkäyksen kohteeksi. PK-yrityksen päätöksenteko keskittyy yrityksen toimitusjohtajalle ja häntä avustaville avainhenkilöille, joiden tietämys ei aina riitä kattamaan yrityksen kyberturvallisuutta. Johtuen pienestä henkilöstömäärästä ja suurista suhteellisista koulutuskustannuksista, PK-yritykset suhtautuvat epäröiden henkilöstön kouluttamiseen kyberturvallisuuden alalla. Kyberturvallisuuden näkökulmasta PK-yritystä uhkaavat useat eri toimijat, joiden motiivit ja toimintatavat vaihtelevat. Yleisimpinä hyökkäystapoina ovat tietojenkalasteluviestit, erilaiset huijausyritykset sekä haittaohjelmat. Pystyäkseen vastaamaan uhkiin, on yrityksen tunnistettava tietoturvapoikkeamat ja suhtauduttava niihin niiden vaatimalla vakavuudella. Yrityksen on tunnistettava sille tärkeät hyödykkeet ja suojattava ne niiden kriittisyyden mukaisesti. Samalla yritykseltä vaaditaan tietoturvallisen työskentelyn mahdollistamiseksi johdon tukea, johdonmukaista tiedottamista sekä jatkuvaa kouluttamista tietoturva-asioissa.

Asiasanat: PK-yritykset, tietohallinto, tietoturva, tietoturvapoikkeama, kyberuhka

ABSTRACT

Matilainen, Juhani
SMEs' cyber preparedness
Jyväskylä: University of Jyväskylä, 2018
Information Systems, Bachelor's Thesis
Supervisor: Makkonen, Pekka

Small and medium-sized enterprises are increasingly targeted by cyberattacks. The main decision-maker of the business is the company's managing director and company's key personnel assisting him, whose might have a limited knowledge about cyber security to cover company's safety. Due to the small number of staff and large relative training costs, small and medium-sized enterprises are hesitant to educate on cyber security. From the cyber security's point of view, small and medium-sized enterprises are threatened by a number of different cyber world actors whose motives and tactics vary. The most common types of attacks are phishing, various types of scamming attacks and different types of malware. In order to respond to threats, the company must identify and address the system vulnerabilities with required seriousness. The most important assets of the company must be identified and protect them in accordance with their criticality. At the same time, support from the management, consistent communication and continuous training in security matters is required to ensure secure way of working.

Keywords: SMEs, data administration, information security, information security incident, cyber threat

KUVIOT

TAULUKOT

SISÄLLYS

1 Johdanto

Pienet ja keskisuuret yritykset ovat Suomessa merkittävä työllistäjä ja niiden osuus koko bruttokansantuotteesta on noin 40% (Yrittäjät, 2017). Yhteiskunnan digitalisaation myötä myös PK-yritykset ovat pakotettuja muokkaaman omaa liiketoimintaansa. Liiketoiminnan muuttuessa yhä riippuvaisemaksi tietotekniikasta ja sen toimivuudesta, on selvää, ettei kyseinen kehitys tule ilman haittavaikutuksia. Kurpjuhnin (2015) mukaan PK-yritykset käyttävät, varastoivat ja tuottavat suuret määrät dataa. Tämä taas herättää kyberrikollisten huomion, sillä PK-yritykset vaikuttavat hyvältä kohteelta (Kurpjuhn, 2015). Samalla kun asiakkaista ja netinkäyttäjistä kerättävän datan määrä lisääntyy, samalla kasvaa myös kyberrikollisten kiinnostus hyökätä dataa keräävä PK-yritystä vastaan. Myös päivittäisten toimintojen tai prosessien häiritseminen on mahdollinen skenaario. Asiaa pahentaa se, että joissain tapauksissa PK-yritys on pakotettu hankkimaan ja ottamaan käyttöön tietotekniikkaa (Nguyen, 2009). Pakotettu tietotekniikan käyttöönotto ei luonnollisestikaan ole paras mahdollinen tilanne tietohallinnon tai tietoturvan kannalta.

Kyberturvallisuutta koskevat tutkimukset ja ohjeistukset on suunnattu lähinnä isoille yrityksille tai yksityishenkilöille. Kumpikaan näistä ei kohtaa PK-yrityksen reaalimaailman kanssa. PK-yrityksien erilainen organisaatiorakenne ja –kulttuuri hidastavat tai jopa estävät isoille yrityksille tarkoitettujen tietoturvastandardien implementoinnin suoraan yritykseen. Tästä syystä PK-yrityksille tarvitaan erilliset ohjeistukset, jotka ottavat huomioon PK-yrityksen erityispiirteet ja tukevat tietohallinnon toteutumista. Tämä tutkielma pyrkii kokoamaan yhteen ja tarkastelemaan PK-yrityksille tarkoitettuja ohjeistuksia ja suosituksia.

Tämän kandidaatin tutkielman tarkoituksena on vastata seuraaviin tutkimuskysymyksiin:

- Mitkä ovat todennäköisemmät kyberuhat, joita PK-yritys voi kohdata?
- Miten PK-yritys voi suojautua kyberhyökkäyksiä vastaan?

Tutkielman tutkimusmetodina on kirjallisuuskatsaus. Tutkielmassa käytetyt lähdemateriaalit on haettu Emerald Insight –palvelusta, Google Scholarista sekä Jyväskylän Yliopiston JYKDOK –tietokannasta. Tällöin hakusanoina käy-

tettiin englannin kielisiä *cyber security, SMEs, information management, data management,* sekä näiden hakusanojen erilaisia yhdistelmiä. Kyberhyökkäysten yleisyyttä mittaavat tutkimukset on haettu Googlesta hakusanoina *SME, cyber breach, cyber threat*, tai näiden yhdistelminä.

Tutkielman toisessa luvussa tarkastellaan PK-yrityksen määritelmää. Samalla tutustutaan PK-yritysten erityispiirteisiin ja eroavaisuuksiin verrattuna suuriin yrityksiin. Samalla tarkistellaan PK-yrityksen tietohallintoa ja tapaa toteuttaa sitä.

Tutkielma kolmas luku omistetaan kyberuhille, kyberhyökkäyksille ja tietoturvapoikkeamille. Luvussa käydään läpi kybermaailmassa olevien kyberuhkien rakennemalli. Mallin tarkoituksena on kartoittaa PK-yritystä uhkaavat hyökkääjät. Tutkielmassa käytetyssä mallissa uhat jaetaan kategorioihin hyökkääjän motiivin perustella. Samalla luvussa käydään läpi PK-yrityksessä mahdollisesti tapahtuvia tietoturvapoikkeamia. Luku päätetään jo toteutuneiden kyberhyökkäysten tarkasteluun. Erityisenä mielenkiinnon kohteena on hyökkäysten esiintyvyys ja hyökkäysten yleisimmät tyypit.

Neljännessä luvussa tutustutaan PK-yrityksille yleisesti tarjottuihin ohjeisiin tietoturvan varmistamiseksi. Luvussa annetaan yleisiä ohjeita tietoturvan toteuttamiseksi sekä toimivan tietoturvaohjeistuksen laatimiseksi. Tämän jälkeen luvussa käydään läpi yritykselle tärkeiden hyödykkeiden määrittely. Määrittelyn tarkoituksena on helpottaa tietoturvan kohdentamista sinne, missä sen tarve on kaikkein kriittisin. Viimeisenä asiana luvussa käsitellään henkilökunnan roolia tietoturvan totuttamisessa sekä kouluttamista tietoturvalliseen työskentelyyn.

2 PK-YRITYKSET

Tässä luvussa avataan PK-yrityksen määritelmää sekä tarkistellaan PK-yrityksien erityispiirteitä organisaation ja tietotekniikan näkökulmasta. Luvussa käsitellään myös PK-yritysten tietohallintoa, sillä onnistunut tietohallinto tukee myös tietoturvan toteutumista.

2.1 Pk-yritysten määritelmä

Pk-yritykset (pienet- ja keskisuuret yritykset) työllistävät Suomessa noin 1,4 miljoonaa henkilöä, tuottivat 58% yritysten kokonaisliikevaihdosta ja niiden osuus bruttokansantuotteesta on runsaat 40% (Yrittäjät, 2017).

Suomessa yrityksen tulee täyttää seuraavat määritelmät, jotta yritys lasketaan Pk-yritykseksi (Tilastokeskus, 2017):

- Henkilöstömäärä enintään 249 henkilöä
- Vuosiliikevaihto enintään 50 miljoonaa euroa tai
- Taseen loppusumma enintään 43 miljoonaa euroa
- Täyttää riippumattomuuden määritelmän

Tilastokeskuksen (2017) mukaan yritys täyttää riippumattomuuden määritelmän, mikäli sen osakkeista tai pääomasta vähintään 75 prosenttia on yrityksen hallussa. Mikäli yritys haluaa luovuttaa kyseistä rajaa enemmän pääomaansa tai osakkeitaan muiden yritysten haltuun, on myös omistavien yritysten täytettävä Pk-yrityksen määritelmä. Muutoin yritystä ei lasketa enää Pk-yritykseksi (Tilastokeskus, 2017).

Pk-yritykset voidaan jakaa keskisuuriin-, pien- ja mikroyrityksiin eri kriteereiden mukaisesti. Aina tämä ei ole tarpeen, mutta esimerkiksi kvantitatiivisissa tutkimuksissa yrityksen koko voi toimia luokitteluna. Taulukossa 1 on esitetty eri yrityskokojen määritelmät.

TAULUKKO 1 Eri yrityskokojen määritelmät

	Suuryritys	Keskisuuri yritys	Pienyritys	Mikroyritys
Henkilöstömäärä	yli 250	50 – 249	10 – 49	1 – 10
Liikevaihto	yli 50 milj. €	50 milj. €	10 milj. €	2 milj. €
Tase	yli 43 milj. €	43 milj. €	10 milj. €	2 milj. €
Riippumattomuus	Ei	Kyllä	Kyllä	Kyllä

Pk-yrityksen määritelmän sisään mahtuu suuri joukko erikokoisia yrityksiä, joiden toiminta hyvin erilaista riippuen toimialasta ja henkilöstön määrästä. Tutkielmassa käytetyssä tilastoissa on huomioitu ne yritykset, joiden henkilöstö määrä on alle 250 henkilöä, jollei toisin ole mainittu.

2.2 PK-yrityksen erityispiirteet

Huomattavampia PK-yritysten ominaisuuksia ovat epämuodollinen yrityskulttuuri sekä tukeutuminen yksilöiden tietotaitoon (Cragg, 2008). Epämuodollisen yrityskulttuurin selittää yrityksen vähäinen henkilöstömäärä, joka nopeuttaa kommunikointia luoden joustavuutta yrityksen toimintaan (Cragg, 2008). Pienestä henkilöstömäärästä seuraa se, että yrityksen työntekijät tuntevat toisensa ja toisten työtehtävät paremmin, joten hoidettavat asiat on helpompaa kohdistaa niitä hoitavalle henkilölle. Tällöin yrityksen sisäinen kommunikointi on pääasiassa epävirallisempaa verrattuna suuriin yrityksiin, joissa suuriempi henkilöstömäärä ja korkeampi hierarkia pakottaa kommunikaation muodollisempaan ja virallisempaan suuntaan. PK-yritykset siis ovat organisaatiorakenteensa takia joustavampia, tieto kulkee yrityksessä nopeammin ja ne reagoivat nopeammin muutoksiin (Cragg, 2008; Ayat, Masrom, Sahibuddin & Sharafi, 2011). Kuitenkin epämuodollinen yrityskulttuuri ja -kommunikaatio saattaa aiheuttaa sen, että henkilökunnan sisäiset riidat saattavat tapahtuessaan haitata merkittävästi organisaation toimintaa (Ayat ym., 2011). Tällöin yrityksen vaihtoehdot, verrattuna suuriin yrityksiin, ovat paljon rajoitetummat.

PK-yrityksissä päätökset tekee yrityksen toimitusjohtaja, joka on usein myös yrityksen omistaja (Bergeron, Croteau, Uwizeyemungu & Raymond, 2015). Täten voidaan sanoa, että toimitusjohtajan rooli yrityksen toimintatapojen ja toimintojen muokkaamisessa, on suuri. Päätöksen teossa toimitusjohtajaa tukevat niin kutsutut "avainhenkilöt" (Bergeron ym., 2015). Avainhenkilöt muodostavat, yhdessä toimitusjohtajan kanssa, yrityksen johtoportaan (Bergeron ym., 2015). Koska henkilöstöä on vähän, yhden työntekijän pitää hallita suuremmpia kokonaisuuksia mitä suuressa yrityksessä työskentelevän henkilön (Cragg, 2008). Tällöin yhdellä työntekijällä saattaa olla yrityksessä useita rooleja, joita hän hoitaa (Ayat ym., 2011). Työntekijän useista rooleista yrityk-

sessä saattaa seurata se, että työntekijä päätyy hoitamaan sellaista tehtävää, johon hänellä ei ole pätevyyttä tai osaamista. Tämä heijastuu myös yrityksen päätöksen tekoon niin toimitusjohtajan kuin avainhenkilöiden osalta, sillä ei ole yllättävää, että yrityksellä on aukkoja tarvittavassa tietämyksessä (Cragg, 2008). Vaikka tämä tiedostettaisiin, saatetaan henkilöstön kouluttamista vierastaa, sillä yrityksessä pelätään sitä, että juuri koulutettu henkilö jättää yrityksen (Cragg, 2008). Tämän lisäksi pienelle yritykselle henkilöstön kouluttamisesta aiheutuneet kulut ovat suuria yrityksiä suhteutettuna suuremmat. (Ayat ym., 2011)

2.3 PK-yrityksen tietohallinto

Devos, Van Landeghem ja Deschoolmeester (2012) argumentoivat, ettei suurille yrityksille tarkoitettuja tapoja toteuttaa tietohallintoaan voida suoraan siirtää PK-yritysten käyttöön. Suurimpana syynä on suurten yritysten ja PK-yritysten erilaiset yrityskulttuurit. Suurien yritysten korkea hierarkkinen organisaatiorakenne ja formaali kommunikaatio eivät sovellu PK-yritysten tarpeisiin. Informaatioteknologian käyttöön ja hallinnointiin tarvitaan yksinkertainen ja epämuodollinen hallintajärjestelmä, joka tukee PK-yrityksen epämuodollista yrityskulttuuria paremmin ottaen yksilön paremmin huomioon (Devos ym., 2012). Tulee myös huomata, että mikäli PK-yrityksen tietohallintoa aletaan toteuttaa suoraan suurille yrityksille tarkoitettujen standardien pohjalta, lisäävät nämä yrityksen byrokratiaa ja sitä kautta haittaavat yrityksen ydintehtävien suorittamista (Ayat ym., 2011).

Yrityksen päätöksenteon keskittyessä toimitusjohtajalle ja avainhenkilöille on näiden osallistumisella ja tuella merkittävä rooli tietohallinnon onnistumisessa (Nfuka & Rusu, 2011). Tietohallintoa toteuttaessa yrityksen johdon tulisi arvioida tarkkaan yrityksen nykyistä ja tulevaa informaatioteknologian käyttöä. Samalla tulee varmistaa, että käyttö vastaa liiketoiminnan tavoitteita (Ayat ym., 2011). PK-yrityksen tietohallinnon toteuttamisen tärkeänä osana on myös johdon kontrolli informaatioteknologian käytöstä. Tällä tarkoitetaan sitä, että johdon tulee valvoa ohjeistusten ja määräysten noudattamista (Ayat ym., 2011).

Johtuen nopeasti muuttuvasta ja kehittyvästä informaatioteknologiasta, yrityksen toimitusjohtajalla ei usein ole tarvittavaa tietoa tai aikaa perehtyä yrityksen tietotekniikka hankintoihin (Devos ym., 2012). O'Reganin, Simsin ja Ghobadianin (2005) mukaan PK-yrityksen rajoitetummat resurssit tekevät niistä suuria yrityksiä alttiimpia ulkoisille vaikutuksille. Tästä syystä PK-yritys ei aina hanki uutta informaatioteknologiaa omasta tahdostaan vaan olosuhteiden pakottamana. Suurin osa PK-yritysten IT-hankinnoista onkin seurausta ulkoisesta ja sisäisestä paineesta (Nguyen, 2009). Mikäli IT-hankinnat tehdään pakon edessä, on ymmärrettävää, ettei johto ole täysin varma millainen ratkaisu olisi yritykselle paras. Uuden teknologian käyttöönottoa haittaa myös yrityksen johdon tietämättömyys teknologian ja yrityksen välisestä suhteesta sekä epävarmuus teknologian tuomista mahdollisuuksista (Nguyen, 2009). Ongelmaksi muodostuu myös se, ettei tietoteknisten ratkaisujen tarjoaja aina ymmärrä PK-

yrityksen tarpeita, joten tuloksena on jotain muuta, mitä yritys todella tarvitsisi (Kurki, 2010). Samalla on myös huomattava, että PK-yritykset ovat usein huonosti informoituja siitä, mitä ominaisuuksia käyttöönotettavassa tietotekniikassa on (Devos ym., 2012). Monesti teknologian käyttöönottoa yritetään ilman yksityiskohtaista suunnitelmaa. Tämä selittää heikon onnistumisprosentin uuden teknologian implementoinnissa (Nguyen, 2009).

PK-yrityksen ottaessa käyttöön uutta teknologiaa on onnistuminen kiinni kolmesta tekijästä: toimitusjohtajan kyvyt, avainhenkilöiden kyvyt ja johtoryhmän yrityksen ulkopuoliset suhteet (Bergeron ym., 2015). Merkittävimpinä esteinä toimivat investointeihin käytettävän rahan määrä sekä henkilöstön puute (Cragg, 2008). Voidaankin siis argumentoida, että jos PK-yrityksellä on puutteelliset tiedot hankkimastaan tietotekniikasta, aukkoja tietämyksessään jo käytössä olevan teknologian suhteen ja heikot mahdollisuudet kouluttaa henkilöstöään, tämä heijastuu myös yrityksen tietoturvaan, tietohallinnon toteuttamiseen ja informaatioteknologian tehokkaaseen käyttöön.

3 KYBERUHAT

Luvussa avataan kyberuhkien ja aiheeseen liittyvien termien käsite. Samalla tarkistellaan erikseen erilaisia kyberuhkia. Lopuksi käydään läpi tietoturvapoikkeamia ja PK-yrityksiä kohtaan tehtyjä, jo toteutuneita kyberhyökkäyksiä.

3.1 Kyberuhkien rakennemalli

Kybermaailmassa toimii erilaisia kyberuhkia, joita voidaan jakaa eri kategorioihin eri kriteereiden mukaisesti. Eri uhkatekijöiden ammattitaito suorittaa hyökkäyksiä vaihtelee, samoin motiivi. Määritellessä erilaisia kyberuhkia tulee myös huomata, etteivät kaikki yritystä uhkaavat kyberuhat tule yrityksen ulkopuolelta. Vastoin yleistä käsitystä, uhat saattavat olla peräisin organisaation sisältä (Heikkilä, Rättyä, Pieksä & Jämsä, 2016). Lehdon ja Neittaamäen (2015, s. 9) mukaan Cavelty (2010) ja Ashenden (2011) jakavat kybermaailman uhkatekijät viiteen eri kategoriaan: kybervandalismi, kyberrikollisuus, kybervakoilu, kyberterroristmi ja kybersodankäynti. Mallissa uhkatekijät erotetaan toisistaan tekijän motiivin perusteella (Cavelty, 2010; Ashenden, 2011).

Kybervandalismi kattaa mallissa vandalismin, hakkeroinnin sekä haktivismin. Järvinen ja Rousku (2017, s. 34) määrittelevät haktivisteiksi sellaiset tieto- ja viestintäteknologiaa hyödyntävät käyttäjät, jotka toimivat omien tarkoitusperiensä edistämiseksi. PK-yritys saattaa myös kohdata kostona tehtyjä kyberhyökkäyksiä. Stewart, Chapple ja Gibson (2015, s. 815-816) kirjoittavat, että kyberhyökkäyksen tekijä voi olla esimerkiksi entinen työntekijä, jonka motiivina on kauna entistä työnantajaansa tai tiettyä yrityksessä työskentelevää henkilöä kohtaan. Kybervandaaleihin lukeutuu myös satunnainen hyökkääjä tai kokeilija, jonka motiivina on mielenkiinto, jännityksen hakeminen, maineen hankkiminen, tai vahingon tuottaminen pelkästään oman onnistumisentunteen kannalta (Stewart ym., 2015, s. 815-816.; Järvinen & Rousku, 2017).

Kyberrikollisen motiivina toimia on taloudellisen hyödyn saavuttaminen (Lehto & Neittaanmäki 2015 s. 11; Järvinen & Rousku, 2017 s. 35). Kyberrikolli-

suus jaetaan Lehdon ja Neittaanmäen (2015, s. 11) mukaan kolmeen eri kategoriaan:

1. Verkossa tapahtuva perinteinen rikollisuus. Esimerkiksi petokset ja väärentäminen.
2. Laittoman materiaalin levittäminen tietoverkkoja käyttäen. Esimerkkeinä rasistinen materiaali ja lapsipornografia.
3. Tietoverkkorikollisuus, jolla tarkoitetaan vain ja ainoastaan tietoverkoissa tapahtuvaa rikollisuutta. Esimerkiksi palvelunestohyökkäys ja tietomurto.

PK-yrityksestä kyberrikolliset etsivät esimerkiksi luottokorttien numeroita, henkilötietoja tai muuta informaatiota, josta voivat hyötyä taloudellisesti. Tulee huomata, ettei taloudellinen hyöty tarkoita aina välttämättä rahaa vaan voi tarkoittaa myös palveluita, joita kyberrikollinen pyrkii saamaan ilmaiseksi (Steward, Chapple, Gibson, 2015, s. 814-815). Järvisen ja Rouskun (2017, s. 35) mielestä tietoturvan tarkoitus on estää se, ettei tietoja, rahaa tai omaisuutta menetetä ulkopuolisille tai niitä varasteta. Kaikki edellä mainitut asiat ovat yrityksen toiminnan jatkuvuuden kannalta elintärkeitä.

Kybervakoilulla tai kybertiedustelulla tarkoitetaan Lehdon ja Neittaanmäen (2015, s. 12) mukaan Internetissä ja tietoverkoissa tapahtuvaa toimintaa, joka tarkoituksena on hankkia toimintaa harjoittavalle organisaatiolle suojauksen alaista informaatiota. Tietoa voidaan kerätä yksityisistä ihmisistä, kilpailijoista, erilaisista ryhmistä tai ryhmittymistä, hallituksista tai vastustajista. Motiivit ovat poliittisia, sotilaallisia tai toiminnalla pyritään saavuttamaan taloudellista etua. (Lehto & Neittaanmäki, 2015, s. 12) Kybervakoilua voi suorittaa esimerkiksi toinen alalla toimiva yritys, joka suorittaa perinteistä teollisuusvakoilua tietoverkkoja hyväksikäyttäen (Stewart ym., 2015, s. 814). Mikäli jokin organisaatio pyrkisi tietoisesti hankkimaan yritykseltä heille kuulumatonta informaatiota, esimerkiksi liikesalaisuuksia, voidaan tämä laskea kybervakoiluksi.

Kyberterrorismi tähtää vahingon tuottamiseen ja pelon lietsontaan tietoverkkoja hyväksikäyttäen (Lehto & Neittaanmäki, 2015, s. 13; Stewart ym., 2015 s. 815). Kyberterroristin kohteena on yleensä yhteiskunnan kriittinen infrastruktuuri mahdollisimman suuren vaikutuksen aikaansaamiseksi (Järvinen & Rousku, 2015, s. 37).

Kybersodankäynnille ei Lehton ja Neittaanmäen (2015, s. 13-14) mukaan ole yhtä, yksiselitteistä määritelmää, mutta yleisesti sitä käytetään kuvaamaan valtion suorittamia toimia kybermaailmassa. Tällöin kyseessä on valtion asevoimat.

3.2 Tietoturvapoikkeamat

Joka ikinen tietoturvapoikkeama organisaatiossa ei välttämättä ole organisaation ulkopuolisen henkilön suorittama kyberhyökkäys. Tietoturvapoikkeamalla (*eng. Information security incident*) tarkoitetaan organisaation tietoturvalinjausten vastaista tilaa tai tapahtumaa, joka vaarantaa tai saattaa vaarantaa organisaati-

on hallussa olevat tiedot tai tuottamat palvelut (Työturvallisuuskeskus, n. d.). Jokainen yrityksessä koettu tietoturvapoikkeama ei kuitenkaan ole kyberhyökkäys. Järvinen ja Rousku (2017, s. 43) ohjeistavat kirjassaan, että tietoturvapoikkeama on usein seurausta inhimillisestä erehdyksestä ja syntynyt täysin vahingossa. Henkilöstöä voidaankin pitää suurimpana tietoturvapoikkeamien aiheuttajana. (Järvinen & Rousku, 2017, s. 43) Stewart ym., (2015, s. 817) kirjoittavat, että suurin syy tietoturvapoikkeaman raportoimatta jättämiseen on, ettei poikkeamaa havaita. Tämän vuoksi poikkeamien havaitsemiseen on organisaatiossa kiinnitettävä huomiota (Stewart ym., 2017.). Organisaatiossa pitää määritellä tietty toimintamalli, jonka mukaan toimitaan tietoturvapoikkeaman ilmaantuessa. Stewart ym. (2017, s. 821 - 824) esittelevät kirjassaan kolmen vaiheen poikkeaman käsittelyn:

Havaitsemisen ja tunnistamisen vaiheessa organisaatiossa havaitaan tietoturvapoikkeama ja siitä ilmoitetaan eteenpäin asiaankuuluvalle taholle. Poikkeaman tunnistamisessa tärkeää on tietää mikä on organisaation tietoverkoissa normaalia toimintaa ja havaita poikkeamat.

Seuraavaksi suoritetaan **vastatoimet ja raportointi**. Tällöin organisaation tietoturvapolitiikkasta tulisi löytyä ohjeistus tilanteen varalle. Vaiheessa suoritetaan tarvittavat toimenpiteet ja raportoidaan poikkeamasta. Yrityksen sopimukset ja lainsäädäntö voivat velvoittaa tietoturvapoikkeamien raportoinnista niitä hoitaville tahoille. Vaiheeseen voi kuulua myös todisteiden kerääminen ja säilyttäminen tilanteesta ja poikkeamasta riippuen.

Viimeisenä vaiheena on **toipuminen ja korjaustoimet**. Vaiheessa korjataan tapahtuman aiheuttamat vahingot. Vaiheeseen voi liittyä esimerkiksi järjestelmän palauttaminen normaalitilaan, vahingoittuneen datan palautus varmuuskopioista ja havaittujen haavoittuvuuksien paikkaaminen. Samalla käydään läpi tietoturvapoikkeamaan johtaneet tapahtumat ja organisaation vastatoimet. Tällä pyritään parantamaan organisaation toimintaa tulevaisuudessa (Stewart ym., 2015, s. 821- 824.).

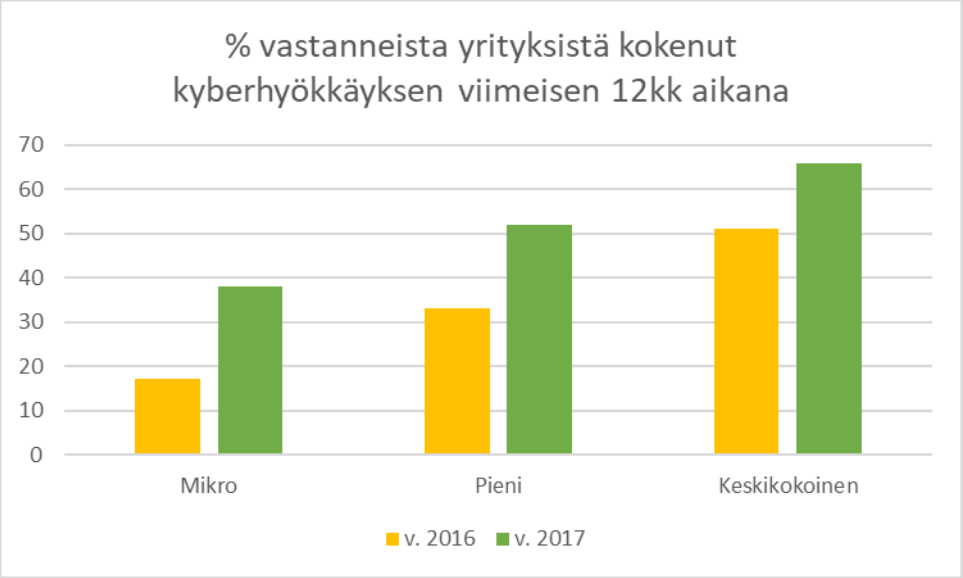
Stewart ym. (2015, s. 817) kirjoittavat, että tietoturvapoikkeamat tullee olla kirjattuna organisaation tietoturvapolitiikkaan. Poikkeamia listatessa huomioidaan organisaation informaatioteknologian käyttö sekä jo tiedossa olevat, mahdolliset poikkeamat. Järvinen ja Rousku (2017, s. 42) listaavat kirjassaan PK-yritykselle yleisiä tietoturvapoikkeamia, joihin tulisi reagoida:

- Päätelaite on varastettu
- Salassa pidettävää tietoa on varastettu tai vuotanut ulkopuolisille
- Käyttäjätunnus ja salasana ovat paljastuneet ulkopuoliselle
- Tietokone ilmoittaa haittaohjelmasta
- Tietoa on menetetty esimerkiksi laiterikon tai ohjelmistovian vuoksi
- Organisaation toimitiloissa liikkuu henkilöitä, joilla ei ole tiloihin kulkuoikeutta
- Salassa pidettävää tietoa päätynyt sellaiselle, jolla ei ole niihin oikeutta
- Organisaatiossa on ilmennyt ohjeistuksen vastaista toimintaa

3.3 Toteutuneet kyberhyökkäykset

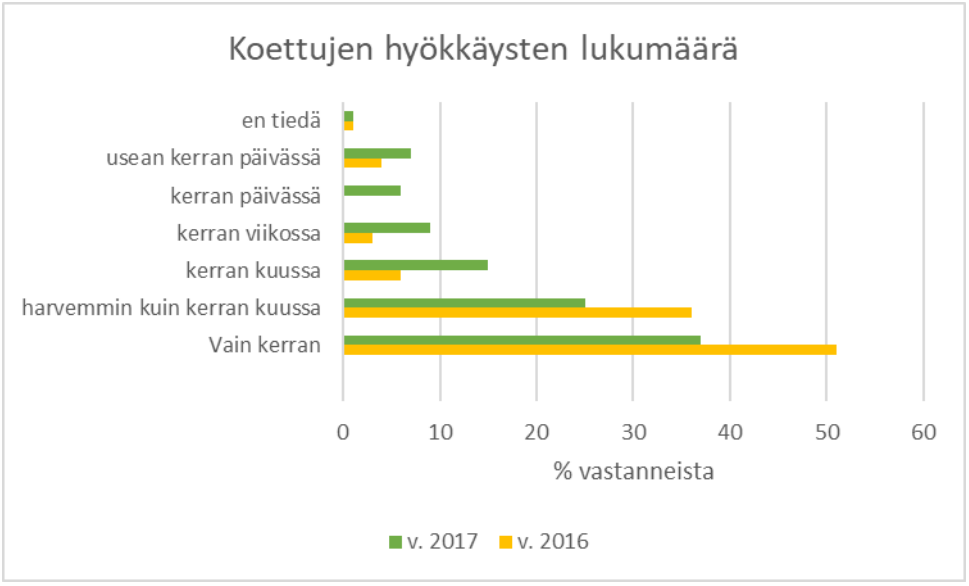
PK-yrityksiin kohdistuneista kyberhyökkäyksistä on tehty muutamia kyselytutkimuksia. Seuraavaksi tarkastellaan PK-yrityksiin kohdistuneita kyberhyökkäyksiä, niiden tyyppiä sekä yrityksen reagoimisaikaa. Pohjana käytetyt tutkimukset ovat peräisin Isosta-Britanniasta vuodelta 2015 – 2017 ja ovat saman instituution tekemiä. Tutkimukset on valittu pohjaksi siksi, että ne tarjoavat jonkinlaisen kuvan kyberhyökkäysten yleisyydestä ja kehittymisestä.

Buttonin ym. (2017) tekemän tutkimuksen mukaan 46% kaikista vastanneista yrityksistä oli kokenut kyberhyökkäyksen viimeisen 12 kuukauden aikana. Kaiken kaikkiaan vastanneita oli yhteensä 1523 yritystä, joista 1348 yritystä lasketaan PK-yritykseksi (Button ym., 2017). Button, Klahr, Amili, Shah ja Wang (2016) kirjoittavat samasta aihepiiristä vuotta aiemmin julkaistussa raportissaan, että hyökkäyksestä raportoi 24% yrityksistä. Tällöin vastanneita yrityksiä oli yhteensä 1008, joista PK-yrityksiä 801 (Button ym., 2016). Vastanneiden PK-yritysten määrät on esitelty kuviossa 1. Tuloksia lukiessa tulee huomata, että vuoden 2017 tutkimuksessa (Button ym., 2017) ilmoittavat, etteivät vuosien 2016 ja 2017 tulokset ole täysin vertailukelpoisia keskenään johtuen tutkimusten kysymysten asettelusta ja muutoksista. Myöskin Ison-Britannian yrityksiä tutkinut organisaatio FSB (2016) raportoi, että 66% pienistä yrityksistä oli ollut kyberrikoksen uhrina viimeisen 12 kuukauden aikana. Tällöin vastanneita yrityksiä oli ollut 1006 kappaletta. Australialaisia PK-yrityksiä tutkinut NSW (2017) taas raportoi, että kyberrikoksen uhriksi joutuneita yrityksiä oli vähemmän kuin 30%. Tällöin vastanneita yrityksiä oli 1086 kappaletta. Vaikka eri tutkimukset antavat eri lukemia PK-yritysksiin kohdistetuista hyökkäyksistä, varmaa on, että kyberhyökkäykset ovat suhteellisen yleisiä myös PK-yrityksissä. Tästä voidaan päätellä, että oletus siitä, etteivät PK-yritykset ole kyberhyökkäysten kohteena, on väärä.



KUVIO 1 Kyberhyökkäyksen kokeneiden yritysten osuus

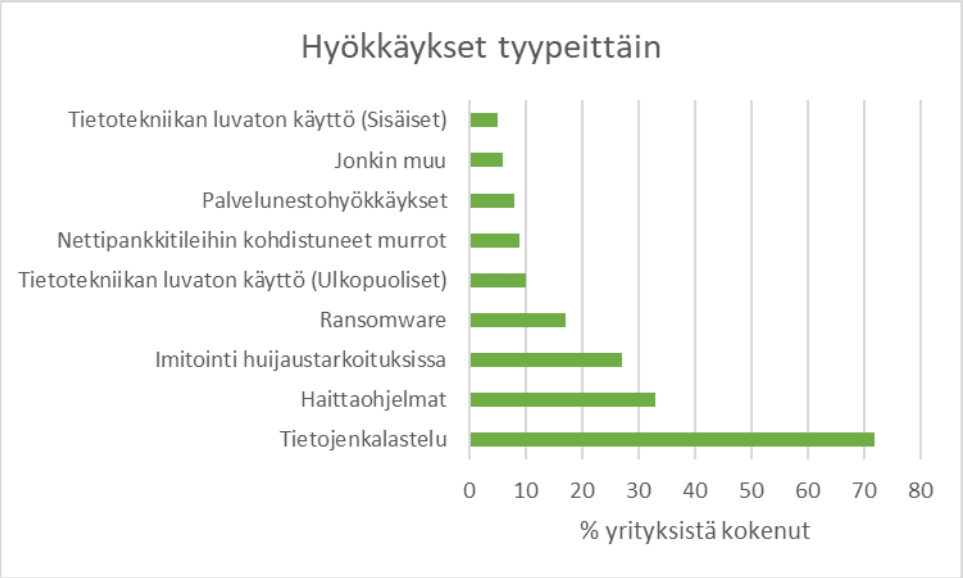
Button ym., (2017) kertovat raportissaan, että kaikista niistä yrityksistä, jotka kokivat vähintään yhden kyberhyökkäyksen viimeisen 12 kuukauden aikana, kyseinen hyökkäys jäi ainoaksi. Kuitenkin pieni vähemmistö yrityksistä on jatkuvasti hyökkäysten kohteena. Hyökkäysten määrä tutkitun 12 kuukauden aikana on eritelty kuviossa 2. Kuviota tarkastellessa tulee muistaa, että kyselytutkimuksessa oli huomioitu kaiken kokoiset yritykset, ei vain PK-yrityksiä. Tulokset ovat saman suuntaisia myös FSBn (2016) raportin kanssa, jonka mukaan yritys joutuu kyberrikoksen uhriksi keskimäärin 4 kertaa kahden vuoden aikana.



KUVIO 2 Koettujen hyökkäysten lukumäärä

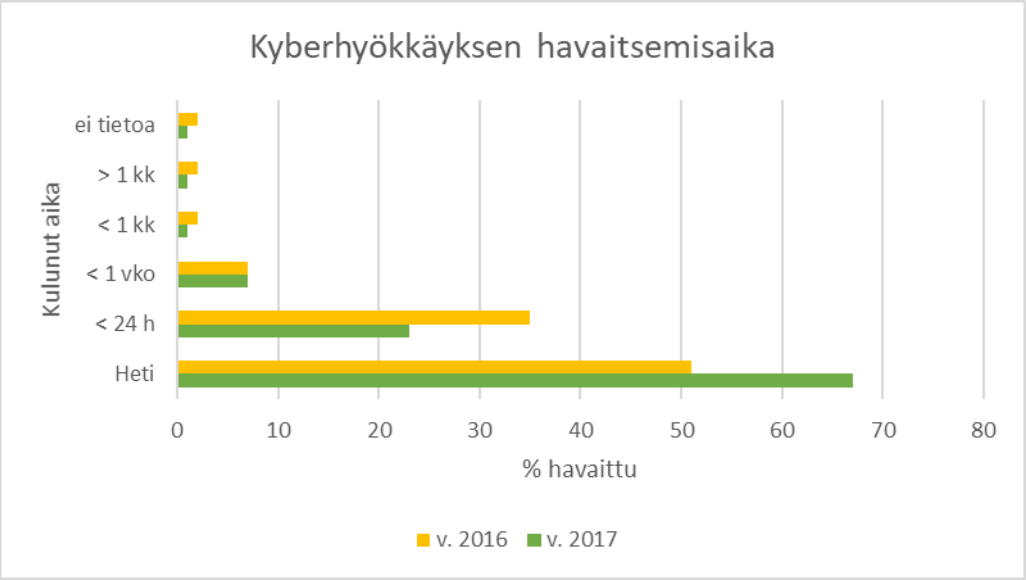
Tutkielmassa käytetyn Button ym., (2017) kyselytutkimuksen mukaan koettujen kyberhyökkäysten tyyppejä on useita, joista esiin yleisimpinä nousivat erilaiset tietojenkalastelutavat (*eng. phishing*). Tutkimuksessa mainittiin tietojenkalastelusta sähköpostia tai valheellista internetsivua hyväksikäyttäen. Toiseksi yleisimpänä mainittiin erilaiset haittaohjelmat. Noin kolmannes vastanneista yrityksistä oli kokenut myös käyttäjän manipulointiin perustuvan hyökkäyksen, jossa joko yritystä lähestyttiin imitoimalla jotain henkilöä tai instituutiota (*eng. impersonating attack*). Myös viime vuosina uutisiin nousseet kiristys- tai kiristyshaittaohjelmat (*eng. ransomware*) raportointiin erillisinä hyökkäyksinä muista haittaohjelmista. Erilaiset hyökkäystyypit ja niiden yleisyydet ovat kuvattuna kuviossa 3.

Huomattavinta kaikkien erilaisten hyökkäysten osuuksissa on juurikin henkilökuntaan kohdistettujen hyökkäysten suuri määrä. Buttonin ym. (2017) mukaan neljä yleisintä hyökkäystyyppiä voidaan suoraan yhdistää tietotekniikkaa käyttävän henkilökunnan inhimillisiin tekijöihin. Tämä tukee väitettä henkilökunnan kouluttamisen tärkeydestä (Button ym., 2017).



KUVIO 3 Hyökkäykset tyypeittäin

Tutkimusten mukaan kyberhyökkäys havaitaan yrityksessä nopeasti. Buttonin ym. (2017) ja Buttonin ym. (2017) tutkimusten mukaan reilusti noin puolet yrityksistä havaitsee hyökkäyksen välittömästi. Tilastoja tutkiessa on huomattava, että kyseiset tilastot koskevat kaikkia tutkimuksessa mukana olleita yrityksiä. Tällöin tilastoissa ovat myös suurien yritysten vastaukset. Kuitenkin kyseiset tilastot antavat jonkinlaisen arvion yritysten kyvystä havaita kyberhyökkäyksiä. Yrityksen toimintaa pahiten häiritsevän hyökkäyksen havaitsemiseen käytetty aika on esitelty kuviossa 3.



KUVIO 4 Kyberhyökkäysten havaitsemisaika

Tutkimukset antavat jonkinlaisen kuvan siitä, että kyberhyökkäykset ovat suhteellisen yleisiä myös PK-yrityksissä. Tämä on vastaan sitä yleistä käsitystä, ett-

eivät PK-yritykset kiinnosta kyberrikollisia tai niihin ei suoriteta kyberhyökkäyksiä. Täyttä varmuutta hyökkäysten yleisyydestä ei saada, mutta tietynlainen trendi voidaan havaita. Pohjana käytetyt 'Cyber security breaches survey' -tutkimukset on toteutettu suurimmaksi osaksi puhelinhaastatteluilla (Button ym., 2017). Haastatteluna suoritettuihin tutkimuksiin voidaan suhtautua hieman varauksellisesti, sillä ei ole täyttä varmuutta haastatellun yrityksen edustajan tilannekuvasta tai täysin rehellisistä vastauksista. Kyberhyökkäyksen paljastuminen saattaa vahingoittaa yrityksen brändikuvaa (KPMG, 2017). Tällöin voi valehtelukin tulla kysymykseen, vaikkei yrityksen nimeä julkaistussa tutkimuksessa mainittaisikaan.

4 PK-YRITYSTEN TIETOTURVA

Tässä luvussa tarkastellaan PK-yritysten tietoturvaa yleisellä tasolla. Samalla luvussa käydään läpi PK-yrityksen tietoturvan kehittämisen tärkeitä elementtejä sekä yleisiä suosituksia tietoturvan kehittämiseen. Luku päätetään yritysten henkilöstön roolin tarkasteluun tietoturvan toteutumisen osana.

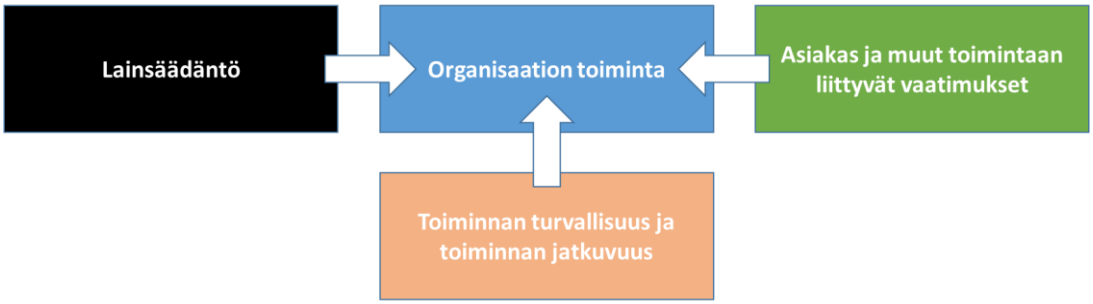
4.1 PK- yrityksen tietoturva yleisesti

Yrityksen tietoturvan suunnittelun ja kehittämisen tulisi lähteä oletuksesta, ettei yksikään tietoturvaratkaisu ole täysin turvallinen (Järvinen & Rousku, 2017, s. 40). Heikkilän ym. (2016) mukaan suurimmat ongelmat tietoturvansuhteen PK-yrityksillä ovat yleisesti tietoturvaan budjetoitujen varojen määrä sekä huono tilannetietoisuus. Tämä yleisesti saattaa näkyä ylioptimistisena suhtautumisena tietoturvaan (Heikkilä ym., 2016). Kurpjuhn (2015) kirjoittaa, että yrityksen investointi tietoturvaan saattaa myös olla hankala käsittää yrityksen johtoportaalle, sillä tietoturva ei lisää tuottavuutta tai vähennä kustannuksia. Tietoturva kannattaakin nähdä vakuutuksena (Kurpjuhn, 2015).

Yrityksen tietoturvaan on olemassa monta vaikuttavaa tekijää, jotka määrittävät tietoturvan tason. Pelkästään teknisiin ratkaisuihin ei tietoturvassa voida tukeutua, vaan organisaation sisäinen tietoturva tulisi olla yhdistelmä teknisiä ratkaisuja, tilanteeseen sopivaa hallintoa sekä henkilöstön huomioonottamista (Singh, Gupta & Ojha, 2014). Heikkilän ym. (2016) mukaan yritykset ovat usein hyvin perillä tietoturvan teknisistä ratkaisuista, mutta pahimmat puutteet löytyvät henkilöstön käyttäytymisestä ja prosesseista.

Ulkoisten vaikuttavien tekijöiden osalta organisaation tulee tunnistaa organisaatioon kohdistuvat uhat, riskit sekä tietoturvaan vaikuttavat tekijät. Vaikuttavia tekijöitä ovat vallitseva lainsäädäntö, asiakasvaatimukset ja sopimukset sekä liiketoiminnan turvallisuus sekä jatkuvuus. (Järvinen & Rousku, 2017.) Vallitsevalla lainsäädännöllä tarkoitetaan sitä, että yrityksen tulee noudattaa sen maan, jossa yritys toimii, vallitsevaa lainsäädäntöä tietoturvan suhteen. Myös yrityksen toimiala saattaa asettaa tiettyjä rajoituksia tai vaatimuksia tieto-

turvan suhteen. Yritykselle saattaa myös tulla vaatimuksia asiakkuus- ja kumppanuussuhteista. Osana liiketoimintaansa, PK-yritykset käsittelevät myös henkilötietoja, joiden käsittelystä määrätään erikseen lailla (Heikkilä ym., 2016). Yrityksen toiminnan turvallisuus ja jatkuvuus ovat myös tärkeitä tekijöitä toteutettaessa organisaation tietoturvaa. Vaikuttavat tekijät on esitelty kuviossa 5:



KUVIO 5 Organisaation tietoturvaan vaikuttavat tekijät (Järvisen ja Rouskun, 2017, s. 31 mukaan)

Järvinen ja Rousku (2017, s. 43) pitävät henkilöstön aktiivista raportointia tietoturvapoikkeamista tärkeänä, sillä vain aktiivisien raportoinnin seurauksena ongelmatilanteisiin voidaan puuttua. Wiion (2013) mukaan yritykseen tulisi saada raportoinnin osalta sellainen ilmapiiri, että liian hätäinen raportointi on yritykselle parempi vaihtoehto kuin henkilökunnan huoleton suhtautuminen mahdollisiin tietoturvapoikkeamiin. Hawkinsin (2017) mukaan organisaation reagoinnin nopeus vaikuttaa suoraan siihen, miten pahaa tuhoa mahdollinen hyökkäys saa organisaatiossa aikaan. Äärimmäisen tärkeää on nopean raportoinnin mahdollisuus siten, ettei henkilökunnan tarvitse miettiä mahdollista oman maineen menetystä raportointitilanteessa (Wiio, 2013 s. 18).

4.2 Yrityksen tietoturvan suunnittelu

Yrityksen tietoturvan toteuttamisessa tulisi määritellä ensiksi se, mitkä ovat tarpeelliset toimenpiteet riittävän suojaustason saavuttamiseksi. Suunnitellessa tietoturvaa, on suojatoimet suhteutettava riskeihin ja oltava tarkoituksen mukaisia (Järvinen & Rousku, 2017, s 32). Stewart ym. (2015, s. 18) mukaan yrityksen tietoturva on aina kompromissi suojauksen ja käytettävyyden välillä. Tällä tarkoitetaan sitä, että tietoturvan näkökulmasta turvatason noustessa käytettävyys huononee (Sun, Ahluwalia & Koong, 2011). Tämän lisäksi on huomioitava suojausratkaisujen kustannukset ja suhteutettava mahdollisen vahingon rahalliseen arvoon (Stewart ym., 2015, s. 18). Näiden lisäksi on otettava huomioon henkilöstön kyky ja halu ylläpitää organisaatiolle riittävää tietoturvaa. Täten tietoturvan ylimitoittaminen on itseasiassa organisaatiolle haitaksi. Haitta saattaa ilmetä esimerkiksi työnteon vaikeutumisena tai jopa estymisenä (Järvinen & Rousku, 2017, s. 32).

Henkilöstön näkökulmasta tietoturvan parantaminen on yritykselle hyödyllistä vain siihen pisteeseen asti, jota henkilöstö pitää tarpeellisena (Sun, Ahluwalia & Koong, 2011). Henkilöstön näkökulmasta siis tietoturvan ylimitoittaminen on siis työntekoa haittaava ratkaisu, joka voi kääntyä itseään vastaan luoden uusia tietoturva-aukkoja organisaatioon.

Tietoturvan suunnittelun osana yrityksen tulisi myös tehdä ohjeistus poikkeustilanteiden varalle. Yksityiskohtainen suunnittelu on organisaatiolle tärkeää nopean hyökkäyksestä palautumisen ja vahinkojen minimoimisen vuoksi (Hawkings, 2017). Tällöin on tarkoituksena varmistaa, että jokainen organisaation osa tuntee oman vastuualueensa hyökkäyksen sattuessa ja osaa toimia ohjeistuksen mukaisesti. Tehokas suunnitelma koostuu kahdesta komponentista (Hawkings, 2017):

- Nopea, luotettava ja turvallinen viestintätapa
- Resurssien tehokas ohjaus ongelmien ratkaisemiseksi

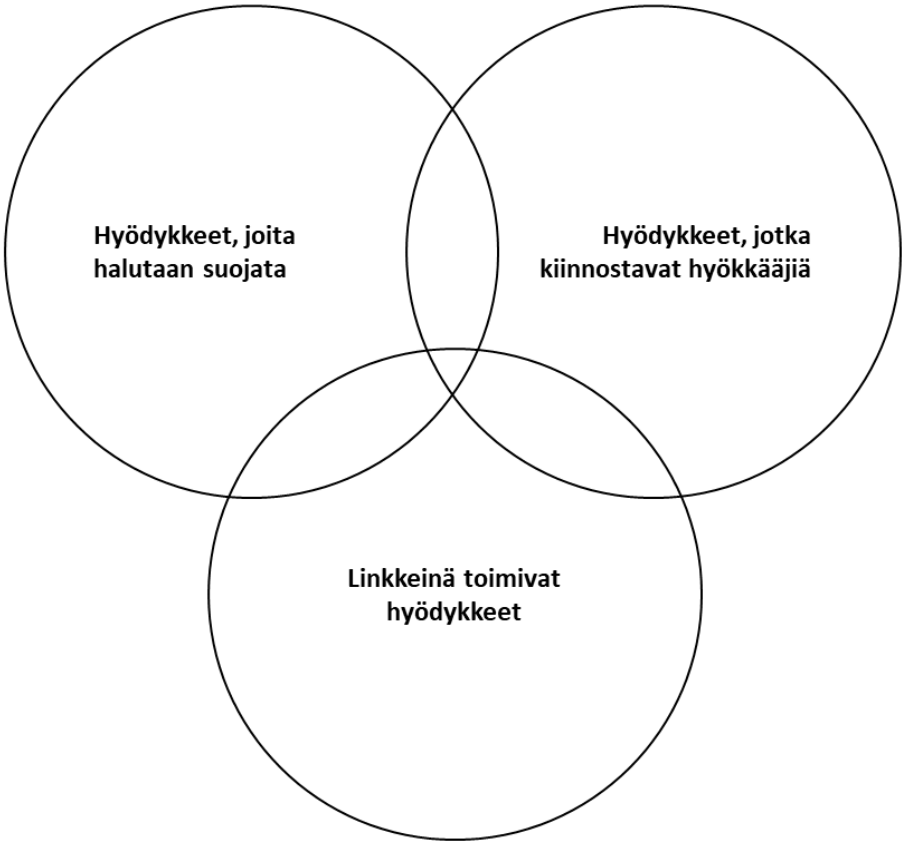
4.3 Yritykselle tärkeiden hyödykkeiden määrittely

Organisaation tietoturvaa suunniteltaessa ja toteuttaessa ongelmaksi saattaa muodostua kysymyksiä siitä mitä tulisi suojata ja miten. Paras lähestymistapa organisaation tietoturvaa toteuttaessa on toimintojen suojaaminen niiden kriittisyyden mukaisesti (Järvinen & Rousku, 2017). Organisaation toimintakyvyn ja jatkuvuuden kannalta välttämättömät toiminnot ovat tällöin tärkein prioriteetti. Organisaatiolle tärkeät toiminnot vaihtelevat organisaatioittain, joten yleisiä ohjeita on vaikea antaa vaan niiden määrittely on tehtävä jokaiselle organisaatiolle erikseen. Tärkeiden ja suojausta vaativien hyödykkeiden määrittely on organisaation tietoturvan toteutumisen kannalta tärkeää, sillä henkilöstö on valmis noudattamaan tietoturvaohjeistuksia vain, jos he pitävät suojausratkaisuja organisaatiolle tarpeellisena (Sun, Ahluwalia & Koong, 2011).

Shostack (2014) esittelee kirjassaan hyödykeperustaisen uhkamallinnuksen (*eng. asset-centered threat modeling*), jossa organisaation hyödykkeet listataan ja jaotellaan kolmeen eri kategoriaan. Kategorioiden pohjalta voidaan määrittää mahdolliset uhat, jotka kyseisiä hyödykkeitä uhkaavat. Mallin pohjalta organisaatio voi selvittää tietoturvan toteuttamiseksi kriittiset elementit:

- Hyödykkeet, joita halutaan suojata
- Hyödykkeet, jotka hyökkääjiä todennäköisesti kiinnostavat
- Hyödykkeet, jotka toimivat linkkinä kahden edellisen elementin välillä

Hyödykkeiden väliset suhteet on kuvattu kuviossa 6.



KUVIO 6 Hyödykkeiden väliset suhteet (Shostackin, 2014, s. 37 mukaan)

Hyödykkeet, joita halutaan suojata ovat Shostackin (2014 s. 38) mukaan organisaatiolle tärkeitä hyödykkeitä, jotka voivat olla niin aineellisia tai aineettomia. Esimerkiksi organisaation maine, brändikuva tai asiakasluottamus ovat aineettomia hyödykkeitä, joita vastaan on hyökkääjän vaikea hyökätä suoraan. Asiantuntijapalveluita tarjoavan yrityksen KPMGn (2017) mukaan 89% yrityksistä kokee, että organisaatiota vastaan tehty kyberhyökkäys vahingoittaa organisaatiota. Tällöin brändin maineen menetys, asiakkaiden kaikkoaminen ja uusien liiketoimintasuunnitelmien toteuttaminen vaikuttavat organisaation kykyyn selviytyä kilpailussa (KPMG, 2017). Heikkilä ym. (2016) kirjoittavat että, varsinkin teollisuuden alalla toimivissa yrityksissä, aineettomiksi hyödykkeiksi voidaan myös laskea yrityksen immateriaalioikeudet. Suojatessa yrityksen valmistamia tuotteita, tulisi suojaus mitoittaa kattamaan koko tuotteen elinkaari (Heikkilä ym., 2016.). Kuitenkin onnistuessaan hyökkäys voi vahingoittaa kyseisiä hyödykkeitä ja aiheuttaa yritykselle haittaa. Mallissa aineellisena hyödykkeenä voidaan pitää yrityksen päätelaitteita, joiden rikkoutuminen haittaa yrityksen päivittäisiä toimintoja.

Hyödykkeet, jotka todennäköisesti kiinnostavat hyökkääjiä ovat Shostackin (2014 s. 38) mukaan suhteellisen helposti määriteltäviä, konkreettisia asioita. Hyökkääjälle kiinnostavat hyödykkeet ovat riippuvaisia hyökkääjän mo-

tiivista. Kyberrikolliselle kiinnostavat hyödykkeet ovat esimerkiksi henkilötiedot, luottokorttien numerot tai käyttäjätunnukset.

Linkkeinä toimivilla hyödykkeillä Shostack (2014) tarkoittaa hyödykkeitä, jotka mahdollistavat hyökkääjille pääsyn haluamansa hyödykkeeseen, jota on haluttu suojata. Esimerkkinä järjestelmän ylläpitäjän tietokone ja käyttäjätunnukset, joiden avulla hyökkääjä pääsee esteettä sisään yrityksen tietojärjestelmään.

Tulee huomata, että kyseinen malli ei kerro miten kyseisiä hyödykkeitä tulisi suojata, vaan antaa karkean arvion siitä, mihin organisaatiossa tulee kiinnittää erityisesti huomiota. Shostack (2014 s. 39) huomauttaa ettei hyödykkeiden, niiden välisten suhteiden tai niitä uhkaavat uhkat ole aina yksinkertaisia määrittää. Mallin tarkoitus on tarjota karkea arvio organisaation tärkeimmistä hyödykkeistä ja niiden turvaamisesta (Shostack, 2014 s. 39).

4.4 Henkilöstön rooli tietoturvassa

Kirjassaan Wiio (2013, s. 14) kertoo, että yrityksen onnistuneen tietoturvan perusedellytys on johdon tuki. Johdon ensimmäisiä tehtäviä Cyber Security Coalitionin (2016) mukaan on tietoturvavastaavan nimittäminen. Tulee myös huomata, että mikäli yrityksellä ei IT- tai tietoturvavastaavaa ole henkilöstömäärän tai budjetin takia ole, ovat myös ulkoistaminen tai konsulttipalvelut mahdollinen vaihtoehto (Heikkilä ym., 2016). Wiio (2013) kirjoittaa, että jos kyseessä on pieni, muutaman hengen yritys, on yrityksessä vain sovittava, kuka on yrityksen tietoturvavastaava. Valitulle vastaavalle on mahdollisuuksien mukaan annettava aikaa sekä resursseja kehittää osaamistaan (Wiio, 2013 s. 16). Onnistuneen tietoturvan toteutuminen tarvitsee jatkuvaa seurantaa, joten tietoturvavastaavan tulee olla tietoinen uusista standardeista ja yritystä uhkaavista, uusista uhista (Heikkilä ym., 2016). Eling ja Schnell (2016) huomauttavat, että tietotekniikan kehittyessä nopeasti, uudet teknologiat saattavat kasvattaa organisaation tietoturvariskiä. Yrityksen johdon tulisikin ottaa selvää tietosuojaa ja tietoturvaa koskevasta lainsäädännöstä sekä tarvittaessa muutettava toimintaansa vastaamaan vaatimuksia (Cyber Security Coalition, 2016). Tietoturvavastaavan rooli on siis tilannetietoisuuden ylläpidon ja yrityksen johdon informoinnin kannalta elintärkeä.

Johdon tulee tarjota henkilökunnalle selkeä ja yksiselitteinen tietoturvastrategia, jonka mukaan yrityksen henkilöstö on kykenevä toimimaan. Johdolle kuuluu myös vastuu tietoturvastrategian valvomisesta organisaatiossa. Samalla henkilökunnalle on tarjottava koko organisaatiota koskevat tietoturvalinjaukset (Cyber Security Coalition, 2016). Strategian laadinnassa ja tiedottamisessa tulee yrityksen johdon olla johdonmukainen, sillä epäjohdonmukaisuus heijastuu negatiivisesti henkilökunnan suhtautumisesta tietoturvaan (Singh ym., 2014). Voidaan siis päätellä, että yrityksen tietoturvavastaavan ylläpitämä tilannekuva ja johdon sitoutuminen vaikuttavat suoraan yrityksen sisäisen viestinnän johdonmukaisuuteen. Singh ym., (2014) kirjoittavat, että tietoturvastrategiassa tu-

lee olla selkeästi määritellyt tavoitteet, toimintatavat, tehtävät ja vastuualueet. Samalla on määriteltävä henkilökunnalle turvalliset työskentelytavat. Tällä pyritään välttämään tilanne, jossa henkilökunta ei tiedä yrityksen tavoitteista tietoturvan suhteen (Singh ym., 2014.). Tietoturvapolitiikkaa ei tulisi kuitenkaan pakottaa yrityksen henkilöstölle, sillä pakottamisen tuomat haittavaikutukset pahimmassa tapauksessa ylittivät hyvin laaditun tietoturvapolitiikan tuomat hyödyt. Sun, Ahluwalia ja Koong (2011) alkavat kiertää suojausratkaisuja ja laiminlyömään ohjeistuksia, jos kokevat tietoturvapolitiikan haittaavan työskentelyä tai työtyytyväisyyttä. Oikein laaditun tietoturvapolitiikan käyttöönottoa voidaan kuitenkin pehmittää korostamalla suojattavien järjestelmien ja datan kriittisyyttä sekä suojauksen tarvetta (Sun, Ahluwalia & Koong, 2011).

Henkilöstön kouluttamista ja informointia mietittäessä tulee johdon ottaa huomioon, että henkilöstön kyky ja halu työskennellä tietoturvallisella tavalla ja noudattaa tietoturvaohjeistuksia, on vahvasti yksilöstä kiinni. Nykäsen (2011) mukaan ohjeistusten vastainen käyttäytyminen on seurausta yksilön henkilökohtaisista tavoista ja tottumuksista, joita puolustellaan erilaisilla syillä. Kuitenkin Kinnusen (2015) mukaan henkilöstön oletetaan tuntevan tietoturva-asiat ennestään, ilman erillistä koulutusta. Henkilöstön kouluttamisella pyritään saamaan koko henkilöstö sisäistämään yrityksen tietoturvapolitiikka ja varsinkin suojattavien hyödykkeiden tärkeys. Yleisesti henkilöstölle voidaan antaa konkreettinen esimerkki siitä miksi pitää toimia tietoturvallisella tavalla ja miten se tapahtuu (Nykänen, 2011). Kinnunen (2015) kirjoittaa, että kun työntekijät saadaan ymmärtämään tietoturvakriteereiden tärkeys, motivoituvat he sisäisesti noudattamaan tietoturvaohjeistuksia. Motivoinnissa on tärkeimpiä elementtejä ovat usko oman tekemisen tärkeydestä ja toisen henkilön tai tilanteen vaatimus (Kinnunen, 2015). Koulutuksen pääasiallinen tarkoitus on siis auttaa henkilöstöä kehittämään työskentelyään tietoturvan suhteen itseohjeutuvaksi sekä moraalista vastuuta kantavaksi (Nykänen, 2011).

5 Yhteenveto

Tutkielman tarkoituksena oli kartoittaa pienten ja keskisuurien yritysten kybervalmiutta sekä kykyä vastata nykyisiin kyberuhkiin. Samalla käytiin läpi muutamia yleisiä suosituksia, joiden pohjalta yrityksen kyberturvallisuutta voidaan kehittää. Tutkielmaa lukiessa tulee muistaa, että kybermaailma ja sen ilmiöt ovat alati muuttuva kokonaisuus, joka vaatii yrityksiltä mukautuvuutta uuteen vallitsevaan tilanteeseen.

PK-yrityksiksi lasketaan kirjava joukko eri kokoisia ja eri toimialoilla toimivia yrityksiä. Jokaisen yrityksen tilanne ja osaamistaso informaatioteknologian hallinnassa on erilainen. PK-yrityksen organisaatiorakenne eroaa huomattavasti paljon tutkittujen, isojen yritysten organisaatiorakenteesta. Huomattavampia piirteitä olivat matala hierarkia, epämuodollinen yrityskulttuuri ja päätöksenteon keskittyminen yrityksen toimitusjohtajalle sekä yrityksen avainhenkilöille. Johtuen pienestä henkilöstömäärästä PK-yrityksen henkilöstö on pakotettu ottamaan useita rooleja organisaatiossa. Tämä aiheuttaa sen, että henkilöstölle jää aukkoja työtehtävien suorittamiseksi tarvittaviin tietoihin ja ammattitaitoon. PK-yritykset myös vierastavat henkilöstön koulutusta, koska koulutuksen kustannukset ovat organisaatiolle suhteessa suuremmat kuin suurelle yritykselle tai pelkäävät juuri koulutetun henkilön jättävän organisaation.

Mikäli PK-yrityksellä ei ole palveluksessaan henkilöä, joka tuntee informaatioteknologiaa ja sen ominaisuuksia, jätetään yrityksen tietohallinto osittain tai kokonaan suunnittelematta. Tilannetta pahentaa sen, että usein yritys on pakotettu hankkimaan uutta teknologiaa joko organisaation sisäisestä tai ulkoisesta painostuksesta. Tällöin uusi teknologia vain lisätään organisaation käyttöön miettimättä mikä olisi järkevin ja turvallisin tapa teknologian käyttöön. Tästä voidaan vetää johtopäätös, että jos organisaation johdolla on hankaluuksia uuden teknologian käyttöönotossa ja käytön suunnittelussa, myös organisaation tietoturva jää ilman huomiota.

Kybermaailmassa toimii PK-yritykselle useita uhkia, jotka organisaatiota vastaan hyökätessään voivat aiheuttaa merkittäviä tappiota. Uhista voidaan nostaa esille kyberrikolliset sekä kybervandaalit. Yrityksen ollessa tietoinen tyypillisimmistä hyökkäystyypeistä, on yrityksen johdon ryhdyttävä toimiin tietoturvan parantamiseksi. Tutkielmassa esiteltiin yksi tapa tietoturvapoik-

keamien käsittelyyn yrityksessä. Tärkeimpänä asiana kuitenkin nostettiin esille henkilökunnan kannustaminen raportointiin sekä tarpeeksi ripeä reagointi tietoturvapoikkeamien sattuessa. Samalla myös muistutettiin kirjallisten ja selkeiden ohjeiden tärkeydestä tietoturvaa toteuttaessa.

Tutkielman kirjoittamista muutamana edeltävänä vuonna PK-yritykset raportoivat kokemiensa kyberhyökkäysten määrästä vaihtelevasti. Kuitenkin myytti siitä, ettei PK-yritykset kiinnosta hyökkääjiä, on kumottu. Tyypillisesti PK-yritys kohtaa vain muutaman kyberhyökkäyksen vuodessa. Hyökkäysten määrä vaihtelee suuresti yrityksittäin, sillä jotkut yritykset raportoivat, ettei heitä vastaan ole suoritettu yhtään hyökkäystä. Useita hyökkäyksiä kokevia yrityksiä on myös, mutta tällaiset yritykset ovat vähemmistö. Huomattavaa on, että liki puolet hyökkäyksistä havaitaan heti ja suurin osa yhden vuorokauden sisällä. Tyypillisimpiä hyökkäystyyppejä ovat erilaiset huijausviestit, tietojenkalasteluviestit ja haittaohjelmat. Myös palvelunestohyökkäyksiä ja tietojärjestelmään tunkeutumisia havaittiin.

Yrityksen tietoturvaa toteuttaessa esille tärkeimpänä nousi johdon tuki tietoturvan kehittämiseksi, joka oli perusedellytys toimivan tietoturvan aikaansaamiseksi. Yrityksen ei tule kuitenkaan liioitella suojausratkaisuissa, sillä suojauksen lisääminen haittaa aina käytettävyyttä. Suojaus tulisikin kohdistaa ennalta määriteltyjen, yritykselle kriittisten elementtien suojaamiseen. Henkilöstön sitoutumista tietoturvan toteuttamiseen ylläpidetään johdonmukaisella tiedottamisella, kouluttamisella sekä selkeällä, ajantasaisella tietoturvapolitiikkalla.

Tutkielman tuloksista nousee esille yleiset suositukset siitä, miten PK-yrityksen tietoturva voidaan toteuttaa. Tietoturva tulee kuitenkin suunnitella ja toteuttaa jokaiselle yritykselle erikseen. Tutkielmassa mainittiin, että yleisistä standardeista voi olla hyötyä tietoturvaa toteuttaessa, mutta ne eivät sellaisenaan sovellu PK-yritysten käyttöön. Pienien ja keskisuurien yritysten tietotekniikan käyttö ja laitteiden määrä vaihtelevat, samoin henkilökunnan osaamistaso. Tästä syystä tutkielmassa ei voitu vastata suoraan siihen, onko jokin ratkaisu hyvä tai huono. Jo tapahtuneita kyberhyökkäyksiä tarkastellessa tulee muistaa, että kyselytutkimuksen käyttö on suuntaa-antavaa. On mahdollista, että osa yrityksistä ei ole joko huomannut kyberhyökkäystä tai eivät antaneet totuudenmukaista kuvaa kyselyitä toteuttaessa. Tuloksiin vaikuttaa myös kysymysten asettelu. Kyselytutkimukset oli suoritettu englannin kielisissä maissa, joten sinällään tulokset eivät ole suoraan verrattavissa Suomeen tai suomalaisiin PK-yrityksiin.

Tutkielman kirjoittaminen nosti esille jatkotutkimusaiheita, joiden avulla PK-yritysten tietoturvaa olisi mahdollista tarkastella lähemmin. Yrityksen tietoturvaratkaisuihin vaikuttavat tekijät, motiivit sekä kouluttaminen voisivat kaivata huomiota. Kyberhyökkäykset tulevat olemaan osa yritysten arkea, joten myös PK-yritysten resilienssi voisi olla mielenkiintoinen tutkimusaihe. Tietoturvan lähtiessä ihmisestä, myös henkilökunnan kouluttaminen sekä motivointi voisivat olla mainitsemisen arvoisia lähteitä. Samalla kun kybermaailma muuttuu ja PK-yritykset jatkavat merkittävänä työllistäjänä, näiden kahden yhdistelmä tuottaa monia tutkittavan arvoisia aiheita.

LÄHTEET

Ashenden D. (2011) Cyber security : time for engagement and debate. In : Ottis R (ed) Proceedings of the 10th european conference on information warfare and security (ECIW 2011, Tallinn). Academic Publishing, Reading, UK, pp 11-16

Ayat, M., Masrom, M., Sahibuddin, S., & Sharifi, M. (2011). Issues in implementing IT governance in Small and Medium Enterprises. In *Proceedings - 2011 2nd International Conference on Intelligent Systems, Modelling and Simulation, ISMS 2011* (pp. 197-201). DOI: 10.1109/ISMS.2011.40

Bergeron, F., Croteau, A., Uwizeyemungu, S. & Raymond, L. (2015). IT Governance Theories and the Reality of SMEs: Bridging the Gap. *IEEE.* DOI: 10.1109/HICSS.2015.542

Button, M., Klahr, R., Amili, S., Shah, J. N. & Wang, V. (2016). *Cyber Security Breaches Survey 2016.* Saatavilla osoiteesta https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/521465/Cyber_Security_Breaches_Survey_2016_main_report_FINAL.pdf

Button, M., Klahr, R., Shah, J. N., Sheriffs, P., Rossington, T., Pestell, G. & Wang, V. (2017). *Cyber security breaches survey 2017.* Saatavilla osoiteesta https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf

Cavelty, M.D. (2010) The reality and future of cyberwar, *Parliamentary Brief.* Haettu 30.3.2010

Cyber Security Coalition. (2016). *Cyber Security Guide for SME.* Saatavilla osoitteesta https://www.cybersecuritycoalition.be/content/uploads/cybersecurity-guide-sme-EN.pdf

Cragg, P. (2008). Identifying key Information Systems competencies in small firms. *Total Quality Management & Business Excellence, 19:1-2, 29-35.* DOI: 10.1080/14783360701601926

Devos, J., Van Landeghem, H. & Deschoolmeester, D. (2012). Rethinking IT governance for SMEs. *Industrial Management & Data Systems, Vol. 112 Issue: 2, pp.206-223.* https://doi.org/10.1108/02635571211204263

Eling, M. & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance, Vol. 17 Issue: 5, pp.474-491.* https://doi.org/10.1108/JRF-09-2016-0122

FSB. (2016). *Cyber Resilience: How to protect small firms in the digital economy.* Saatavilla osoitteesta https://www.fsb.org.uk/docs/default-source/fsb-org-uk/FSB-Cyber-Resilience-report-2016.pdf?sfvrsn=0

Hawkings, N. (2017). Why communication is vital during a cyber-attack. *Network Security. Vol. 2017. Issue 3. pp. 12-14.* https://doi.org/10.1016/S1353-4858(17)30028-4

Heikkilä, M., Rättyä, A., Pieskä, S. & Jämsä, J. (2016). Security Challenges in Small- and Medium-Sized Manufacturing Enterprises. *Conference: 2016 International Symposium on Small-scale Intelligent Manufacturing Systems (SIMS).* DOI: 10.1109/SIMS.2016.7802895

Järvinen, P. & Rousku, K. (2017). *Työpaikan tietoturvaopas: tunnista uhat, hallitse riskit.* Helsinki: Alma Talent.

Lehto, M., & Neittaanmäki, P. (Eds.). (2015). *Cyber security: analytics, technology and automation*. Saatavilla osoitteesta https://ebookcentral.proquest.com

Kinnunen, N. (2015). *Tietoturvaohjeistusten noudattamisen motivaatio ja sen muuttuminen* (Väitöskirja). Acta Wasaensia, 331. Vaasan Yliopisto. Haettu osoitteesta https://www.univaasa.fi/materiaali/pdf/isbn_978-952-476-637-1.pdf

KPMG. (2017). *Small Business Reputation & Cyber Risk.* Saatavilla osoitteesta https://home.kpmg.com/content/dam/kpmg/pdf/2016/02/small-business-reputation-new.pdf

Kurki, M. (2010). *Pk-yrityksen tietotekniikka käytännönläheisesti.* Helsinki: Kauppakamari.

Kurpjuhn, T. (2015). The SME security challenge. *Computer Fraud & Security. Vol. 2015, Issue: 3, March 2015, p. 5-7.* https://doi.org/10.1016/S1361-3723(15)30017-8

Nfuka, E. N. & Rusu, L. (2011). The effect of critical success factors on IT governance performance. *Industrial Management & Data Systems, Vol. 111 Issue: 9, pp.1418-1448.* https://doi.org/10.1108/02635571111182773

Nguyen, T. H. (2009) Information technology adoption in SMEs: an integrated framework. *International Journal of Entrepreneurial Behavior & Research, Vol. 15 Issue: 2, pp.162-186.* https://doi.org/10.1108/13552550910944566

NSW Government. (2017). Cyber Scare: A look at small to medium-sized business and the emergence of cybercrime in Australia. Saatavilla osoitteesta https://www.smallbusiness.nsw.gov.au/__data/assets/pdf_file/0007/104857/cyber-scare-full-report.pdf

Nykänen, K. (2011). *Tietoturvakoulutuksen vaikuttavuuden arviointi yksilön ja organisaation tietoturvakäyttäytymiseen* (Väitöskirja). A Scientiae Rerum Naturalium 581. Oulun Yliopisto. Haettu osoitteesta http://jultika.oulu.fi/files/isbn9789514295713.pdf

O'Regan, N., Sims, M. & Ghobadian, A. (2005). High performance: ownershipand decision-making in SMEs. *Management Decision, Vol. 43 Issue: 3, pp.382-396.* https://doi.org/10.1108/00251740510589760

Shostack, A. (2014). *Threat modeling – Designing for Security.* Indianapolis, IN: John Wiley & Sons, Inc.

Singh A. N., Gupta, M. P. & Ojha, A. (2014). Identifying factors of organizational information security management. *Journal of Enterprise Information Management, Vol. 27 Issue: 5, pp.644-667.* https://doi.org/10.1108/JEIM-07-2013-0052

Stewart, J. M., Chapple, M. & Gibson D. (2015). *CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide (7. uud. painos).* Indianapolis, IN: John Wiley & Sons, Inc.

Sun, J., Ahluwalia, P. & Koong, K. S. (2011). The more secure the better? A study of information security readiness. *Industrial Management & Data Systems, Vol. 111 Issue: 4, pp.570-588.* https://doi.org/10.1108/02635571111133551

Tilastokeskus. (2017, 8. marraskuuta). Käsiteet – Pienet ja keskisuuret yritykset. Haettu 8.11.2017 osoitteesta http://www.stat.fi/meta/kas/pienet_ja_keski.html

Työturvallisuuskeskus. (n. d.). Liite: Tietoturvapolitiikkaan liittyvät määritelmät. Haettu 21.3.2018 osoitteesta http://tietoturva.tkk.fi/fi/politiikka/liite2.htm

Yrittäjät (2017, 12. huhtikuuta). Yrittäjyys Suomessa. Haettu 13.1.2018 osoitteesta https://www.yrittajat.fi/suomen-yrittajat/yrittajyys-suomessa-316363

Wiio, A. (2013). *PK-yrityksen kyberturvallisuuden kehittäminen.* Saatavilla osoitteesta https://s3-eu-west-1.amazonaws.com/huoltovarmuuskeskus/app/uploads/2016/08/31144436/2013_Kyberturvallisuusopas_www.pdf?AWSAccessKeyId=AKIAITCZ

YCPQYFESGSAQ&Expires=1517053747&Signature=sWAUHRb9JYsU2%2B06Uj5yxl48MJ0%3D