jamk.fi

Pk-yritysten varautuminen kyberturvallisuusuhkien varalle

- tutkimus nykytilasta pienyrityksissä

Aimo Pellinen

Opinnäytetyö
Toukokuu 2018
Tekniikan ja liikenteen ala
Insinööri YAMK, Teknologiaosaamisen johtamisen tutkinto-ohjelma

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
PELLINEN, Aimo	Opinnäytetyö, ylempi AMK	31.05.2018
	Sivumäärä 116	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: (x)

Työn nimi

Pk-yritysten varautuminen kyberturvallisuusuhkien varalle - tutkimus nykytilasta pienyrityksissä

Tutkinto-ohjelma

Teknologiaosaamisen johtamisen tutkinto-ohjelma

Työn ohjaaja(t)

KARJALAINEN, Mika ja JURVELIN, Jouni

Toimeksiantaja(t)

Jyväskylän ammattikorkeakoulu, IT-instituutti

Tiivistelmä

Digitalisaatio nähdään sekä yritysten että julkisen sektorin tuottavuutta ja kilpailukykyä lisäävänä tekijänä, mutta sen yhtenä varjopuolena ovat lisääntyvät tieto- ja kyberturvallisuusuhkat, jotka toteutuessaan vaikuttavat merkittävästi organisaation toimintaan ja sen jatkuvuuteen. Opinnäytetyön tarkoituksena oli tuottaa tietoa Keski-Suomen alueella toimivien pk-yritysten kyberturvallisuustietoisuuden ja kyberuhkiin varautumisen nykytilasta liiketoiminnan eri osa-alueilla.

Tietoperustassa nostettiin esille digitalisaation taustalla vaikuttavia teknisiä kehitystrendejä sekä digitalisaation vaikutuksista aiheutuvaa yhteiskunnan ja sen talouden rakenteiden sekä markkinoiden muuttumista ja sen vaikutuksia erityisesti pk-yrityksiin. Toinen tietoperustan pääteema oli kyberturvallisuus sekä siihen liittyvien uhkien mahdolliset vaikutukset yrityksiin.

Tutkimusaineisto kerättiin kevään 2016 aikana strukturoidun haastattelututkimuksen avulla JAMK:n IT-instituutin toteuttamaan Cyber Scheme Finland –pilottiprojektiin osallistuneissa 20 pk-yrityksessä. Tutkimus rakentui tutkimuskysymyksien perusteella laadituista viidestä kysymyssarjasta. Tuloksia tarkasteltiin kysymyksittäin, kysymyssarjoittain ja toimialoittain, mutta kuitenkin siten että vastaajien anonymiteetti säilyi.

Tutkimuksen tuloksista voitiin todeta, että kyberturvallisuus on terminä jossain määrin epäselvä, mutta sitä pidettiin hyvin hallittuna yrityksen kilpailutekijänä. Tiedon kriittinen merkitys liiketoiminnalle tunnistettiin hyvin, mutta sen arvon määrittely oli vielä vähäistä. Kyberturvallisuuteen ja sen hallintaan liittyvissä prosesseissa oli paljon kehittämisen varaa. Myöskään henkilöstön kyberturvallisuustietoisuuteen ja osaamiseen ei oltu panostettu. Sen sijaan fyysinen turvallisuus oli kyberturvallisuuden näkökulmasta melko hyvällä tasolla.

Avainsanat (asiasanat)

kyberturvallisuus, tietoturva, pienet ja keskisuuret yritykset, varautuminen, sertifiointi

Muut tiedot

liite: haastattelussa käytetty kyselylomake, 2 sivua

jamk.fi

Description

Author(s)	Type of publication	Date
PELLINEN, Aimo	Master's thesis	31.5.2018
	Number of pages 116	Language of publication: Finnish
		Permission for web publication: (x)

Title of publication

Cyber security preparedness in SMEs – study on present situation

Degree programme

Degree Programme in Technological Competence Management

Supervisor(s)

KARJALAINEN, Mika and JURVELIN, Jouni

Assigned by

JAMK University of Applied Sciences, Institute of Information Technology

Abstract

Digital transformation is seen as a significant factor in improving both productivity and competitiveness of enterprises and the public sector, but there is a growing shadow of information and cyber security threats that, when realized, may have a significant impact on the organization's operations and its continuity. The aim of this thesis was to provide information on the current state of cyber security awareness and preparedness against cyber threats in different areas of business among SMEs operating in the Central Finland area.

The theoretical background highlighted the technical developments underlying the digitalization and the changes in society and its structures, the market and the effects of digitalization, particularly on SMEs. Another theme in the background base was cybersecurity and the potential impacts of relevant cyber threats menacing companies.

The study material was collected during spring 2016 through a structured interview study in the 20 SMEs participating in the Cyber Scheme Finland -pilot project implemented by the JAMK Institute of Information Technology. The study was constructed of five question series prepared based on the research questions. The results were reviewed by question, question series and industry by keeping the anonymity of the respondents.

From the results of the study, it was noted that cyber safety was somewhat ambiguous, but was considered as well-controlled one of company's competitive factors. The critical importance of information/data for the business was well identified, but its' value was still unknown in most of the companies. It was also noted, that there was a lot work to be done in the processes of cyber security management. Also the cybersecurity awareness and competence of the personnel are on insufficient level. On the other hand, the area of physical security was organized reasonably well from the cyber security point of view.

Keywords/tags (subjects)

cyber security, data security, small and medium-sized enterprises, preparedness, certification

Miscellanous

Attachments: questionnaire, 2 pages

SISÄLLYS

1 JOHDANTO

Tieto sekä sen käsittelyssä ja tallentamisessa käytettävä teknologia ovat yhä useamman yrityksen kriittisiä menestystekijöitä. Henkinen pääoma, tuotteiden suunnitteluun, valmistusprosessiin, henkilöstöön, asiakassuhteisiin tai strategiaan liittyvät luottamukselliset tai arkaluontoiset tiedot muodostavat osan yritysten kilpailuedusta. Samalla tarve käyttää ja jakaa tietoa entistä laajemmin ja tehokkaammin uusia tieto- ja viestintätekniikoita käyttäen lisää yrityksen tietopääomaan liittyviä riskejä, sillä uutiset tietomurroista ja palvelunestohyökkäyksistä ovat jo arkipäivää lehdistössä.

Niin suuret kuin pienet yritykset ovat nyt alttiina yhä kasvavalle tietoverkkorikollisuudelle, jossa toimijoita ovat hakkerit, valtiolliset toimijat ja mahdollisesti myös kilpailijat. Liiketoiminnan näkökulmasta on hyvin tärkeää, että yritys - suuri tai pieni - kykenee tunnistamaan tietoverkkojensa turvallisuusuhkia ja arvioimaan turvallisuusriskejä. Samaan aikaan yritysjohtajien on myös tunnistettava, että kyberturvallisuusriskien hallinta on kokonaisvaltainen ja jatkuva prosessi, jossa ei ole olemassa absoluuttista turvallisuutta eikä sitä tulla koskaan saavuttamaankaan.

Tämä ylempään ammattikorkeakoulututkintoon (YAMK) liittyvä opinnäytetyö käsittelee kyberturvallisuuden huomioonottamista pk-yritysten strategiassa ja toiminnassa. Työn tavoitteena on tuottaa tietoa Keski-Suomessa toimivien pk-yritysten kyberturvallisuustietoisuuden ja kyberuhkiin varautumisen nykytilasta eri osa-alueilla. Tutkimuksen tuloksia voidaan hyödyntää kyberturvallisuustietoisuuden lisäämisessä erityisesti pk-yritysten keskuudessa. Tietoisuuden lisäämisellä pyritään nostamaan esille kehittämistarpeita ja -toimenpiteitä, jotka lisäisivät yritysten sietokykyä kyberuhkia vastaan. Tarve opinnäytetyöhön sisältyvän tutkimuksen tekemiseen tuli esille Jyväskylän ammattikorkeakoulun IT-instituutissa vuosina 2015-2016 toteutetussa Cyber Scheme Finland –pilottiprojektissa, jonka yhteen toimenpidekokonaisuuteen sisältyi tähän työhön sisältyvän tutkimuksen tekeminen. Opinnäytetyö koostuu tausta- ja teoriaosasta sekä empiirisestä tutkimuksesta, joka toteutettiin strukturoituna haastattelututkimuksena. Tutkimuksessa kartoitettiin pk-yritysten toimintaan strategiaan ja toimintaprosesseihin liittyviä seikkoja, joiden perusteella voidaan arvioida yritysten kyberturvallistietoisuutta ja sen nykytilaa.

Tutkimuksen aihe oli ajankohtainen jo sen toteuttamisen hetkellä ja asian merkitys on digitalisaation myötä edelleen lisääntynyt. Tutkimuslaitos Gartner:in laatimalla

strategisten teknologiatrendien Top 10 –listalla ei ole yhtään sellaista trendiä, johon ei liittyisi kyberturvallisuus tavalla tai toisella (Gartner's top 10 Strategic Technology Trends for 2017. 2016).

Tämä opinnäytetyö jakautuu seitsemään sisällölliseen lukuun. Toisessa ja kolmannessa luvuissa kuvataan tutkimuksen ja sen aiheen kannalta keskeisinä teemoina digitalisaatiokehitystä sekä kyberturvallisuutta. Ne ilmiöinä vaikuttavat tutkimuksen kohderyhmän lisäksi kaikilla tasoilla aina yksilöstä globaaleihin vaikutuksiin saakka. Neljännessä luvussa kuvataan tutkimuksen taustalähtökohdat, tavoitteet ja tutkimuskysymykset sekä tutkimusmenetelmä. Viides luku kuvaa tutkimuksen toteuttamista ja sen vaiheita. Kuudennessa luvussa kuvataan tutkimuksen tulokset ja verrataan niitä soveltuvin osin samaan teemaan liittyviin, mutta kohderyhmältään laajempiin kansallisiin ja kansainvälisiin tutkimuksiin. Seitsemäs luku keskittyy johtopäätöksiin, pohdintaan ja tulosten hyödyntämiseen.

2 PK-YRITYSTEN DIGITAALINEN TOIMINTAYMPÄRISTÖ

2.1 DIGITALISAATIO KÄSITTEENÄ

Digitalisaatio on yleisyydestään huolimatta käsite, jolle ei löydy tarkkaa määritelmää. Eräs maailman johtavista tutkimuslaitoksista, Gartner Inc., kuvaa digitalisaatiota seuraavasti:

"Digitalization is the use of digital technologies to change a business model and provide new revenue and value-producing opportunities; it is the process of moving to a digital business." (Digitalization. IT Glossary. 2016.)

Suomen valtiovarainministeriön antoi Valtiokonttorille tehtäväksi syksyn 2015 kuluessa selvittää, millaisilla toimenpiteillä valtionhallinnon tuottavuutta voidaan digitalisaation avulla lisätä. Tehdyssä selvityksessä digitalisaatiolla tarkoitetaan:

> *Kokonaisvaltaista toimintatapojen uudistamista, joka sisältää myös uusien digitaalisten teknologioiden käyttöönottoja. Digitaalisilla teknologioilla tarkoitetaan muun muassa analytiikkaa, big dataa, mobiiliteknologioita, pilvipalveluita, robotiikkaa, sosiaalista mediaa ja asioiden internetiä (ml. teollinen internet).* (Valmiina digikiriin: Digitalisaatio ja virastojen tuottavuuspotentiaali 2015, 11)

Selvityksen tuloksista kertovassa esittelymateriaalissa todetaan:

”Digitalisaatio on tapa, jolla organisaatio tuottaa arvoa uusien, ketterien toimintatapojen sekä digitaalisten teknologioiden avulla.” (Valmiina digikiriin: Virastojen ehdotuksilla uutta tehoa tuottavuuteen – digitalisaation siivittämänä. 2015, 1.)

Hieman eri sanoin, mutta lähes saman sisältöisesti kuvaavat digitalisaatiota Manninen, Brandt, Kallionpää ja Lepola vuonna 2015 julkaistussa kirjassaan ”Uuskasvun polut – Digitalisaation lupaus”:

”Digitalisaatiolla viitataan tietotekniikan hyödyntämiseen sellaisella syvyydellä, että tieto- ja viestintätekniikka sulautuu yhä useampaan arkiseen asiaan sekä yksilöiden että yritysten arjessa.” (Manninen ja muut 2015, 32.)

Digitalisaatiosta todetaan, että kyse ei ole sinänsä uudesta ilmiöstä vaan kyseessä on tietoyhteiskunnan murroksesta seuraavaa jatkumoa. Selkeänä erona aikaisempaan ja samalla suurena mahdollisuutena on tällä hetkellä usean ICT-alueen teknologisen ajurin yhtäaikainen positiivinen toiminnallinen ja taloudellinen kehitys.

Kaikille ylläoleville määritelmille on yhteistä digitaalisten teknologioiden hyödyntäminen uudella, aikaisemmasta poikkeavalla tavalla ja organisaation tai yksilön toiminnassa.

2.2 DIGITALISAATIOSTA MAKROTASOLLA

Tarkasteltaessa digitalisaatiota ja sen vaikutuksia pk-yritysten toimintaan, on asiaa hyödyllistä lähestyä myös *makrotasolta* käsin. Makrotason digitalisaatiolla tarkoitetaan tässä yhteydessä yhteiskunnan ja sen talouden rakenteiden sekä markkinoiden muuttumista, mikä heijastuu *mikrotasolle* yksittäisten yritysten ja ihmisten käyttäytymiseen ja toimintaan. (Ilmarinen & Koskela 2015, 23.)

Euroopan Unionin tavoitteena on tukea ja varmistaa eurooppalaisten yritysten kilpailukyky globaaleilla markkinoilla ja toisaalta turvata EU-kansalaisten yksilönsuoja ja tasa-arvo. Euroopan komissio hyväksyi vuonna 2010 Euroopan digitaalistrategian osana älykkään, kestävän ja osallistavan kasvun yleistä Eurooppa 2020 -strategiaa. Digitaalistrategiassa ehdotettiin yhteensä 101 toimenpidekokonaisuutta seitsemälle eri osa-alueelle, joita ovat: 1) digitaaliset sisämarkkinat, 2) yhteensopivuus ja standardit; luottamus ja turvallisuus, 3) nopeat ja ultranopeat internetyhteydet, 4) tutkimus ja

innovaatiotoiminta, 5) digitaalinen lukutaito, 6) osaaminen ja osallistuminen sekä 7) tieto- ja viestintätekniikan hyödyt yhteiskunnalle. Näillä toimenpidekokonaisuuksilla Euroopan komissio pyrki edistämään hyvää investointiympäristöä sekä digitaalisten teknologioiden käyttöä, ja edellyttää jäsenmaiden ja niiden alueiden sitoutumista strategian toteuttamiseen. (Digital agenda for Europe: Rebooting Europe's economy 2010, 5-6.)

Euroopan digitalisaatiokehitys suhteessa erityisesti Yhdysvaltoihin ja Itä-Aasian maihin on ollut Euroopan komission suurennuslasin alla. Kehitystä vauhdittaakseen komissio esitti toukokuussa 2015 yhteensä 16 uutta lakia ja toimenpidettä sisältävän digitaalisia sisämarkkinoita koskevan strategiansa "A Digital Single Market: Bringing down barriers to unlock online opportunities".

Strategia jakautuu kolmeen pilariin, joita seuraavassa pyrin kuvaamaan erityisesti pk-yritysten näkökulmasta:

1. *"Digitaaliset tavarat ja palvelut paremmin kuluttajien ja yritysten saataville koko Euroopassa"*

EU:n komission teettämän selvityksen vain 15 % Euroopan kansalaisista tekee verkko-ostoksia muista EU-maista samalla kun vain 7 % eurooppalaisista pk-yrityksistä tekee kauppaa muihin maihin. Komission mukaan eurooppalaiset kuluttajat voisivat vuosittain säästää 11,7 miljardia euroa, mikäli heillä olisi käytettävissä ostoksiinsa koko Euroopan valikoima. Toisaalta voidaan ajatella, että kyseisellä summalla he voisivat ostaa lisää tuotteita ja palveluja, jolloin ko. rahamäärä tuottaisi lisää myyntiä alueella toimiville yrityksille. Tämänhetkiselle rajoittuneelle tilanteelle markkinoilla on olemassa monia syitä. Kielitaidollisten esteiden lisäksi korkeina pidettävät kuljetuskustannukset, kuluttajansuojaan kuten esimerkiksi virheellisten/epäsopivien tuotteiden palauttamiseen liittyvät haasteet sekä verkkomyynnissä usein käytössä olevat maarajoitukset koetaan esteiksi, jotka tulisi poistaa. Myös tekijänoikeuteen liittyvät seikat rajoittavat verkossa olevan sisällön ostamista muissa EU-maissa. (A digital single market in Europe: Bringing down barriers to unlock online opportunities 2016, 5.)

2. ”Digitaalisille verkostoille ja palveluille suotuisa toimintaympäristö”

Digitaalisen toimintaympäristön kehittämiseen liittyy myös nopeiden laajakaistayhteyksien rakentaminen koko EU:n alueelle. 4G-verkon ja –teknologian sekä valokuituverkon käyttö on levinnyt hitaasti erityisesti maaseutuympäristössä, missä pitkät etäisyydet ja harva asutus nostavat yhteyksien rakentamisen hintaa. Lisäksi taajuuspula tietyissä osissa Eurooppaa on ollut esteenä 4G-teknologian käytön leviämiselle. Seuraavan sukupolven 5G-verkkoa pidetään ratkaisevana käännekohtana sekä telealan toimijoiden, että Euroopan keskeisten toimialojen kannalta. Näiden osapuolten, sekä korkeakoulujen ja tutkimuslaitosten keskinäinen yhteistyö tulevaa 5G -verkkoa ja sen kapasiteettia hyödyntävien tuotteiden ja palvelujen kehittämisessä on Euroopan digitalisaatiokehityksen onnistumisen kannalta erittäin tärkeää. (A digital single market in Europe: Bringing down barriers to unlock online opportunities 2016, 9-10.)

Digitalisaatio kuten muutkaan yhteiskunnalliset kehitystrendit eivät valitettavasti tuo kuitenkaan pelkästään positiivisia asioita. Tietoverkoissa liikkuvan, lähes exponentiaalisesti kasvavan datan määrä on lisännyt tietoverkoissa tapahtuvien tietoturvapoikkeamien ja tietoverkoissa tapahtuvia rikoksia. Tietoverkkoturvallisuuden vaarantaneiden tapahtumien määrä kasvoi globaalisti tarkasteltuna jopa 38 % vuoden 2015 aikana ja tietoverkoissa tapahtuvan rikollisuuden taloudellinen arvo on kansainvälisessä mittakaavassa ylittänyt jo huumekaupan arvon. (A digital single market in Europe: Bringing down barriers to unlock online opportunities 2016, 13.)

Lisääntyviin tietoverkkouhkiin vastatakseen solmi Euroopan komissio 5.7.2016 yhdessä European Cyber Security Organization ABLS:n (ECSO) kanssa ns. Public-Private-Partnership –sopimuksen (PPP), jonka tavoitteena on vahvistaa Euroopan kyberturvallisuusresilienssiä sekä edistää kilpailukykyisen ja innovatiivisen kyberturvallisuusteollisuuden toimintaa (Contractual arrangement between the European Union and the European Cyber Security Organisation 2016, 3). Sopimuksessa Euroopan komissio sitoutui tukemaan kyberturvallisuuteen liittyvää tutkimusta ja tuotekehitystä yhteensä 450 M€ suuruisella rahasummalla H2020 –ohjelmasta vuoteen 2020 mennessä. ECSO puolestaan sitoutui siihen, että sen jäsenten toimenpiteiden seurauk-

sena syntyy vastaavalla ajanjaksolla yhteisarvoltaan 1,8 miljardin euron suuruiset investoinnit koko EU:n alueella. (Contractual arrangement between the European Union and the European Cyber Security Organisation 2016, 8-9.).

EU-parlamentti hyväksyi 14.4.2016 Euroopan unionin tietosuoja-asetuksen (GDPR, General Data Protection Rules, 2016/679), joka astui voimaan toukokuussa 2016 ja sen siirtymäaika päättyy 25.5.2018. Se korvaa vuonna 1995 säädetyn tietosuojadirektiivin 95/46/EC. Asetuksen vaikutuspiirissä ovat kaikkia ne yritykset ja muut organisaatiot, joiden toiminnassa syntyy yksilöiviä henkilötietoja sisältävä rekisteri tai jotka käsittelevät henkilörekisterien tietoja. Asetuksen tarkoituksena on taata kuluttajille EU:n alueella harmonisoitu yksityisyydensuoja, paremmat oikeudet valvoa henkilötietojensa käyttöä sekä oikeus vaatia niiden poistamista.

Yrityksille GDPR asettaa uusia velvoitteita tiedon elinkaaren hallinnalle. Asetuksella todistustaakka yksityisyydensuojasta siirtyy yritykselle (tai rekisterinpitäjälle), mikä käytännössä tarkoittaa kattavan dokumentaation laatimista vaatimustenmukaisuuden osoittamista varten. Asetus myös velvoittaa yrityksiä suojaamaan henkilötiedot käyttämällä moderneja tietoturvaratkaisuja. Mikäli henkilötietoihin kohdistuu tietoturvapoikkeama, on yritys velvollinen ilmoittamaan siitä tietosuojaviranomaisille 72 tunnin sisällä alkaen tietomurron uhkan havaitsemisesta. (Euroopan Parlamentin ja Neuvoston Asetus (EU) 2016/679 2016, 17.)

3. Eurooppalainen digitaalitalous ja -yhteiskunta, joilla on kasvupotentiaalia

Digital Single Market –strategiassaan Euroopan komissio esitti lukuisia toimenpiteitä, pyritään edistämään teollisuuden ja siihen liittyvien palvelujen digitalisoimista elinkeinoelämän eri toimialoilla. Yksi toimenpiteistä on eurooppalaisen pilvipalvelun perustaminen tutkijoiden sekä luonnontieteiden ja tekniikan ammattilaisten käyttöön. Palvelu toimisi varastona massadatalle, jota voitaisiin sen avulla hallita, analysoida ja käyttää uudelleen. (A digital single market in Europe: Bringing down barriers to unlock online opportunities 2016, 14.)

Myös yrityksille massadata ja sen tehokkaampi hyödyntäminen voisi tuoda merkittäviä taloudellisia hyötyjä. Euroopan komission on arvioinut, että jos massadataa käytettäisiin sadassa Euroopan suurimmassa yrityksessä, olisi mahdollista aikaansaada jopa 425 miljardin euron säästöt. Tutkimuksissa on lisäksi arvioitu, että massadatan

analysoinnilla voitaisiin lisätä EU:n talouskasvua 1,9 %, mikä tarkoittaa 206 miljardin euron suuruista lisäystä bruttokansantuotteeseen. (A digital single market in Europe: Bringing down barriers to unlock online opportunities 2016, 14.)

Julkisella sektorilla digitaalisuudesta etsitään lääkettä tuottavuuden kasvuun, palvelujen tehostamiseen ja niiden vaikuttavuuden parantamiseen. Samalla pyrkimyksenä on tasapainottaa julkista taloutta, lisätä viranomaisten yhteistyötä ja saada asiakkaiden asioiden käsittely sujuvammaksi ja ketterämmäksi. Euroopan komission mukaan julkisen sektorin ”lähtökohtaisesti digitaalinen” -strategialla olisi mahdollista saavuttaa vuositasolla jopa 10 miljardin euron säästöt. (A digital single market in Europe: Bringing down barriers to unlock online opportunities 2016, 14.)

Kansallisella tasolla digitalisaatiokehitystä koordinoidaan ja tuetaan pääministeri Juha Sipilän hallitusohjelmalla ”*Ratkaisujen Suomi*”, joka julkistettiin toukokuussa 2015. Digitalisaatio on yksi hallitusohjelman läpileikkaavista teemoista. (Ratkaisujen Suomi, Pääministeri Juha Sipilän hallituksen strateginen ohjelma 2015, 26.)

Ohjelma asettaa tavoitteekseen kymmenen (10) vuoden aikajänteellä sekä julkisten palvelujen että yksityisen sektorin tuottavuusloikan, joka on tarkoitus aikaansaada digitalisaation avulla, purkamalla turhaa sääntelyä ja byrokratiaa sekä johtamiskulttuurin kehittämisellä. Tavoitteen saavuttamiseksi perustettiin hallituskaudelle 2015-2019 viisi kärkihanketta, joiden avulla on tarkoitus saada aikaan konkreettisia edistysaskeleita. Hallituksen kärkihankkeet ovat: 1) Digitalisoidaan julkiset palvelut, 2) Rakennetaan digitaalisen liiketoiminnan kasvuympäristö, 3) Sujuvoitetaan säädöksiä, 4) Otetaan käyttöön kokeilukulttuuri, 5) Parannetaan johtamista ja toimeenpanoa. (Ratkaisujen Suomi, Pääministeri Juha Sipilän hallituksen strateginen ohjelma 2015, 26.)

Kaikilla viidellä kärkihankkeella tuetaan joko suoraan tai välillisesti myös yritysten toimintaa. Sisällöllisesti suoraan yritysten toimintaan vaikuttavalla kärkihankkeella 2) *”Rakennetaan digitaalisen liiketoiminnan kasvuympäristö”* on tarkoituksena edistää esineiden internetiä, laatia tietoturvastrategia, lisätä, robotiikan kehitystyötä ja sen hyödyntämistä sekä hyödyntää massadataa liiketoiminnan kehittämisessä. (Ratkaisujen Suomi, Pääministeri Juha Sipilän hallituksen strateginen ohjelma 2015, 27.)

Hallitusohjelman puolivälitarkastelussa toukokuussa 2017 todettiin mm. että julkisten palvelujen digitalisointia on rahoitettu 15 strategisesti merkittävällä digihankkeella. Hallitus valmistelee uuden tiedonhallintalain, jonka on tarkoitus astua voimaan vuoden 2019 alussa. Lisäksi on tarkoitus vauhdittaa digitaalisten ekosysteemien rakentumista ekosysteemifoorumi -mallilla (Ratkaisujen Suomi: Puolivälin tarkistus. Hallituksen toimintasuunnitelmavuosille 2017–2019 2017, 54-55). Kasvuympäristön edistämiseksi on vahvistettu tietoturvastrategia maaliskuussa 2016 sekä hyväksytty periaatepäätökset älykkäästä automaatiosta ja robotisaatiosta. Älykäs maaseutu -hankkeella edistetään digitalisaatiota hyödyntäviä toimintamalleja erityisesti maaseudulla. (Ratkaisujen Suomi: Puolivälin tarkistus. Hallituksen toimintasuunnitelmavuosille 2017–2019 2017, 56-57.)

Kun palvelut yhä lisääntyvässä määrin siirtyvät verkkoon, edellyttää se niiden käyttäjiltä uusia taitoja niiden hyödyntämiseksi. Tähän liittyen Euroopan komissio julkaisi kesäkuussa 2016 uuden osaamisohjelman Euroopalle (A New Skills Agenda for Europe 2016). Osaamisohjelmalla pyritään varmistamaan kansalaisten tasa-arvoa ja kehittämään niitä taitoja, joilla varmistetaan Euroopan kilpailukyky ja innovaatioiden syntyminen. Ohjelman esitöinä vuonna 2015 tehtyjen selvitysten mukaan 16-74 vuotiaista EU-kansalaisista on 45 % vailla digitaalisia taitoja tai taitotaso on alhainen. Suomen osalta ollaan taitojen osalta paremmassa tilanteessa, koska vastaava luku on 25 %. (Human Capital: Digital inclusion and skills. Europe's Digital Progress Report 2016 2016, 7.)

Osaamisohjelman tavoitteille löytyy selkeät perustelut, sillä alhaisilla digitaalisilla taidoilla on suora yhteys yksilön työllistymiseen sekä osaavan työvoiman saantiin yrityksille. Eurooppalaisista työnantajista noin 40 % ilmoittaa, että heillä on vaikeuksia rekrytoida tarvittavan digitaalisen osaamisen omaavia työntekijöitä (A New Skills Agenda for Europe 2016, 2). Tätä puoltaa myös se, että aktiivisilla työmarkkinoilla olevista EU-kansalaisista 37 % on varustettu riittämättömillä digitaalisilla taidoilla. Suomessa vastaava luku on 17 %. (Human Capital: Digital inclusion and skills. Europe's Digital Progress Report 2016 2016, 8.)

2.3 DIGITALISAATION VAIKUTUKSISTA MIKROTASOLLA PK-YRITYKSIIN

Kuten jo edellä on todettu, digitalisaatio ilmiönä vaikuttaa sekä makrotason kautta, että käytännön tasolla (mikrotasolla) lähes jokaisen yrityksen päivittäiseen toimintaan. Digitalisaatio muuttaa maailmaa peruuttamattomasti ja sopeutuakseen muutokseen ja pysyäkseen sen mukana, tarkoittaa se monelle yritykselle se tarkoittaa muutosta lähes kaikkiin liiketoiminnan perustekijöihin.

Elinkeinoelämän keskusliitto EK selvitti vuonna 2015 tekemällään kysetutkimuksella pk-yritysten toimintaedellytyksiä ja niiden toimintaan vaikuttavia muutostekijöitä. Kysymykset liittyivät kahteen teemaan: 1) Yritysten kasvu ja kansainvälistyminen sekä 2) Toimintaympäristön muutos ja yritysten uudistuminen. Kyselyyn vastasi yhteensä 492 pk-työnantajaa, jotka luokiteltiin neljään toimialaryhmään; teollisuus, rakentaminen, kauppa ja palvelut. (Pk-yritysten toimintaympäristö. Kasvu ja uudistuminen 2015, 10.)

Kyselytutkimukseen vastanneista kaikista yrityksistä 48 % arvioi digitalisaation vaikuttavan omaan toimintaansa sekä toimialaansa ”paljon” tai ”melko paljon”. Vastanneista 13 % ei osannut vastaushetkellä arvioida vaikutuksia. Toimialoittain kaupan alan yrityksistä 57 % ja palvelujen toimialoilla 54 % yrityksistä arvioi vaikutuksen olevan samaa suuruusluokkaa. Vähiten digitalisaatiolla arvioitiin olevan vaikutusta rakentamisen toimialalla, jossa 69 % vastanneista yrityksistä arvioi vaikutuksen olevan ”vähäinen” tai ”ei lainkaan”. Teollisuuden alan yrityksistä 36 % arvioi digitalisaatiolla olevan ”paljon” tai ”melko paljon” vaikutusta toimintaansa. Teollisuuden alaa edustaneista vastaajista 25 % vastasi ”ei osaa sanoa” ja 39 % heistä arvioi vaikutukset enintään ”vähäisiksi”. (Pk-yritysten toimintaympäristö. Kasvu ja uudistuminen 2015, 6.)

Yritysten työntekijämäärän mukaan tarkasteltuna on myös eroja havaittavissa. Kyselyyn vastanneista alle 10 työntekijän yrityksistä 47 % arvioi digitalisaation vaikuttavan toimintaansa ”paljon” tai ”melko paljon”. Ne yritykset, joiden työntekijämäärä oli 10-49 työntekijää oli arvioivat digitalisaation vaikutuksia lähes samalla tavalla (46 %). Sen sijaan yli 50 henkilön yrityksistä 63 % arvioi vaikutuksiksi ”paljon” tai ”melko paljon”. (Pk-yritysten toimintaympäristö. Kasvu ja uudistuminen 2015, 6.)

Myös yrityksen elinkaaren vaiheella näyttää tutkimuksen mukaan olevan merkitystä arvioitaessa digitalisaation vaikutuksia yrityksen toimintaan. Alku- tai kasvuvaiheessa olevista yrityksistä 70 % arvioi vaikutuksia olevan ”paljon” tai ”melko paljon” ja 30 % arvioi vaikutukset ”vähäisiksi” tai niitä ”ei ole lainkaan”. Merkillepantavaa alku- tai kasvuvaiheessa olevien yrityksen vastauksissa on se, että yrityksille oli muodostunut oma kantansa digitalisaatioon, jolloin ”ei osaa sanoa” -vastauksia ei esiintynyt lainkaan. (Pk-yritysten toimintaympäristö. Kasvu ja uudistuminen 2015, 6.)

Vakaan toiminnan vaiheessa olevista yrityksistä 48 % arvioi vaikutuksia olevan ”paljon” tai ”melko paljon”, 12 % ei osannut arvioida vaikutuksia ja 40 % arvioi vaikutukset korkeintaan ”vähäisiksi” Omistajanvaihdostilanteessa olevista yrityksistä 33 % arvioi vaikutuksia olevan ”paljon” tai ”melko paljon”, 26 % ei osannut arvioida vaikutusten suuruutta ja 41 % vastaajista arvioi vaikutusten olevan ”vähäisiä” tai niitä ei ilmene lainkaan. Suurehkoja eroja vastauksissa elinkaaren vaiheesta riippuen aiheuttanee todennäköisesti erot yritysten omistajien ikärakenteessa ja toisaalta se, että osa alku- tai kasvuvaiheen yrityksistä on jo lähtökohtaisesti perustettu digitalisaation hyödyntämisen varaan. (Pk-yritysten toimintaympäristö. Kasvu ja uudistuminen 2015, 6.)

2.3.1 Teknologisia kehitystrendejä

Digitalisaation teknologisia osatekijöitä voidaan tarkastella ja jaotella monilla tavoin. Manninen ym. jaottelevat teoksessaan ”Uuskasvun polut – Digitalisaation lupaus” jo kehityksessään osittain toisiinsa kytkeytyneet ja samanaikaisesti vaikuttaneet teknologiset kehityssuunnat kuuteen kokonaisuuteen, joissa kaikissa on viime vuosien aikana tapahtunut merkittäviä teknisiä ja toiminnallisia kehitysaskeleita.

Näitä teknologiatrendejä ovat:

- Massadata ja sen analytiikan kehittyminen
- Mobiiliteknologian kehitys ja mobiliteetti
- Pilvipalvelujen kehitys
- Viestinnän digitalisoituminen
- Internet of Things / Internet of Everything (IoT / IoE)
- Ohjelmistokehitys (Manninen ym. 2015, 48.)

Tarkastelen seuraavassa kutakin edellä mainituista kuudesta digitalisaatiokehityksen taustalla vaikuttaneesta tekijästä tarkemmin:

1) Massadata ja sen analytiikan kehittyminen

Datan kerääminen ja sen hyödyntäminen on yrityksille entistä helpompaa ja kustannustehokkaampaa. Suurista tietomääristä voidaan data-analytiikan ja tekoälyn avulla löytää piirteitä, joita ei inhimillisen päättelyn avulla kyettäisi löytämään. Data-analytiikan mukanaan tuomat mahdollisuudet asiakaskäyttäytymisen seurantaan ja asiakkaiden profilointiin ovat keinoja markkinoinnin uudistamiseen ja fokusointiin. Data voi olla myös kauppatavaraa, kuten Google:n kaltaisten menestyvien globaalien teknologiayritysten esimerkki osoittaa.

2) *Mobiiliteknologian kehitys ja mobiliteetti*

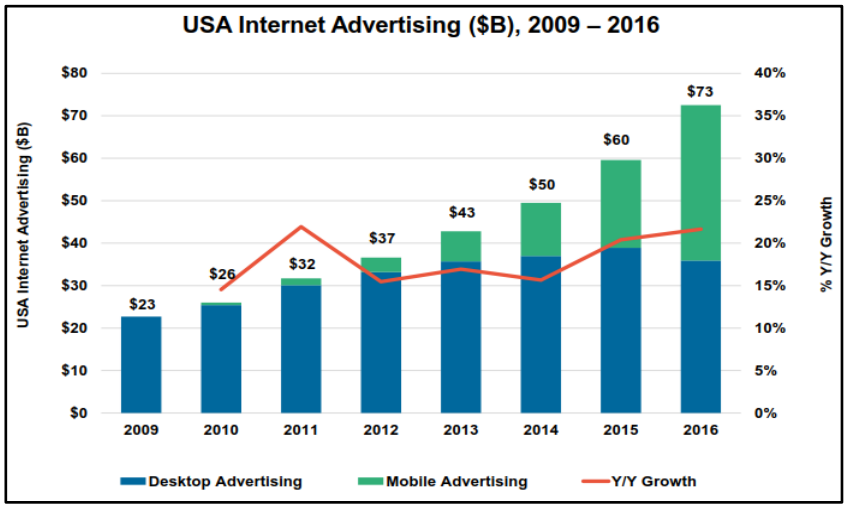
Teknologiatrendeistä mobiliteetin kehitys on yksi eniten digitalisaation vaikuttavista tekijöistä. Mobiiliverkkojen ja niissä käytettävien teknologioiden kehitys sekä mobiililaitteiden teknologinen kehitys ovat ”ruokkineet” toistensa kasvua. Mobiliteetin kehitystä hyvin kuvaava mobiilidatan määrän kasvu on ollut erittäin nopeaa ja se tulee myös sellaisena jatkumaan, kuten Cisco julkaisussaan Global Mobile Data Traffic Forecast Update 2016–2021 kuvion 1 mukaan ennustaa (Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–2021. White Paper 2107, 5.)

KUVIO 1: Globaali mobiilidatan määrän ennuste alueittain (Cisco VNI Mobile 2017)

Dataliikenteen kasvuun eniten vaikuttavana tekijänä on ollut erityisesti älypuhelinten ja muiden mobiiliverkkoon liitettävien laitteiden määrän käytön lisääntyminen. Mobiililaitteiden valmistajien välinen teknologiakilpajuoksu on omiaan edesauttamaan

laitteiden määrän lisääntymistä. Niiden kehittynyt käytettävyys yhdistettynä älykkäisiin mobiiliapplikaatioihin vaikuttaa niiden käytön määrään.

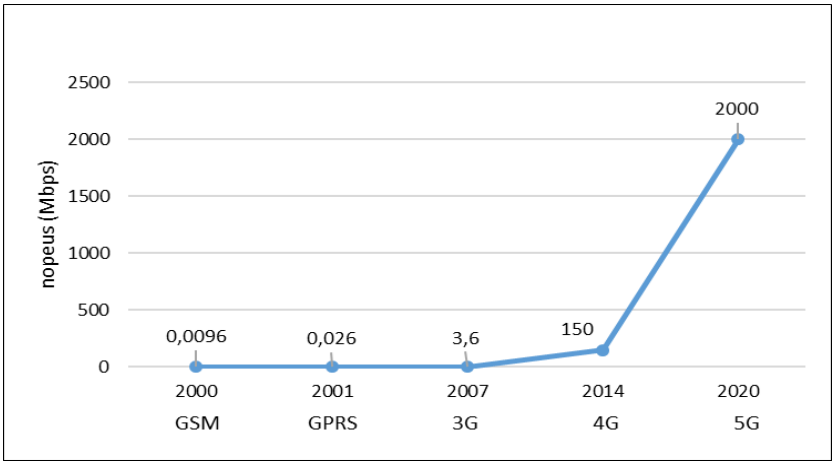
Mobiliteetin ja sen mukana myös mobiilidatan määrän kasvuun vaikuttaa laitteiden määrän lisäksi myös useat muut tekijät. Internetissä tapahtuva mainonta on yhä enemmän optimoitu mobiililaitteille, kuten kuviossa 2 oleva esimerkki USA:n internetmarkkinoinnin kehityksestä osoittaa (Meeker2017, 12). Samalla sen rakenne ja sisältö ovat sopeutuneet ja kehittyneet tukemaan mobiliteettia. Mainonnasta on tullut entistä reaaliaikaisempaa sekä interaktiivisempaa, siinä hyödynnetään enemmän videoita ja vähemmän tekstiä.



KUVIO 2. Internet-markkinoinnin kehitys USA:ssa vuosina2009-2013 (IAB/PWC Internet Advertising Report 2016)

Mainonnan ja kaupankäynnin lisäksi sekä yksityishenkilöiden että yritysten ja muiden organisaatioiden viestintä tapahtuu lisääntyvässä määrin mobiilisti. Osa yritysten asiakaspalvelusta on jo siirtynyt mobiiliratkaisuihin ja myös julkisella sektorilla, kuten esimerkiksi terveydenhuollossa, tavoitellaan merkittäviä kehitysaskeleita mobiilipalveluihin lähivuosien aikana. Yhä useamman yrityksen toiminnanohjaus perustuu mobiiliapplikaatioihin ja –laitteisiin. Niiden avulla saadaan toimintaprosesseja virtaviivaistettua ja nopeutettua mahdollisimman reaaliaikaisiksi. Tällä saavutetaan myös kustannussäästöjä ja turvataan kilpailukykyä. Myös maksuliikenne on jo osittain muuttunut mobiiliksi turvallisen teknologian kehittymisen myötä, jolloin käteismuodossa liikkeellä olevan rahan määrä vähenee.

Tietoverkkojen kehityksessä suurimmat harppaukset on tehty mobiiliverkoissa, joiden tiedonsiirtonopeudet ja –kapasiteetti on kasvanut räjähdysmäisesti. Verkkojen kehitys onkin ollut yksi perusedellytys mobiili- ja älylaitteiden määrän ja käytön lisääntymiselle ja niitä hyödyntävien palvelujen lisääntymiselle. Suomalainen teleoperaattori Elisa ja sen edeltäjät ovat olleet alusta saakka mukana rakentamassa maahamme mobiiliyhteyksiä. Kuviossa 3 osoitetaan Elisan näkökulmasta mobiiliverkkojen tiedonsiirtonopeuden kehitystä 2000-luvulla (Tavoitteena maailman paras verkko. 2018).



KUVIO 3: Latausnopeuden kehitys teleoperaattori Elisan mobiiliverkoissa (Elisa 2018)

Suomessa on Tilastokeskuksen vuosittain tekemän kyselytutkimuksen mukaan kosketusnäytöllisten älypuhelinten määrä kasvanut noin 5 % vuosivauhtia aikavälillä 2013-2017. Sitä ennen vuotuinen kasvu oli vieläkin nopeampaa. Vuoden 2017 tutkimuksen mukaan kolmella neljästä oppivelvollisuusiän ylittäneestä henkilöstä oli omassa käytössään älypuhelin. Heistä noin 10 % ei käyttänyt älypuhelintaan internetyhteyksiin. Älypuhelimen käytön yleisyys on lähes yhtäläistä sekä miesten että naisten keskuudessa. (Väestön tieto- ja viestintätekniikan käyttö 2017. 2. Internetin käyttö mobiililaitteilla 2017, 7.)

Yhteenvetona voidaan todeta, että jo tällä hetkellä mobiliteetti on helpottanut ja nopeuttanut toimintaprosesseja lähes kaikilla toimialoilla ja se myös mahdollistaa yhä useammassa työtehtävässä ajasta ja paikasta riippumattoman töiden tekemisen, ostamisen ja sähköisten palvelujen käytön.

3) Pilvipalvelujen kehitys

Pilvipalvelut ovat tietotekniikkapalveluja, joita käytetään verkkopalveluina internetissä. Niillä pyritään aikaansaaman aina saavutettavissa oleva, kapasiteetiltaan riittävä tietovarasto ja sen käyttöön tarvittavat palvelut yksityisen kuluttajan tai yrityksen käyttöön. Koska pilvipalvelun käyttöönotto ei edellytä mittavia tila- ja laiteinvestointeja, on käyttöönoton taloudellinen kynnys matala. Toimiakseen tehokkaasti, tulee palvelun käyttöä varten olla läpäisykykyiset tietoverkot ja tehokkaat, varmennetut datakeskukset. Palvelut ovat yleensä luonteeltaan käyttötarpeen mukaan skaalautuvia ja niistä maksetaan palveluntuottajalle käyttöä vastaava korvaus.

Tilastokeskuksen tekemän ”Tietotekniikan käyttö yrityksissä 2017” – tutkimuksen mukaan Suomessa käyttää maksullisia pilvipalveluja 66 % kaikista yrityksistä. Toimialojen välillä on melko suuria vaihteluja, sillä informaation ja viestinnän toimialalla käyttäjiä on peräti 87 % yrityksistä, kun taas kuljetus- ja varastointialoilla vastaava luku on 45 %. Lähes yhtä suurta oli vaihtelu tarkasteltaessa käyttöä yrityskoon mukaan. Suurinta pilvipalvelujen käyttö oli yli 100 henkilöä työllistävissä yrityksissä, joista 86 % käytti pilvipalveluja, kun taas 10-19 työntekijän yrityksistä palveluja käytti 59 %. (Tietotekniikan käyttö yrityksissä 2017, 12.)

Tutkimuksessa kysytyistä pilvipalveluja eniten yritysten käyttämiä olivat sähköposti (76%) sekä tiedostojen tallentaminen (63%). Yli puolet vastanneista yrityksistä käytti toimisto-ohjelmia (57 %) tai kirjanpitoon käytettäviä sovelluksia (51%). Pilvipalveluissa toimivia tietokantoja oli 45 % yrityksistä ja CRM-ohjelmistoja käytti vastanneista kolmasosa. Pilvipalveluissa tarjolla olevaa laskentatehoa hyödynsi vastanneista yrityksistä vain 16 %. (Tietotekniikan käyttö yrityksissä 2017, 13.)

4) Viestinnän digitalisoituminen

Digitaalinen viestintä on kehittynyt ja muuttanut muotoaan jättiharppauksin. Modernia teknologiaa hyödyntävä sosiaalinen media nykymuodossaan mahdollistaa viestien jakamisen ja välittämisen sekunnin murto-osassa ympäri maapalloa oleville seuraajille/vastaanottajille. Viestintä myös mobiililaitteilla on nopeaa, helppoa ja kustannuksiltaan hyvin edullista.

Yritysten näkökulmasta viestinnän digitalisoituminen on suuri mahdollisuus tuoda ja saada esille tuotteita ja palveluja markkinoille reaaliajassa rakentamalla joustavia

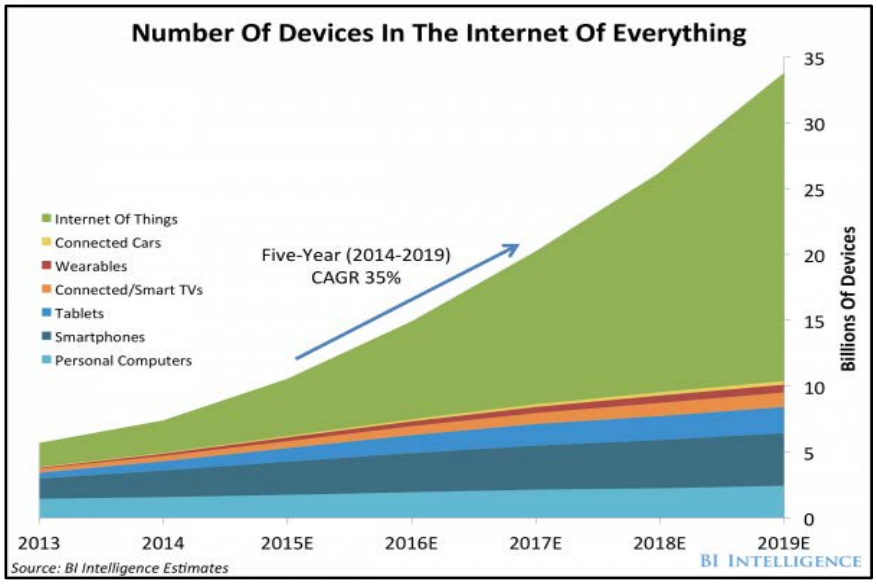
markkinointikampanjoita ja tukemalla yrityksen imagoa potentiaalisten asiakkaiden, yhteistyökumppaneiden tai työntekijöiden hankkimiseksi. Digitaalisuus mahdollistaa myös uusien toimintamallien kehittämisen suhteessa asiakkuuksien hoitamiseen koko tilaus-toimitusprosessin aikana sekä koko arvoketjussa.

Tilastokeskuksen vuonna 2017 tekemän tutkimuksen mukaan on sosiaalisen median käyttö yrityksissä lisääntynyt merkittävästi. Tutkimukseen vastanneista vähintään kymmenen henkilöä työllistävistä yrityksistä sosiaalista mediaa ilmoitti käyttävänsä 63 % (Tietotekniikan käyttö yrityksissä 2017, 1). Sosiaalisen median tyypeistä erityisesti yhteisöpalvelujen (kuten Facebook tms.) käyttö on viiden viimeksi kuluneen vuoden aikana lähes kaksinkertaistunut. Vuonna 2013 vähintään kymmenen henkilöä työllistäneistä yrityksistä sitä käytti 34 %, kun vuonna 2017 vastaava luku oli jo 61 %. (Tietotekniikan käyttö yrityksissä 2017, 10.)

Tutkimuksen mukaan sosiaalista mediaa käytetään yleisimmin informaation ja viestinnän toimialojen yrityksissä, joista 95 % ilmoittaa käytöstään. Vähiten käyttäjiä (42 %) löytyy rakennusalan yritysten keskuudesta. Yritysten työntekijämäärän mukaan tarkasteltuna käyttöaste on pienimmillään 58 % yrityksissä, jotka työllistävät 10–19 henkilöä. Sosiaalisen median käyttö on suurinta yli 100 henkilöä työllistävissä yrityksissä, joista 86 % ilmoitti sitä käyttävänsä. (Tietotekniikan käyttö yrityksissä 2017, 9.)

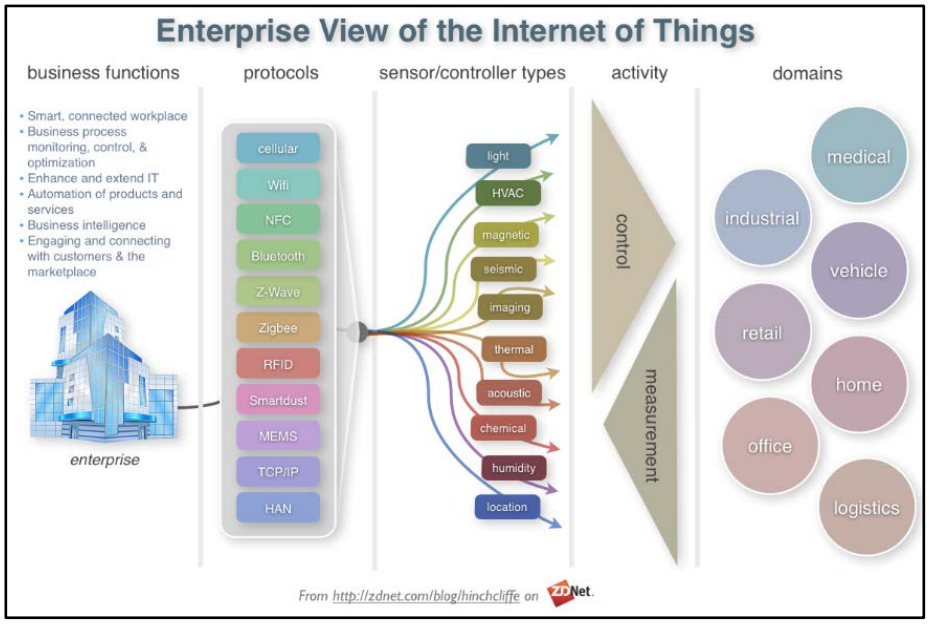
5) Internet of Things / Internet of Everything (IoT / IoE)

Esineiden Internet, teollinen internet, M2M, Internet of Everything ovat kaikki nimityksiä teknologiatrendille, jossa tietoverkkoihin kytkettävien laitteiden määrä on kasvanut ja edelleen kasvaa räjähdysmäisesti, kuten kuviossa 4 osoitetaan (Internet of Things Market Statistics – 2015 IoT stats. 2015). Nimitysten erona on useimmissa tapauksissa se, kuinka paljon laitteiden tuottamaa dataa tuotetaan ja ohjataan analytiikan ja automaation avulla. Esineiden internet (IoT) on nopeasti vakiintumassa sekä kuluttaja- että yritystoiminnassa. Yhä useampi näinä päivinä markkinoille ilmestyvä uusi digitaalinen laite sisältää valvovan tai ohjaavan sovelluksen, kiinteistöautomaatio sekä etäohjattavat kodinkoneet lisääntyvät ja lähes kaikki uudet sähköiset laitteet digitalisoituvat liitettäväksi 24/7-periaatteella Internetiin.



KUVIO 4: Internetiin kytkettyjen IoT-laitteiden määrän kehitys 2013-2019 (Ironpaper 2015)

Kehitystrendinä IoT:tä voidaan tarkastella sekä yritysten että kuluttajien näkökulmasta. IoT on ollut jo pitkään käytössä yritysten toiminnassa ja sitä on menestyksekkäästi hyödynnetty osana liiketoimintaa. Parhaan hyödyn yksittäinen yritys saa siitä silloin, kun päätös IoT:n kuten muidenkin uusien teknologioiden käytöstä täysin perustuu yrityksen liiketoimintastrategiaan ja siihen ollaan valmiita panostamaan riittävät voimavarat. Dion Hinchcliffe, joka toimii pääanalyytikkona Constellation Research –tutkimuslaitoksessa kuvaa blogitekstissään IoT:n yritysnäkökulmaa alla olevan kuvion 5. mukaan (Hincliffe 2014). Se osoittaa selkeästi, että käytettävät protokollat ja teknologiat tulee suunnitella ja rakentaa liiketoimintalähtöisesti, jotta ne mahdollisimman hyvin palvelisivat sitä.



KUVIO 5: IoT:n yritysnäkökulma *(Zdnet 2014)*

Kuluttajien näkökulma on useille vielä uusi ja vieras. Mediassa on toki jo pitkään puhuttu älykodeista ja siitä, että niissä monet kodinkoneet, kuten esimerkiksi leivänpaahtimet, jääkaapit ja lämmitysjärjestelmien ohjausyksiköt liitetään internetiin. Näin varmasti tulee lisääntyvässä määrin tapahtumaan sitä mukaa, kun kuluttajat kokevat saavansa siitä todellista lisäarvoa, kuten esimerkiksi säästönä energiankulutuksessa. Alla olevassa taulukossa 1 kuvattu kodinkoneiden liittämistä internetiin sekä yrityksen että kuluttajan näkökulmasta. Kun liitettävyydestä saadaan molemmille osapuolille riittävä tunnistettu lisäarvo, on se hyvä lähtökohta kestävälle uusien palvelujen ja liiketoiminnan kehittämiselle. (Tollefson 2016)

TAULUKKO 1: Kodinkoneiden internetiin liittämisen tuoma lisäarvo kuluttajalle ja valmistajalle (Tollefson 2016.)

Kuluttaja
Laitteen käytönajoitus edullisimmilla energiahinnoilla
LVI-järjestelmien automaattinen ohjaus älypuhelimen GPS-paikkatiedolla
Kodinkoneiden etäohjaus ja asetusten muuttaminen älypuhelimen sovelluksella
Bluetooth Smart-majakoista vuorovaikutustietoa automaattisesti
Pilvisovellukset antavat käyttösuosituksia ja tietoa kodinkoneen käytön kehityssuunnasta
Laitevalmistaja
Tiedonkeruu laitteen toimintojen seuraamiseen
Laitteen käyttöön liittyvien kulutustarvikkeiden automaattimarkkinointi
Vikatilanteiden tunnistus ja huoltotoimien ehdotus
Etädiagnostiikan avulla vähemmän huoltokäyntejä
Kerätään tietoa kodinkoneen toimintojen käytöstä tutkimus- ja kehitystyön optimoimista varten

6) Ohjelmistokehitys

Digitalisoituva talous tuo mukanaan merkittäviä liiketoimintamahdollisuuksia sekä kiihdyttää taloudellisia ja sosiaalisia murroksia. Lähes kaikki digitaalisen talouden palvelut ja tuotteet ovat ohjelmistopohjaisia. Ohjelmistotuotannon on muutosvauhdissa pysyäkseen ollut luovuttava perinteisistä tavoista suunnitella ja rakentaa ohjelmistoja ja integroida niitä toisiinsa. Nykypäivänä ohjelmistointensiivisillä yrityksillä on oltava reaaliaikainen tietoon käyttäjien valinnoista ja riittävä ymmärrys asiakkaiden tarpeesta. Lisäksi niillä tulee olla valmius ja kyvykkyys tehdä nopeita kokeiluja uusilla liiketoiminta-alueilla.

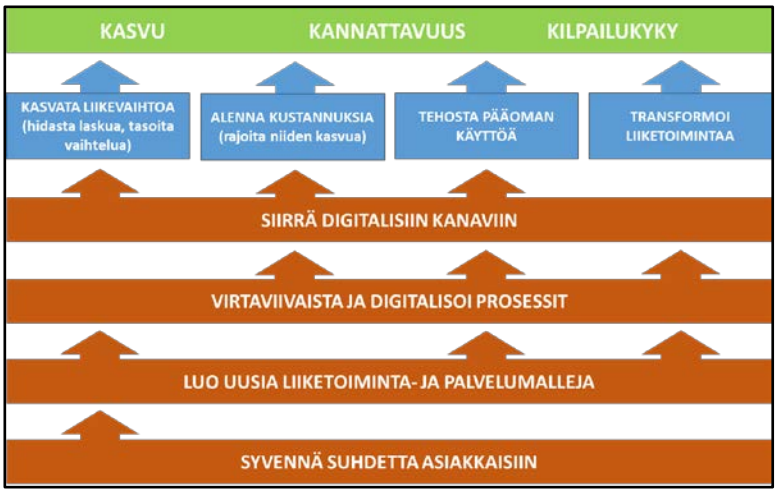
Viime vuosien suurin kehitysaskel ohjelmistokehityksessä on saavutettu kehityssyklejä nopeuttamalla ja reaaliaikaista asiakaspalautetta hyödyntäen. Internet-talouden keskeinen konsepti on ajatus vähimmäiskelpoisesta tuotteesta (MVP - minimum viable product) tai palvelusta, jolla pyritään määrittelemään pienin mahdollinen asiakkaalle lisäarvoa tuova toteutus. Kun siihen perustuvaa tuotetta tai palvelua tuotetaan, keskitytään alkuperäisen tuotteen tai palvelun ominaisuuksien parantamiseen. Tämä toimintamalli mahdollistaa jokaisen kehityssyklin lyhentämisen, edistymisen arvioinnin sekä asiakkaiden palautteen ja näkemyksen käyttämisen tuotteen ja sen kehitysvaiheiden arvon mittaamiseen. Myös avoimen lähdekoodin hyödyntämisen lisääntyminen on merkittävässä määrin toiminut ohjelmistoprojektien kehitysnopeutta lisäävänä ja kustannustasoa alentavana tekijänä.

Yrityksille on meneillään olevan liiketoiminnan muutoksen päätavoitteena luoda kestävä perusta seuraavan sukupolven kilpailukykyiselle strategialle ja toimintaprosesseille, joilla yhdessä kyetään vastaamaan nopeasti muuttuvan toimintaympäristön olosuhteisiin. Yritysten on pystyttävä tuottamaan arvoa reaaliajassa ja sopeutumaan radikaalisti uusiin liiketoimintaolosuhteisiin ja mahdollisuuksiin myös olemassa olevien liiketoiminta-alueiden ulkopuolella. Tämä lähestymistapa edellyttää yrityksissä uusia johtamismenetelmiä ja -tyylejä sekä perusteellista uudelleenarviointia siitä, miten voidaan jatkuvasti parantaa ja kehittää olemassa olevaa liiketoimintamallia. Tämä tarkoittaa myös sitä, että yrityksissä on oltava valmius yksittäisen tuotteen tai palvelun sijaan tarkastella myös koko organisaation toimintatapoja ja liiketoimintamallia ja tarvittaessa jopa muuttaa yrityksen identiteettiä ja tarkoitusta. Esimerkiksi

useat perinteiset televiestintälaitteiden toimittajat täydentävät tarjontaansa palveluilla ja liittymällä sisällöntuottajiin. Tässä toimintamallissa ollaan digitaalisen talouden ytimessä.

2.3.2 Yritysten kokemuksia digitalisaatiosta

Yritysten näkökulmasta digitalisaatio on useimmilla toimialoilla kasvun mahdollistaja, koska sen avulla on mahdollista kehittää ja uudistaa nykyisiä toimintaprosesseja ja tuotteita sekä palveluja. Sen mukanaan tuomia keinoja esittää oleva kuvio 6, joka on mukailtu Ilmarinen & Koskelan teoksesta Digitalisaatio Yritysjohdon käsikirja (Ilmarinen & Koskela 2015, 31).



KUVIO 6. Liiketoiminnan kehittäminen digitalisaation keinoin (Ilmarinen & Koskela 2015.)

Monessa yrityksessä digitalisaation merkitystä ei vielä syystä tai toisesta nähdä edellä olevan kuvion osoittamassa laajuudessa. Osa yrityksistä mieltää digitaalisuuden tarkoittavan toiminnassaan lähinnä joidenkin työtä helpottavien ja tehostavien digitaalisten työkalujen käyttöönottoa.

Tässä opinnäytetyössä tehtävän tutkimuksen kohdejoukkona on pääasiassa mikro- ja pienyrityksiä. Taustoittaakseni nimenomaan pienyritysten kokemuksia digitalisaatiosta perehdyin Suomen Yrittäjien kesäkuussa 2016 julkaisemaan, Owal Group Oy:llä teettämään selvitykseen ”Digitaalisesti suuntautuneiden pienten yritysten menestystekijät”. Sitä varten tehdyssä tutkimuksessa haastateltiin 34 pääosin nuoren pienyrityksen edustajaa. Yrityksistä kolme toimi paikallisesti tai alueellisesti, 20 yritystä toimi valtakunnallisesti ja 11 kansainvälisesti. (Digitaalisesti suuntautuneiden pienten yritysten menestystekijät 2016, 7.)

Vastaustensa perusteella pienyritykset tyypiteltiin kolmeen ryhmään lähinnä sillä perusteella, mikä on digitaalisuuden merkitys yrityksen liiketoiminnalle (Digitaalisesti suuntautuneiden pienten yritysten menestystekijät 2016, 4).

1) ”*Diginatiivit yritykset*”, joilla koko ansaintamalli perustuu digitaalisuuteen. Niiden osuus haastatelluista yrityksistä oli 59 %. (Digitaalisesti suuntautuneiden pienten yritysten menestystekijät 2016, 10.)
2) ”*Digikiinnostuneet yritykset*”, joilla jokin osa liiketoiminnasta perustuu digitalisuuteen tai digitalisuutta käytetään merkittävästi liiketoiminnan tukena. Yritykset ovat kiinnostuneita liiketoiminnan kehittämisestä digitaalisuuden suuntaan. Niiden osuus haastatelluista yrityksistä oli 32 %. (Digitaalisesti suuntautuneiden pienten yritysten menestystekijät 2016, 11.)
3) ”*Digireaktiiviset yritykset*” näkevät digitalisoitumisen pakollisena liiketoiminnan ylläpitämiseksi toimintaympäristön muuttuessa, mutta näkevät sen mahdollisuutena liiketoiminnan tehostamiseksi. Niiden osuus haastatelluista yrityksistä oli 9 %. (Digitaalisesti suuntautuneiden pienten yritysten menestystekijät 2016, 12.)

Digitaalisuuden merkittävimmäksi hyödyksi nousi selvityksen mukaan yritystoiminnan kannattavuuden paraneminen ja liiketoiminnan tehostuminen ainakin jollakin sen osa-alueella. Tätä mieltä oli 60 % Diginatiiveista yrityksistä ja 2/3 Digikiinnostuneista yrityksistä. Digitaalisuudesta nähdään näissä molemmissa ryhmissä olevan hyötyä yhteistyössä sekä asiakkaiden että yhteistyöverkoston kanssa. Molemmat ryhmät kokevat saaneensa digitaalisuuden avulla uusia liiketoimintamahdollisuuksia ja asiakkuuksia, joista osa on kansainvälisiä. Lisäksi molemmat ryhmät sitä mieltä, että niillä olisi digitaalisuuttaan edelleen kehittämällä mahdollisuus luoda uutta tai tehostaa nykyistä liiketoimintaa. (Digitaalisesti suuntautuneiden pienten yritysten menestystekijät 2016, 12.)

Selvimpänä erona näiden kahden yritystyypin välillä suhtautumisessa digitalisaatioon on se, että Diginatiivien yritysten tavoitteena on tuoda digitaalisuudella suoraa lisäarvoa asiakkailleen samalla kun Digikiinnostuneet yritykset tavoittelevat välitöntä hyötyä nimenomaan itselleen. (Digitaalisesti suuntautuneiden pienten yritysten menestystekijät 2016, 27-28.)

Kolmannelle yritystyypille eli Digireaktiivisille yrityksille digitaalisuus on haastattelujen perusteella tuonut hyötyä kaikille liiketoiminnan osa-alueille mm. uusien asiakasryhmien, parantuneen asiakaspalvelun sekä liiketoimintaprosessien tehostumisen myötä. Digitaalisuus nähdään yrityksissä kuitenkin lähinnä työvälineenä, jota ei ole nostettu strategisen ajattelun tasolle. (Digitaalisesti suuntautuneiden pienten yritysten menestystekijät 2016, 28.)

”Digitaalisesti suuntautuneiden pienten yritysten menestystekijät” –selvitykseen haastatellut yritykset kokevat digitalisaatiosta olevan vain vähän haittoja. Suurimmaksi haitaksi mainittiin tietohallintoon ja tietoturvaan liittyvät haasteet, joita 25 % haastatelluista piti tietoturvariskinä ja lähes puolet prosessiriskinä. Esimerkkeinä haasteista voidaan mainita yhteysongelmat tietoverkkoon tai pilvipalveluihin. Liiketoiminnan digitalisointi edellyttää yrityksiltä teknisten investointien lisäksi resursseja myös osaamisen ja uuden liiketoiminnan kehittämiseen ja kehittämistarpeiden perustelemiseen henkilökunnalle ja asiakkaille. (Digitaalisesti suuntautuneiden pienten yritysten menestystekijät 2016, 14.)

Vaikka edellä kuvattu selvitys onkin otokseltaan pieni, eikä sen perusteella voi vetää suuria johtopäätöksiä, osoittaa se suuntaa pienyritysten tilanteesta ja näkökulmista digitalisaation suhteen.

Kauppakamariryhmä järjesti vuonna 2013 keskisuurten yritysten johdolle suunnatun digitalisaatiokiertueen 10 eri paikkakunnalla Suomessa. Kiertueen aikana tarjoutui tilaisuuksia käydä vuoropuhelua yritysjohtajien kanssa ja selvittää miksi suomalaisten yritysten digitalisaation hyödyntäminen on hidasta. (Lakaniemi 2014, 3.)

Paikkakuntakohtaisissa keskusteluissa korostui kunkin alueen elinkeinorakenne ja erityisesti ICT-alan yritysten osuus alueen yrityskannasta. Kiertueen tilaisuuksissa käytyjen keskustelujen perusteella näyttää siltä, että digitalisaation keskisuurille yrityksille tuomat hyödyt ja edut ovat yhdensuuntaisia em. Suomen Yrittäjien selvityksessä pienyritysten esille nostamien asioiden kanssa. Kiertueen tuloksista koottu ”Digitalisaatio keskisuurissa yrityksissä” –niminen raportti julkaistiin Liikenne- ja viestintäministeriön julkaisuna 14/2014. Raportin mukaan yritykset korostivat seuraavia digitalisaation hyötyjä (+) ja haasteita (-):

+ Digitalisaatio koetaan mahdollisuutena rakentaa suhteellista kilpailuetua sekä jalostaa ja hyödyntää tietoa uusilla tavoilla. Se tukee myös uusien hybridituotteiden eli fyysisen tuotteen ja palvelun sisältämien kokonaisuuksien tuomista markkinoille. (Lakaniemi 2014, 18.)

+ Kehittyvä teknologia mahdollistaa uusia, tuottavuutta edistäviä liiketoimintatapoja ja on siten kasvun mahdollistaja. (Lakaniemi 2014, 18.)

+ Digitalisaatio edesauttaa yrityksiä pääsemään kansainvälisille markkinoille, koska yrityksen sijainnin merkitys vähenee. Tässäkin asiassa teknologia on vain väline, onnistuminen edellyttää kykyä ja osaamista verkottua ja markkinoida kansainvälisesti. (Lakaniemi 2014, 18.)

- Yritysten johdon on ymmärrettävä digitalisaation mahdollisuudet koko yrityksen liiketoiminnan kannalta ja tarkasteltava sen tuomia potentiaalisia hyötyjä sekä sisäisten että ulkoisten liiketoimintaprosessien (koko arvoketju) näkökulmista. (Lakaniemi 2014, 18.)

- Digitalisoituminen vaatii riittävän sekä joustavan kapasiteetin omaavia ja toiminnaltaan varmistettuja tietoliikenneyhteyksiä myös pienemmillä paikkakunnilla. Niiden puuttuminen on esteenä/hidasteena yritysten investoinneille siirryttäessä uusiin teknologioihin ja liiketoimintatapoihin. (Lakaniemi 2014, 11.) Investointeja vaikeuttaa joillakin alueilla yhteisen ymmärryksen vähyys laite-/ohjelmistotoimittajien ja yritysten johdon välillä (Lakaniemi 2014, 12).

- ICT-palveluihin liittyvän tietoturvan taso nousi yhdessä tilaisuudessa yhdeksi keskeisistä digitalisaation haasteista, mutta koko kiertueella sitä ei haasteeksi tunnistettu (Lakaniemi 2014, 15).

Merkillepantavaa, mutta kuitenkin tuolle aikakaudelle (vuodet 2013-2015) ominaista oli se, että yritysten huoli tietoturvasta ja –suojasta oli molempien edellä kuvattujen selvitysten mukaan vielä melko alhainen, osittain varmasti johtuen digitalisoitumisen alkuvaiheesta monien yritysten kohdalla. Toisin kuin monet muut liiketoiminnan haasteet, tietoverkkojen ja muun digitaalisen toimintaympäristön turvallisuuden riskienhallinta on edelleen haaste, johon ei ole saatavissa helppoa ratkaisua. Riittävän tietoisuuden hankkiminen toimintaympäristöön sisältyvistä uhkista ja niiden vaiku-

tuksista liiketoimintaan on ensimmäinen askel tällä tiellä. Vaikka monet palvelun-tuottajat tarjoavatkin selvityksiä tietoverkkojen uhkista, on pk-yrityksille ja niiden ”kielelle” sopivaa materiaalia auttamaan liiketoiminnan hallintaa suhteessa tieto-verkkoturvallisuuteen kuitenkin vain vähän olemassa.

Yrityksissä on olemassa lukuisia mahdollisia haavoittuvuuksia, kuten organisatoriset, tekniset, inhimilliset ja fyysiset tekijät. Ilman oikeanlaista käsitystä haavoittuvuuk-sista, uhkista ja niihin liittyvistä riskeistä voivat yritykset tuhlata voimavarojaan pyrki-myksissään lieventää kyberturvallisuusriskejään. Koska teknologiaympäristö ja uhkien vektorit muuttuvat jatkuvasti, on tiedostettava, ettei absoluuttista turvallisuutta voida ponnisteluista huolimatta koskaan saavuttaa.

Suomessa oli Tilastokeskuksen mukaan vuonna 2016 yhteensä lähes 356 790 yritystä, joista 99 % oli alle 50 henkilöä työllistäviä yrityksiä. Pk-yritysten (>250 työntekijää) osuus kaikkien yritysten kokonaisliikevaihdosta oli samana vuonna 59 %. Kun otetaan lisäksi huomioon, että pk-yritykset muodostavat merkittävän osan suuryritysten toi-mittajaverkostosta, on pk-yritysten kyberturvallisuudella kriittinen merkitys paitsi pk-yritysten itsensä kannalta, myös kansallisen kyberturvallisuuden kannalta tarkastel-tuna. (Yritykset 2016. 2017.)

3 KYBERTURVALLISUUDEN NYKYTILAA YRITYKSISSÄ

3.1 KYBERTURVALLISUUS KÄSITTEENÄ

Digitalisaatio pitää sisällään monen muun globaalin ilmiön tavoin sekä positiivisia että negatiivisia piirteitä. Edellä todettiin digitalisaation olevan yrityksille ja muille toimijoille suuri mahdollisuus kehittää ja tehostaa toimintaansa ja kilpailukykyään. Toisaalta se on myös uhka sen vuoksi, että se kiristää kilpailua ja tekee kilpailusta kansainvälisempää kuin aikaisemmin. On käynnissä globaali kilpajuoksu siitä, kuka onnistuu hyödyntämään digitalisaation nopeimmin ja tehokkaimmin.

Yksi digitalisaation suurimmista varjopuolista ovat lisääntyneet tietoturvauhkat ja –rikokset, jotka valitettavasti ovat arkipäivää jo useimmilla toimijoilla. Esimerkiksi vuonna 2015 tietoturvatapahtumien määrä Euroopassa nousi 38 %. Samana vuonna 80 % eurooppalaisista yrityksistä kohtasi vähintään yhden tietoturvatapahtuman. Eu-roopan kansalaisista 86% uskoo, että kyberrikollisuuden aiheuttama riski kasvaa. Maailmanlaajuisesti tarkasteltuna kyberhyökkäysten arvioidaan aiheuttavan yli 400

miljardin euron kustannukset joka vuosi. Euroopan kyberturvallisuusstrategia julkistettiin vuonna 2013. (Reform of cyber security in Europe. 2018.)

Tässä opinnäytetyössä jo aiemmin esiintynyt sana ”kyberturvallisuus” on tässä muodossaan terminä vielä melko nuori, sillä se on maassamme noussut julkiseen keskusteluun vasta kuluvan vuosikymmenen aikana. Joulukuussa vuonna 2010 Suomen puolustusministeriö julkaisi Valtioneuvoston periaatepäätöksen ”Yhteiskunnan turvallisuusstrategia 2010”. Kyseessä oli ensimmäistä kertaa vuonna 2003 julkaistun Yhteiskunnan turvallisuusstrategian kolmas päivitys. Siinä termiä ”kyberturvallisuus” ei vielä lainkaan esiinny. mutta siinä määritellään termiä ”*kyberuhka*” seuraavasti:

> *Termi on vielä kansallisissa käytännöissä vakiintumaton. Tässä strategiassa sitä käytetään kuvaamaan uhkaa, joka liittyy toisistaan riippuvaisiin verkostoihin, sisältäen erilaiset tieto- ja tiedonsiirtoverkot, internetin, puhelinverkot, tietokonejärjestelmät sekä kriittisen tuotannon sulautetut prosessorit ja kontrollointilaitteet.* (Valtioneuvoston periaatepäätös. Yhteiskunnan turvallisuusstrategia 2010, 86.)

Tekstin seassa ja kaavioissa ”kyberuhka” -sanaa kuvataan myös muodossa ”*tietoliikenteen ja tietojärjestelmien vakavat häiriöt*” (Yhteiskunnan turvallisuusstrategia 2010, 86).

Termiä ”kyberturvallisuus” on kansainvälisesti määritelty useiden eri tahojen toimesta, mutta täysin eksaktia yhteistä määritelmää ei ole vielä - osittain ilmiön monimuotoisuudesta johtuen - onnistuttu esittämään. Vuonna 2013 julkaistu *Suomen kansallinen kyberturvallisuusstrategia* määrittelee ”kyberturvallisuus”-termiä sitä avaavine tarkennuksineen seuraavasti:

> *Kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan.*
>
> *Tarkennus 1: Tavoitetilassa kybertoimintaympäristöstä ei aiheudu vaaraa, haittaa tai häiriötä sähköisen tiedon (informaation) käsittelystä riippuvaiselle toiminnalle eikä sen toimivuudelle.*
>
> *Tarkennus 2: Luottamus kybertoimintaympäristöön perustuu siihen, että sen toimijat toteuttavat tarkoituksenmukaisia ja riittäviä tietoturvallisuusmenettelyjä (”yhteisöllinen tietoturva”). Menettelyjen avulla pystytään estämään tietoturvauhkien toteutuminen, ja niiden mahdollisesti toteutuessa estämään, lieventämään tai sietämään niiden vaikutuksia.*

> *Tarkennus 3: Kyberturvallisuus käsittää yhteiskunnan elintärkeisiin toimintoihin ja kriittiseen infrastruktuuriin kohdistuvat toimenpiteet, joiden tavoitteena on saavuttaa kyky ennakoivasti hallita ja tarvittaessa sietää kyberuhkia ja niiden vaikutuksia, jotka voivat aiheuttaa merkittävää haittaa tai vaaraa Suomelle tai sen väestölle.* (Suomen kyberturvallisuusstrategia 2013, 13.)

Määritelmän ymmärtäminen edellyttää myös termin ”kybertoimintaympäristö” avaamista ja määrittelyä. Samassa strategiadokumentissa termi “kybertoimintaympäristö” määritellään seuraavasti:

> *Kybertoimintaympäristö on sähköisessä muodossa olevan informaation (tiedon) käsittelyyn tarkoitettu, yhdestä tai useammasta tietojärjestelmästä muodostuva toimintaympäristö.*
>
> *<u>Tarkennus 1:</u> Ympäristölle on tunnusomaista elektroniikan ja sähkömagneettisen spektrin käyttö datan ja informaation varastointiin, muokkaamiseen ja siirtoon viestintäverkkojen avulla. Ympäristöön kuuluvat myös datan ja informaation käsittelyyn liittyvät fyysiset rakenteet.*
>
> *<u>Tarkennus 2:</u> Informaation (tietojen) käsittely tarkoittaa informaation (tietojen) keräämistä, tallettamista, järjestämistä, käyttöä, siirtämistä, luovuttamista, säilyttämistä, muuttamista, yhdistämistä, suojaamista, poistamista, tuhoamista sekä muita informaatioon (tietoihin) kohdistuvia toimenpiteitä.* (Suomen kyberturvallisuusstrategia 2013, 12)

Hieman eri sanoin määrittelee Suomen Ulkoministeriö termiä *”kybertoimintaympäristö”* ulko- ja turvallisuuspolitiikkaa käsittelevällä sivustollaan seuraavasti:

> *Kybertoimintaympäristöllä tarkoitetaan ihmisten luomaa digitaalista rinnakkaistodellisuutta, joka maailmanlaajuisesti yhdistää informaatioteknologian, automatisoitujen ohjausjärjestelmien, internetin ja sosiaalisen median kautta toisiinsa ihmisiä ja laitteita valtioiden rajojen yli.* (Kyberturvallisuus ja kybertoimintaympäristö 2014.)

”Kyberturvallisuus” -termiä on määritellyt myös Limnell, Majewski ja Salminen teoksessan Kyberturvallisuus, jossa lyhyesti ja ytimekkäästi kuvataan termin tarkoittavan ”*digitaalisen maailman turvallisuutta*” (Limnell ym. 2014, 39)

Etelä-Afrikassa sijaitsevan Nelson Mandela Metropolitan University:n ICT-instituutin johtaja Rossouw von Solms ja hänen kollegansa PhD Johan van Niekerk pohtivat kyberturvallisuuden käsitettä Computers & Security lehdessä 38/2013 julkaistussa artikkelissaan “From information security to cyber security”. Heidän mukaansa kyberturvallisuutta pidetään usein synonyyminä tietoturvallisuudelle (information security). Tietoturvallisuudella tarkoitetaan omaisuutena olevan tiedon suojamista mahdollisia vaaraa aiheuttavia uhkia ja haavoittuvuuksia vastaan. Kyberturvallisuus on

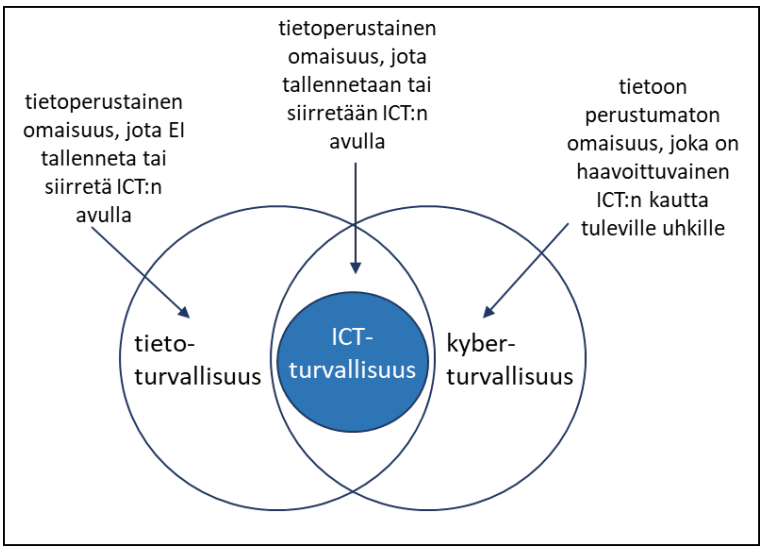
heidän mielestään käsitteenä tietoturvallisuus –käsitettä laajempi. Termillä tarkoitetaan von Solms:in ja van Niekerk:in mukaan:

> *Kyberavaruuden, sähköisessä muodossa olevan tiedon, kyberavaruutta tukevan ICT:n sekä kyberavaruuden käyttäjien suojaamista mukaan lukien henkilökohtainen, yhteisöllinen ja kansallinen kapasiteetti sekä aineelliset tai aineettomat intressit, jotka ovat haavoittuvia kyberavaruudesta peräisin oleville hyökkäyksille.* (von Solms & van Niekerk 2013, 101)

Kyberavaruudella (cyberspace) tarkoitetaan likimain samaa kuin ”kybertoimintaympäristö” –termillä, mutta sanatarkka määritelmä vaihtelee sisällöltään riippuen käsitteen määritelleestä tahosta.

Kansainvälinen standardointiorganisaatio ISO määrittelee standardissaan ISO/IEC 27032:2012 kyberavaruuden seuraavasti: *”complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form”* (ISO/IEC 27032:2012(en) 2012)

Kyberturvallisuus -termistä keskusteltaessa nousee esille usein rinnakkaisina käytetyt termit *”tietoturvallisuus”*, *”ICT-turvallisuus”* sekä *”tietoverkkoturvallisuus”*. Näiden käsitteiden eroja kuvaavat von Solms ja van Niekerk edellä mainitussa artikkelissa kuvion 7 mukaisella tavalla (von Solms & van Niekerk 2013, 101). Kuva havainnollistaa selkeästi, että edellä mainitut käsitteet ovat keskenään toisiaan leikkaavia. Kyberturvallisuudelle on ominaista, että se pitää sisällään nimenomaan ICT:n kautta tai sen avulla omaisuuteen kohdistuvia uhkia. Se on käsitteistä laajin ja siihen liittyvä inhimillinen elementti sekä kansalliset intressit ovat yhä merkittävämpiä tekijöitä kyberturvallisuudessa.



KUVIO 7: Tietoturvallisuuden, ICT-turvallisuuden ja kyberturvallisuuden keskinäinen suhde (von Solms & van Niekerk 2013)

3.2 YRITYKSIIN KOHDISTUVIA KYBERUHKIA

Uhanalaisia kohteita yrityksissä

Yrityksen näkökulmasta on tärkeää tunnistaa, mitkä asiat ja omaisuus yrityksessä voivat olla uhattuina. Raha, maine, tietojärjestelmät ja IT-pohjaisia palvelut ja liiketoimintaan liittyvä tieto ovat yleisimpiä kohteita, joihin kyberuhkat voivat kohdistua. Liiketoimintaan liittyvä tieto on yritykselle omaisuutta, joka voi olla monessa muodossa: asiakasluettelot, asiakastietokannat (esim. CRM-järjestelmissä), yrityksen omat sekä mahdolliset asiakkaiden taloustiedot, suunnitteilla olevat liiketoiminta-operaatiot, tuotteiden hinnoittelu, tuotemallit tai valmistusprosessiin liittyvät ohjaustiedot. Riippumatta siitä, käsitelläänkö ja säilytetäänkö tietoa omissa tietojärjestelmissä vai kolmannen osapuolen tuottamassa pilvipalvelussa liittyy sekä tietoon että IT-palveluihin aina riskinsä.

Uhkatoimijoita

Potentiaalisia uhkatoimijoita voidaan jakaa ulkoisiin ja sisäisiin uhkiin. Ulkoisia uhkia voivat olla esimerkiksi verkkorikolliset, jotka haluavat kiristää yritykseltä rahaa esimerkiksi verkkohyökkäyksellä uhkaamalla, varastaa tai vahingoittaa yrityksen kannalta arvokasta tietoa tai muutoin häiritä yrityksen toimintaa tai vahingoittaa sen julkisuuskuvaa. Kilpailevalla yrityksellä voi olla esimerkiksi verkkovakoilun avulla tarkoituksena hankkia varastetulla liiketoimintatiedolla itselleen taloudellista etua tai haitata toisen yrityksen liiketoimintaa. Ulkoinen uhka voi olla – usein tietämättään -

myös yhteistyökumppani tai alihankkija, jolla ei ole oma kyberturvallisuustaso riittävän korkealla. Myös entinen työntekijä voi haluta aiheuttaa haittaa entiselle työantajalleen. Ulkoinen uhkatoimija voi olla myös kokeilunhaluinen hakkeri/hakkeriryhmä, joka testaa omia kykyjään. Sisäisenä uhkana on useimmissa tapauksissa nykyinen työntekijä, joka osaamattomuuttaan, huolimattomuuttaan, vahingossa tai tarkoituksellisesti haluaa aiheuttaa haittaa.

Uhkien toteutumisen tapoja

Uhka voi toteutua monella eri tavalla. Kyseessä voi olla esimerkiksi tietokoneen tai muun yrityksen tietojärjestelmään kytketyn, yrityksen tietoa sisältävän laitteen luvaton käyttöönotto tai siihen tunkeutuminen joko tietoverkon välityksellä tai fyysiseen läsnäoloon perustuen. Uhka voi toteutua myös yrityksen verkkosivuston kautta, jolloin sinne lisätään tai sieltä poistetaan tietoja. Verkkosivuston käyttöä voidaan myös vaikeuttaa tai estää esimerkiksi palvelunestohyökkäyksen avulla. Uhka voi kohdistua myös ns. kolmannen osapuolen tietojärjestelmissä; kuten pilvipalveluissa tai rahalaitoksissa säilyttävään yrityksen omistamaan tietoon. Inhimillisen tekijän roolin lisääntyessä on nykypäivänä myös hyvin yleistä tietojen kalastelu sähköpostin tai sosiaalisen median välityksellä yrityksen henkilöstöltä. Samaa väylää pitkin voidaan saada henkilöstön jäsen klikkaamaan ajattelemattaan hiirellä sähköpostilinkkiä, jonka kautta asentuu haittaohjelma yrityksen tietojärjestelmään.

Uhkien toteutumisen vaikutuksia yritykselle

Seuraukset kyberuhkan toteutumisesta voivat olla yritykselle hyvin moninaisia. Välittömiä taloudellisia menetyksiä voi aiheutua rahoitus- ja pankkitietojen varastamisesta, mikäli hyökkääjä pääsee sillä tavoin vaikuttamaan yrityksen maksuliikenteeseen. Pidemmällä ajanjaksolla taloudellisia tappioita voi aiheuttaa sellaisten tietojen varastaminen, jota tekijä tai sen ”asiakas” tai toimeksiantaja myöhemmin käyttää kilpailevaan toimintaan. Pahimmassa tapauksessa menestykset voivat nousta satoihin tuhansiin euroihin. Digitalisaation etujoukoissa olevat, verkkoliiketoimintaan keskittyneet ja siitä riippuvaiset yrityksen voivat niin ikään kokea suuria taloudellisia menetyksiä kyberhyökkäyksen aiheuttamista häiriöistä johtuen. Katkos liiketoimintaa voi pahimmillaan kestää useita päiviä ja aiheuttaa asiakkaiden menettämistä ja mainevahinkoja.

Mikäli uhkan toteutuessa menetetään henkilötietoja luvattomiin käsiin ja sen perusteella yrityksen todetaan rikkoneen tuottamuksellisesti EU:n tietosuoja-asetusta, voidaan siitä määrätä ko. asetuksen 83 artiklan mukaan hallinnollista sakkoa maksimissaan enintään 20 miljoonaa Euroa tai 4% yrityksen vuotuisesta maailmanlaajuisesta liikevaihdosta. Yritys voi sopimuksista riippuen joutua korvausvelvolliseksi yhteistyökumppaneilleen tai asiakkailleen, mikäli niitä koskevaan tietoon kohdistuva ja vahinkoa aiheuttava kyberuhka realisoituu yrityksen tietojärjestelmissä tai niiden välityksellä. Lisäksi kyberuhkan toteutuessa yritykselle koituu kustannuksia siitä, että saastuneet tietojärjestelmät puhdistetaan, tehdään mahdolliset korjaavat/ehkäisevät toimenpiteet ja otetaan ne uudelleen käyttöön. (Euroopan Parlamentin ja Neuvoston Asetus (EU) 2016/679 2016, 83.)

4 TUTKIMUKSEN TAUSTA, TAVOITE JA TEORIA

4.1 TUTKIMUKSEN TAUSTALÄHTÖKOHTIA

4.1.1 Cyber Scheme Finland –pilottiprojekti

Digitalisoitumisen myötä informaatioteknologiasta ja sen turvallisuudesta on tullut lähes poikkeuksetta elementti, joka vaikuttaa vähintäänkin epäsuorasti lähes kaikkien yritysten liiketoimintaan ja sen jatkuvuuteen. Tieto ja sen käsittelyssä ja tallentamisessa käytettävä informaatioteknologia ovat useimpien yritysten kriittisiä menestystekijöitä. Henkinen pääoma, tuotteiden suunnitteluun, valmistusprosessiin tai strategiaan liittyvät luottamukselliset tai arkaluontoiset tiedot muodostavat usein suurimman osan yritysten kilpailuedusta. Samalla tarve käyttää ja jakaa tietoa entistä laajemmin ja tehokkaammin uusia tieto- ja viestintätekniikoita käyttäen lisää yrityksen tietopääomaan liittyviä riskejä.

Mikäli suomalainen pk-yritys halusi vuonna 2015 osoittaa asiakkaalle tai yhteistyökumppanille oman kyberturvallisuustasonsa, oli projektin alkaessa siihen käytettävissä olevia, yleisesti tunnettuja tapoja vain kaksi: 1) kansainväliseen ISO/IEC 27001 -standardiin perustuva sertifiointi (Lahnalahti 2013) tai 2) Kansallinen turvallisuusauditointikriteeristö KATAKRI:n mukainen auditointi. (Katakri 2015 Tietoturvallisuuden auditointityökalu viranomaisille. 2015). Molemmat niistä ovat edelleen useimpien pienten yrityksen näkökulmasta liikaa aikaa vieviä, raskaita ja kalliita prosesseja, joihin monellakaan yrityksellä ei yksinkertaisesti ole mahdollisuutta eikä varaa. Tästä

johtuen erityisesti pk-yrityksiä varten oli tarve kehittää yleisesti hyväksytty kyberturvallisuuden viitekehys ja toimintamalli, jonka mukaan niiden kyberturvallisuuden tasoa voidaan arvioida ja siihen perustuen edelleen kehittää.

Suomessa ei tällaista arviointimallia ollut vielä olemassa, mutta Iso-Britanniassa on toukokuusta 2014 lähtien ollut käytössä Cyber Essentials –arviointimalli. Se on kehitetty osana Iso-Britannian kansallista kyberturvallisuusohjelmaa yhteistyössä sikäläisen teollisuuden kanssa. Cyber Essentials -arviointimalli on suunnattu sekä pienille ja suurille yrityksille toimialasta katsomatta ja sen kehittäminen on ollut Iso-Britannian hallituksen vastine kasvaneelle kyberrikollisuudelle. (A brief history of Cyber Essentials 2017)

4.1.1.1 Projektin tavoitteet ja niiden asettelu

Projektin tavoitteiden asettamisessa hyödynnettiin loogisen viitekehykseen (Logical Framework Approach, LFA) perustuvaa tasomaista rakennetta ja interventiologiikkaa. Sen mukaan tavoitteita asetetaan kolmelle tasolle; 1) kehitystavoitteet, 2) projektin tarkoitus ja 3) tulostavoitteet. Tavoitteille muodostuu tällä tavoin keskinäinen hierarkia ja erilaiset konkretiatasot suhteessa projektiin. (Project Cycle Management Guidelines 2004 2004, 49.)

Kehitystavoitteet (overall objectives)

Loogisessa viitekehyksessä ylimmällä tavoitetasolla ovat kehitystavoitteet. Ne ovat pitkän aikavälin tavoitteita, joilla kuvataan projektin laajempaa merkitystä yhteiskunnalle, alueelle tai projektin kohde- ja sidosryhmille. Kehitystavoitteilla myös osoitetaan, mitä ja miten projektilla tuetaan alueellisia, kansallisia tai kansainvälisiä strategisia tavoitteita ja politiikkoja. Niiden asettelussa on merkillepantavaa, että yksittäisellä projektilla ei niitä kyetä saavuttamaan, mutta sillä voidaan osallistua niiden saavuttamiseen yhdessä muiden kehittämistoimenpiteiden kanssa.

Tässä projektissa ei erillisiä kehittämistavoitteita määritetty, mutta todettiin, että projektin avulla tuetaan seuraavien kansallisten ja alueellisten strategisten tavoitteiden toteutumista:

1) Suomen kyberturvallisuusstrategia 2013:

”Kansalaisilla, viranomaisilla ja yrityksillä on mahdollisuus tehokkaasti hyödyntää turvallista kybertoimintaympäristöä ja sen suojaamiseen syntyvää osaamista sekä kansallisesti että kansainvälisesti” (Suomen kyberturvallisuusstrategia 2013, 3).

2) Keski-Suomen maakunnallinen ICT –strategia 2013:

”Keski-Suomeen muodostuu kansainvälisen tason kyberturvallisuuden innovaatiokeskittymä ja Jyväskylä on saavuttanut kansallisella ja kansainvälisellä tasolla maineen kyberturvallisuusosaamisen kaupunkina ja alan edelläkävijänä” (Keski-Suomen maakunnallinen ICT –strategia 2013, 56).

3) Keski-Suomen maakuntaohjelman toimeenpanosuunnitelma 2015-2016:

” Alan huippuosaajille ja yrityksille luodaan kansainvälisesti houkutteleva ja kilpailukykyinen toimintaympäristö, jota tavoitetta Jyväskylässä tehtävä kyberturvallisuuden tutkimus- ja koulutustoiminta jo tukee” (Keski-Suomen maakuntaohjelman toimeenpanosuunnitelma 2015-2016 2014, 6).

4) Jyväskylän ammattikorkeakoulun strategia 2020:

JAMK on merkittävä valtakunnallinen kyberturvallisuuden toimijakoulutuksessa, TKI-toiminnassa ja palvelujen tarjoajana. Keskeisiä JAMKin osaamisalueita ovat kybertilannetietoisuus, -varautuminen, -infrastruktuuri ja -turvallisuusratkaisut. Kyberturvallisuusosaamista hyödynnetään laaja-alaisesti yrityksissä sekä julkisella sektorilla.
(JAMK 2016-2010: Jyväskylän ammattikorkeakoulun strategia 2016, 5.)

Projektin tarkoitus (project purpose)

Jokaisella kehittämisprojektilla on olemassa vain yksi tarkoitus, jolla kuvataan sitä, miksi projekti on tarpeen toteuttaa eli mikä on projektin missio/tehtävä. Tarkoitusta kuvaa usein yksi pitkähkö lause. Kun projektin tarkoitus saavutetaan sen aikana tehtävien toimenpiteiden tuloksena, tulisi sen tuottaa kestäviä hyötyjä kaikille projektin osapuolille. Projektin tarkoituksesta tulee käydä ilmi, että sillä tuetaan kehitystavoitteita.

Projektin tarkoituksena oli rakentaa ja pilotoida työkalut ja kansallinen toimintamalli/-konsepti erityisesti pk-yritysten kyberturvallisuuden arviointia, sertifiointia ja siihen perustuvaa kehittämistä varten.

Tulostavoitteet (results)

Tulostavoitteet kuvaavat niitä muutoksia, joita projektin avulla ja sen aikana on aikaansaatu. Kun kaikki tulokset on aikaansaatu, ne yhdessä tuottavat projektin tarkoituksesta kuvaavan asiantilan. Projektin tulokset eivät kuitenkaan saa olla siinä määrin riippuvaisia toisistaan, että jonkin tuloksen saavuttamatta jääminen vaarantaisi muiden tulosten saavuttamista.

Projektille asetettiin seuraavat tulostavoitteet, jotka kuvaavat projektin avulla aikaansaatavaa muutosta lähtötilanteeseen verrattuna.

1. *Arviointimallin rakenne ja sisältö ovat määriteltyjä.*
2. *Arviointi- ja akkreditointiprosessit ovat kuvattuja.*
3. *Pilotointi on toteutettu alueen pk-yrityksissä.*
4. *Työkalut ja muu infrastruktuuri ovat rakennettu.*

4.1.2 Projektin toteutus ja tulokset

Toimenpiteet

Tulostavoitteiden saavuttamiseksi projektissa toteutettiin seuraavat toimenpidekokonaisuudet:

1. *Arviointimallin rakenteen ja sisällön suunnittelu*
2. *Arviointi ja akkreditointiprosessin suunnittelu*
3. *Työkalujen rakentaminen*
4. *Pilotointiin osallistuvien yritysten valinta ja esivalmennus*
5. *Pilottiarvioinnin toteuttaminen yritysten itsearviointina*
6. *Kehittämisehdotusten antaminen yrityksille*
7. *Uudelleenarvioinnit (tarvittaessa)*
8. *Työkalujen viimeistely palautteen perusteella*
9. *Tulosten levittäminen*
10. *Raportointi*

Tulokset

Projektilla kehitettiin itsearviointiin perustuva arviointimalli, jonka sisältö rakennettiin erityisesti pienten ja keskisuurten yritysten kyberturvallisuuden tason mittaamista varten. Kohderyhmän ominaispiirteet otettiin huomioon arviointikysymysten

sisällössä, kriteeristön vaatimustasossa sekä koko arviointimallin kustannustasossa. Kriteeristön mukaiset vastaukset mahdollistavat FINCSC®-sertikaatin (Finnish Cyber Security Certificate) myöntämisen yrityksen käyttöön. Sertifikaatista yritys saa määräajaksi käyttöönsä sertifiointitodistuksen sekä tavaramerkillä suojatun FINCSC®-merkin esim. internet-sivustolleen lisättäväksi.

Arvioinnin toteuttamista varten suunniteltiin FINCSC®- mallin organisatorinen rakenne sekä siihen kuuluvien toimijoiden roolit ja vastuut. Koska arviointimallin kustannusrakenne tuli saada mahdollisimman alhaiseksi, suunniteltiin ja toteutettiin internetportaali, jonka välityksellä loppuasiakasyritys tekee itsearvioinnin ja arvioijataho sen tarkastaa. Lisäksi FINCSC®- sertifiointitoiminnalle suunniteltiin ja toteutettiin internetsivusto www.fincsc.fi, jonka osaksi edellä kuvattu portaali yhdistettiin. Sivustoa käytettiin projektin aikana myös projektin toiminnasta tiedottamiseen.

Tähän opinnäytetyöhön sisältyvä tutkimus toteutettiin osana toimenpidekokonaisuutta *4. Pilotointiin osallistuvien yritysten valinta ja esivalmennus.* Arviointimallia ja sen toteuttamista testattiin projektissa toteutetun pilottiarvioinnin aikana. Projektia suunniteltaessa asetettiin tavoitteeksi, että projektiin rekrytoidaan mukaan 20 Keski-Suomessa toimivaa pk-yritystä. Pilottiin valittiin yhteensä 22 eri toimialoille sijoittuvaa pk-yritystä, joista pilotoinnin suoritti loppuun 21 yritystä. Niistä yhteensä 17 yritystä hyväksyttiin sertifioinnin piiriin kahden arviointikierroksen jälkeen. Pilotointi tuotti runsaasti hyvä palautetta sekä arviointimallin ja –prosessin rakenteiden, että arvioinnin sisällön kehittämistä varten.

4.2 TUTKIMUKSEN TAVOITE

Tämän tutkimuksen tavoitteena oli tuottaa tietoa Keski-Suomessa toimivien pk-yritysten kyberturvallisuustietoisuuden ja kyberuhkiin varautumisen nykytilasta liiketoiminnan eri osa-alueilla. Tietoa hyödynnetään pk-yritysten kyberturvallisuustietoisuuden ja -osaamisen kehittämisessä sekä FINCSC®-sertifiointijärjestelmän kehittämisessä. Molemmat ovat osa Jyväskylän ammattikorkeakoulun osana toimiva kyberturvallisuuden tutkimus-, kehitys- ja koulutuskeskus JYVSECTEC:in toimintaa.

Termin ”varautuminen” määrittelee Valtionvarainministeriön vuonna 2016 julkaisema Toiminnan jatkuvuuden hallinta –ohje (VAHTI 2/2016) seuraavasti:

> *Varautumisella tarkoitetaan toimintaa, jolla varmistetaan tehtävien mahdollisimman häiriötön hoitaminen kaikissa tilanteissa. Varautumistoimenpiteitä ovat esimerkiksi riskien arviointi, jatkuvuus- ja valmiussuunnittelu, tekniset ja rakenteelliset etukäteisvalmistelut, koulutus, harjoitukset sekä tilojen ja kriittisten resurssien varaukset. Varautuminen jakaantuu suunnitteluun, sen edellyttämiin käytännön valmistelutoimenpiteisiin, näiden toteuttamiseen ja kehittämiseen sekä harjoitteluun.* (Toiminnan jatkuvuuden hallinta 2016, 23.)

4.3 TUTKIMUSKYSYMYKSET

Tutkimuksen avulla haettiin vastauksia seuraaviin tutkimuskysymyksiin:

1. Miten yritykset ymmärtävät kyberturvallisuuden käsitteenä ja millainen merkitys sillä on yritykselle?
2. Miten yritys on tunnistanut tiedon ja sen turvallisen käsittelyn merkityksen liiketoiminnalle?
3. Miten yrityksen toimintaprosesseissa on otettu kyberturvallisuus huomioon?
4. Miten yritys on ottanut kyberturvallisuuden huomioon henkilöstön osaamisessa?
5. Miten kyberturvallisuus on otettu huomioon yrityksen fyysisessä ympäristössä?

4.4 TUTKIMUSMENETELMÄ

Tutkimusmenetelmän valintaa voidaan lähestyä tutkimustyön tarkoituksesta käsin. Tässä tutkimuksessa on kyseessä *reaalimaailman ilmiöiden* tarkastelu, johon liittyy olennaisina osina ihmisen käyttäytyminen, arvot ja asenteet, osaaminen ja kokemukset sekä toiminta. Kun kyse on kyberturvallisuudesta, ihmisen asenteisiin ja toimintaan vaikuttaa puolestaan lukematon määrä ulkoisia tekijöitä, joista suurin osa ei ole etukäteen tiedossa tai edes ennustettavissa. Ihmisen toiminnassa heijastuu se avoin systeemi, jonka osana ihminen on (Hirsjärvi & Hurme 2009, 17).

Tutkimusmenetelmän/-strategian valinta riippuu siitä, millaista tietoa ja keneltä tai mistä sitä etsitään. (Hirsjärvi ym. 2000, 171.) Koska tavoitteena oli kerätä suhteellisen pieneltä pk-yritysten joukolta määrämuotoisella tutkimusinterventiolla tietoa *kuvailemaan* tutkittavia ilmiöitä todellisessa elämässä, valitsin pääasialliseksi tutkimusstrategiaksi *laadullisen eli kvalitatiivisen survey-tutkimuksen*. (Hirsjärvi ym. 2000, 152.) Kvalitatiivisen tutkimustiedon analysointiin käytin *sisäkkäin* myös *kvantitatiivisia* menetelmiä. Kyseessä on yleispiirteiltään *soveltava tutkimus*, joka pyrkii käytännön ongelmanratkaisuun ja toimenpidesuosituksiin.

Laadullisen tutkimuksen toteuttamiseksi on käytettävissä useita erilaisia menetelmiä. Tyypillistä laadulliselle tutkimukselle on, että aineiston hankinnassa käytetään sellaisia menetelmiä, joissa *tarkoituksenmukaisesti valitun* tutkittavan kohdejoukon *näkökulmat* ja *näkemykset* pääsevät esille (Hirsjärvi ym. 2000, 155). Tässä tutkimuksessa kohdejoukon koko ja koostumus määräytyivät pitkälti Cyber Scheme Finland –pilottihankkeen projektisuunnitelman mukaan. *Tiedonkeruun menetelmäksi* valitsin *strukturoidun haastattelututkimuksen*, joka mahdollistaa kohdejoukon henkilökohtaisen osallistumisen ja vuorovaikutuksen tiedonkeruutilanteessa. Se soveltuu menetelmänä todellisen elämän tilanteisiin, joita ei ole mahdollista toteuttaa koejärjestelyillä.

Strukturoidun haastattelututkimukseen päätymiseen vaikutti tiedonkeruumenetelmän osallistavuuden lisäksi se, kyberturvallisuudessa että kyse on suhteellisen ”nuoresta” ilmiöstä ja sen mahdollisista käytännön vaikutuksista yritysten toimintaan on vielä olemassa niukasti kokemusta. Strukturoidun tiedonkeruumenetelmän valintaa puoltaa myös se, että tavoitteena oli tutkittavan ilmiön ja kysymyksenasettelun näkökulmasta saada tutkittavat ”samalle viivalle”. Tällöin vastaajien valitsemat vastaukset perustuvat mahdollisimman hyvin tutkittavien omaan näkemykseen ja tilanteeseen yrityksessä, mutta kuitenkin ovat vertailtavissa keskenään sekä muiden samaan aihepiiriin liittyvien tutkimusten kanssa.

Vaihtoehtoisia tiedonkeruun menetelmiä olisivat tässä tapauksessa olleet *strukturoimaton haastattelututkimus* tai *kyselytutkimus* esimerkiksi sähköisesti toteutettuna. Strukturoimaton haastattelututkimus olisi mitä todennäköisimmin antanut vähemmän keskenään vertailukelpoisia vastauksia haastattelussa esitettyihin kysymyksiin, vaikeuttanut tulosten analysointia ja sitä kautta vastauksen saamista varsinaisiin tutkimuskysymyksiin. Kyselytutkimuksessa olisi puolestaan mahdollisuus kysymyksen väärinymmärtämiseen olisi suurempi, koska menetelmä ei mahdollista kysymyksen ”avaamista” tarvittaessa vastaushetkellä. Samoin kyselyssä saattaa myös vastausprosentti jäädä alhaiseksi (Hirsjärvi ym. 2000, 182). Näistä lähtökohdista käsin strukturoidun haastattelututkimuksen valinta tiedonkeruun menetelmäksi on eräänlainen kompromissi. Menetelmä jossakin määrin rajaa kysymyksenasettelullaan vastaajien yksilöllisiä ajatuksia ja mahdollisuuksia tuoda vapaasti esille ajatuksiaan, mikä voi-

daan nähdä jossakin määrin negatiivisena asiana. Toisaalta se mahdollistaa struktu-roidun rakenteensa ansiosta selkeämmän tulosten analysoinnin sekä vastausten saa-misen tutkimuskysymyksiin, koska vastauksina saatu tieto on niiden kannalta rele-vanttia.

5 TUTKIMUKSEN TOTEUTTAMINEN

5.1 TUTKIMUKSEN VAIHEET

Tutkimus toteutettiin seuraavien vaiheiden mukaan:

1. Tutkimuskokonaisuuden suunnittelu ja aikataulusta päättäminen

Tutkimus liittyi olennaisena osana Cyber Scheme Finland –pilottihankkeessa rakenne-tun sertifiointimallin pilotointiin. Se antoi tutkimuksen toteuttamista varten sisällölli-set raamit ja projektin toteutusaikataulu määritti varsinaisen tutkimuksen ajoittumi-sen. Tässä yhteydessä oli tarpeen ottaa kantaa myös käytettävään tutkimusmenetel-mään, jotta tutkimuksen suunnittelussa oli mahdollista edetä. Menetelmäksi valittiin strukturoitu haastattelututkimus. Menetelmän valintaan liittyviä perusteluja esitel-lään luvussa 5.2.

2. Haastattelukysymysten laatiminen ja arviointi

Kysymysten sisällön ja kysymysasettelun laatiminen on tutkimuksen onnistumisen kannalta yksi perustavaa laatua olevista asioista. Kysymysten lisäksi oli laadittava kir-jalliseen muotoon vastausohje sekä valinnaiset vastausvaihtoehdot. Projektipäällikkö sekä projektissa toiminut yhteistyökumppanin edustaja arvioivat luonnoksen kysy-myksistä sekä niihin liittyvän vastausohjeen vastausvaihtoehtoineen ja antoivat niistä palautteensa, jonka perusteella tein muutoksia kysymyksiin.

3. Haastatteluun osallistuvien yritysten rekrytointi

Haastattelututkimus tehtiin osana Cyber Scheme Finland –pilottiprojektissa tehtyä sertifiointimallin pilotointivaihetta, johon haettiin kohdejoukoksi pääosin Keski-Suo-men alueella toimivia pk-yrityksiä. Lähtökohtaisesti ei ollut merkitystä sillä, kuuluiko yritys mikro-, pien- vaiko keskisuurten yritysten joukkoon. Osallistujiksi haluttiin yri-tyksiä sekä perinteisiltä tuotannollisilta toimialoilta että palvelualoilta. Tarkoituksena

oli saada mahdollisimman monipuolinen kohdejoukko, joka edustaa keskivertoa alueella toimivaa pien- tai keskisuurta yritystä. Tästä syystä potentiaalisesta kohdejoukosta rajattiin pois sellaiset yritykset, jotka tuottavat tieto- tai kyberturvallisuuteen liittyviä palveluja.

Mahdollisuudesta osallistua pilottivaiheeseen tiedotettiin projektin internet-sivustolla, aiheesta järjestetyissä aamukahvitilaisuuksissa sekä kontaktoimalla suoraan puhelimitse tiedossa olevia potentiaalisia yrityksiä, joista osa oli aikaisemmasta yhteistyöstä tuttuja. Pilotoinnin sisällöstä, mukaan lukien tutkimushaastattelun järjestäminen, informoitiin heti ensimmäisen kontaktin yhteydessä. Haastattelun tarkemmasta sisällöstä tai tutkimuskysymyksistä ei tässä yhteydessä keskusteltu. Saamansa informaation perusteella yritysten edustajat tekivät päätöksen osallista pilotointivaiheeseen ja siihen liittyvään tutkimushaastatteluun. (Hirsjärvi & Hurme. 2009, 35.)

Kun kaikki pilotointiin hyväksytyt ja osallistuneet 20 yritystä oli saatu rekrytoitua, lähetettiin yrityksille sähköpostitse kirjalliset ohjeet pilotointiin osallistumisesta. Ohjeissa kerrottiin vielä kirjallisesti, että osana pilotointia ennen itsearvioinnin toteuttamista tullaan tekemään haastattelututkimus, jolla kartoitetaan pk-yritysten kyberturvallisuuden hallinnan nykytilaa eri osa-alueilla. Haastatteluaika sovittiin ohjeen lähettämisen pääosin puhelimitse jokaisen yrityksen yhteyshenkilön kanssa. Haastattelulle pyydettiin varaamaan aikaa noin kaksi (2) tuntia.

4. Kysymyssarjan testaus pk-yrityksessä

Ennen varsinaisen haastattelututkimuksen aloittamista oli koehaastattelun vuoro. Sen tarkoituksena oli testata kysymysten ymmärrettävyyttä ja yksiselitteisyyttä. Testaus tehtiin elintarvikealalla toimivassa pk-yrityksessä, jossa vastaajana oli yrityksen omistajiin kuuluva, markkinoinnista vastaava naishenkilö. Hänen kommenttiensa perusteella tehtiin joihinkin kysymyksiin sanamuotojen tarkennuksia.

5. Tutkimusaineiston keruu pk-yrityksissä haastattelujen avulla

Haastattelut toteutettiin ennalta sovitun yrityskohtaisen aikataulun mukaan kunkin yrityksen toimitiloissa. Haastatellut henkilöt edustivat pääasiassa yrityksen johtoa tai heidän vastuullaan muutoin olivat yrityksen tietotekniset järjestelmät ja tietoturvallisuus.

Jäljempänä olevissa luvuissa kuvataan tutkimusaineiston keruun jälkeen seuraavia työvaiheita, joita ovat:

6. *Aineiston analysoiminen*
7. *Tulosten luotettavuuden arvioiminen, sekä*
8. *Tutkimusraportin laatiminen*

5.2 TUTKIMUSHAASTETTELUN RAKENNE

Kyselyn tekemistä, toteuttamista ja analysointia varten rakensin Microsoft Excel –taulukkolaskentaohjelmaan työkirjan, joka sisältää kyselypohjan (lomakkeen), josta kysymysten sisältö linkittyy yrityskohtaisille välilehdille. Niille syötetty tieto eli käytännössä yritysten vastaukset linkittyvät kyselyn tulokset kokoavalle yhteenveto-välilehdelle. Työkalun valinta kohdistui kyseiseen ohjelmistoon perustuen siitä saatuun aikaisempaan kokemukseen tilastoaineiston käsittelystä.

Kyselylomakkeen suunnittelussa pitää ottaa huomioon, mikä on tutkimuksen tarkoitus ja mitkä ovat tutkimuskysymykset. Haastattelussa kokonaisuutena tulee ottaa riittävässä määrin huomioon haastateltavien henkilöiden tausta, perehtyneisyys asiaa, motivaatio vastaamiseen sekä käytettävissä oleva aika. Huomioon otettavana seikkana on myös vastaajien tietosuoja siten, että yksittäistä vastaajaa ei hänen antamiensa vastausten perusteella pystytä tunnistamaan eikä vastaajille tule tarvetta kantaa huolta vastauksissa annettujen tietojen väärinkäytöstä.

Hyvien haastattelukysymysten laatiminen on tärkeä osa haastattelu ja koko tutkimuksen onnistumista. Hyvän kysymyksen tulisi olla yksinkertainen ja yksiselitteinen, jotta vastaaja voi ymmärtää ja tulkita sen sillä tavoin kuin tutkija tarkoittaa. Tutkijan tulee etukäteen arvioida, sisältävätkö kysymykset epäselviä käsitteitä. Siinä tapauksessa ne tulee erikseen selittää kaikille vastaajille samalla tavalla. Yksi kysymys saa sisältää kysymyksen vain yhteen asiaan. Vaikka kysymysten määrä saattaa tämän vuoksi lisääntyäkin, on sekä vastaajan että tulosten analysoinnin kannalta tärkeää pilkkoa kysymykset vain yhden asian sisältäviksi. Kysymyksiä voi ainakin teoriassa esittää neutraalista näkökulmasta, positiivisesti virittyneestä näkökulmasta tai negatiivisesti virittyneestä näkökulmasta. Kysymyksissä tulee välttää kieltosanojen käyttöä, koska se aiheuttaa vastaajalle ylimääräistä rasitetta (Taanila 2013, 2). Kysymyk-

siin vastaamista edesauttaa se, että kyselyn avulla vastaaja voi kokea, että hänen vastauksillaan on tutkimuksen kannalta tärkeä merkitys ja että siitä voi olla hyötyä myös vastaajalle tulevaisuudessa.

Tutkimuksessa käytetty kysely koostuu viidestä (5) tutkimuskysymysten perusteella rakennetusta kysymyssarjasta (kysymyspatterista). Tällä tavoin oli mahdollista selvittää kokonaisuuksittain kuhunkin tutkimuskysymykseen liittyviä tekijöitä ilman, että vastaajaa rasitettiin hyppäämällä välillä johonkin toiseen aiheeseen. Kyselyn periaatteena oli se, että kussakin kysymyksissä esitettiin jokin väittämä ja vastaaja valitsi asteikolta hänen mielestään sopivimman vaihtoehdon. Vastaajilla oli haastattelutilanteessa käytössään paperille tulostettuna alla olevan taulukon 2 mukainen viisiportainen Likert-asteikko. Vastaajia ohjeistettiin antamaan vastauksensa sanallisen asteikon mukaan, koska se on monessa suhteessa kuvaavampi kuin pelkkä numero. Toisaalta se antaa vastaajalle hieman joustavuutta vetää raja kahden vastausvaihtoehdon välille tilanteessa, kun absoluuttista tietoa ei ole olemassa. Tarkoituksena asteikon laatimisessa kuitenkin oli, että vastausvaihtoehdot ovat toisensa poissulkevia. Numeraalinen asteikko oli laadittu helpottamaan tutkimustulosten analysointia ja kuvailua raportointivaiheessa. Siinä vastausvaihtoehdot muodostavat nousevan skaalan (Hirsjärvi ym. 2000, 187).

TAULUKKO 2: Tutkimustiedon keruussa käytetty Likert-asteikko

EI OLE RELEVANTTI	EI LAINKAAN	HEIKOSTI	KOHTALAISESTI	HYVIN	ERITTÄIN HYVIN
0	1	2	3	4	5

Likert asteikon käytön selkeänä etuna on, että sen avulla saadaan esille kunkin yrityksen kehitysvaihe. Jos vastaus asteikkona olisi käytetty vain kaksiportaista asteikkoa kyllä - ei vaihtoehtoinen, olisi lopputulos ollut ongelmallinen monestakin syystä. Vastaajalla olisi ollut vaikea päättää, kumpiko vaihtoehdoista kuvaa yrityksen tilannetta paremmin, jos kysymykseen liittyen oli yrityksessä jo jotakin tehty. Toisaalta tutkijan näkökulmasta kaksiportainen vastausvaihtoehto ei anna informaatiota toisensa poissulkevien vastausvaihtojen välillä. Lisäksi pelkät kyllä / ei vaihtoehdot eivät mahdollista keskihajonnan laskemista ja vastausten vertailu muihin esimerkiksi Likert -asteikkoa käyttäneisiin tutkimuksiin vaikeutuu.

Kysymyssarjoista ensimmäinen on nimeltään ”Käsitteet ja strategianäkökulma”, joka koostuu yhdestätoista (11) kysymyksestä. Niiden avulla oli tarkoituksena selvittää kyberturvallisuuden käsitettä ja sitä, missä määrin kyberturvallisuus on otettu huomioon yrityksen toiminnassa ja strategiassa. Toisen kysymyssarjan otsikko on ”Tieto ja sen merkitys liiketoiminnalle”. Se sisältää myös yksitoista (11) kysymystä, joilla haluttiin selvittää, miten yritys on tunnistanut tiedon merkityksen yrityksen liiketoiminta-kriittisenä tekijänä. Kolmas kysymyssarja kuuluu otsikon ”Prosessit” alle. Se koostuu viidestätoista (15) kysymyksestä, joilla selvitettiin, miten yritys on käytännön toiminta-prosesseissa ottanut huomioon mahdolliset kyberturvallisuusuhat sekä valmistautunut niitä kohtaan. Neljäntenä kysymyssarjana on ”Henkilöstön tietoisuus ja osaaminen”. Se koostuu kahdeksasta (8) kysymyksestä, joilla haluttiin selvittää, millainen osaaminen ja tietämys yrityksen henkilöstöllä on kyberturvallisuudesta ja miten sitä ylläpidetään ja kehitetään. Viides kysymyssarja on nimeltään ”Fyysinen turvallisuus”. Sarjaan sisältyy seitsemän (7) kysymystä, joilla tarkoituksena oli selvittää, miten yritys on ottanut kyberturvallisuuden huomioon fyysistä ympäristöä suunnitellessaan ja sitä käyttäessään. Kysymyssarjat esitettiin edellä kuvatussa järjestyksessä ja ne sisälsivät kysymyksiä yhteensä 52 kappaletta. Vastaajilla oli jokaisen kysymyksen kohdalla mahdollisuus antaa lisätietoja tai kommentteja. Sen lisäksi jokaisen kysymyssarjan jälkeen oli vastaajalla mahdollisuus kommentoida tai tarkentaa kysymyssarjaan liittyviä vastauksiaan vapaamuotoisesti. Vielä lopuksi sen jälkeen, kun kaikki strukturoidut kysymykset oli läpikäyty, oli vastaajilla vapaaehtoisesti mahdollisuus antaa koko haastatteluun liittyviä vapaamuotoisia ”vapaa sana” –tyylisiä kommentteja tai muuta palautetta. Tutkimuksessa käytetty kyselylomake on tämän opinnäytetyön liitteenä.

Valitsin tutkimuksessani kysymysten asettelussa edellä mainituista näkökulmista positiivisesti virittyneen näkökulman. Projektin toimenpiteenä haastattelututkimus edelsi varsinaista sertifiointimallin pilotointia. Varsinaisen tutkimustehtävän lisäksi halusin kysymysten asettelulla ”herätellä” vastaajia kyberturvallisuuteen liittyviin asioihin, joita sertifiointimallin pilotointivaiheessa heille tulisi hieman eri muodossa kysymyksinä vastaan. Osa kysymyksistä on muodoltaan neutraaleja eli arvovapaita, mutta suurin osa on siinä muodossa, mikä kuvaa ihannetilannetta silloin, kun asiat ovat yrityksessä parhaassa mahdollisessa kunnossa. Näin ollen kysymysten muotoilu ja käytetty arviointiasteikko ovat keskenään yhteensopivia siten, että mitä suuremman numeraalisen tai positiivisimman sanallisen arvon vastaus kysymykseen sisältää,

sitä paremmin asia on yrityksessä hoidettu. Kyselyyn ei sisälly kysymyksiä, joissa käytetään kieltosanoja tai johon voisi vastata numeraalisella arvolla 1 (=ei lainkaan) siitä huolimatta, että asia ei ole yrityksessä ollenkaan kunnossa.

5.3 HAASTATTELUAINEISTON KERUU

Tutkimushaastatteluihin liittyvät tapaamiset toteutettiin jokaisen sertifiointimallin pilotointiin ilmoittautuneen ja siihen hyväksytyn 20 pk-yrityksen kanssa ennakolta sovittuna ajankohtana helmi-maaliskuussa 2016.

Tapaamiset yhtä lukuun ottamatta tapahtuivat kohdeyritysten toimitiloissa. Yksi tapaaminen järjestettiin etäyhteydellä Skype for Business –ohjelmiston avulla. Tapaamisissa oli pääsääntöisesti toimitusjohtaja/yrityksen omistaja tai hänen valtuuttamansa henkilö. Yhdessä yrityksessä oli läsnä myös yrityksen tietotekniikasta vastaava ulkopuolinen palveluntuottaja. Henkilöt olivat läsnä koko tapaamisten ajan. Haastattelun sisältänyt tapaaminen alkoi yleensä osallistujien ja toimenkuvien lyhyellä esittelyillä. Seuraavana oli vuorossa yrityksen toiminnan esittely sekä Jyväskylän ammattikorkeakoulun informaatioteknologian instituutin toiminnan esittely erityisesti kyberturvallisuuden osalta. Koska kyseessä oli Cyber Scheme Finland –pilottihankkeeseen liittyvä toimenpide, kertasimme osallistujille ennakkoon lähetetyn tutustumisaineiston mukaan hankkeen tavoitteet toimenpiteet ja aikataulun. Lisäksi kävimme yksityiskohtaisesti läpi sertifiointimallin pilotoinnin vaiheet sekä pilotoinnin jälkeiset toimenpiteet. Esittelyt herättivät keskustelua ja kysymyksiä, jotka kävimme aina sitä mukaa kuin niitä esiintyi. Tähän kului aikaa keskimäärin noin yksi tunti.

Haastattelua edeltäneet esitykset ja keskustelut toimivat hyvin haastatteluun johdattelevana tienä. Varsinaisen haastatteluosuuden aluksi kerrattiin haastattelun tarkoitus ja käytiin läpi, että tulosten analysoinnissa ja raportoinnissa säilytetään sekä henkilöiden että yritysten tiedot haastattelijan hallussa anonymiteetti säilyttäen. Sen jälkeen kuvattiin lyhyesti kyselyn rakenne ja siihen liittyvät viisi (5) kysymyssarjakokonaisuutta sekä vastaamisessa käytettävä Likert -asteikko vastausvaihtoehtoineen. Vastaajat ohjeistettiin vastaamaan sanallisesti kuvattujen vaihtoehtojen mukaisesti siitä huolimatta, että vastaus kirjattiin numeroina. Varsinainen haastattelu tapahtui siten, että haastattelija luki ääneen kysymyksen ja vastaaja hetken miettimisen kertoi valitsemansa vaihtoehdon. Kysymys toistettiin tarvittaessa. Varsinainen haastattelu

kesti mahdollisine jälkikeskusteluineen puolesta tunnista tuntiin. Kun kaikki 52 kysymystä oli läpikäyty, oli haastateltavilla mahdollisuus kertoa omat kommenttinsa sekä haastattelun teemaan, että sen sisältöön ja toteutukseen liittyen. Joidenkin kysymysten osalta tarkennettiin sanamuotoja ensimmäisten haastattelujen jälkeen kysymysten selkeyttämiseksi, kuitenkin niin että kysymysten asiasisältö säilyi samana.

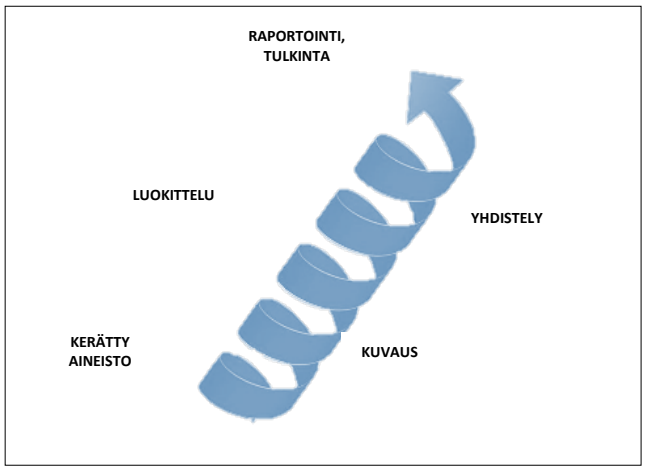
5.4 HAASTATTELUAINEISTON ANALYSOINTI

Aineiston analysointi, tulkinta ja johtopäätösten tekeminen muodostavat yhdessä tutkimuksen tärkeimmän vaiheen (Hirsjärvi ym. 2000, 207). Kun on kyse strukturoidusta tutkimuksesta, analyysivaihe voidaan sijoittaa tutkimuksen elinkaaressa vaiheeseen, jolloin tutkimuksen tulosaineisto on kerätty ja järjestetty. Tässä tapauksessa tutkimusaineisto kerättiin haastattelujen avulla niiden yhteydessä ja sen järjestäminen analysoitavaksi toteutui pääosin samanaikaisesti.

Haastatteluaineiston analysoinnissa käytän sekä määrälliseen tutkimukseen että laadulliseen tutkimukseen liittyviä menetelmiä siitä huolimatta, että tutkimus olikin laadullinen luonteeltaan. Tarkoituksena on käyttää menetelmiä siten että, niillä täydennetään toisiaan ja tulosaineistosta saadaan esille kvantitatiivisia määreitä niiltä osin kuin se tutkimuskysymysten näkökulmasta on tarpeellista.

Osa tutkimusaineistosta käsitellään kvantitatiivisten menetelmien mukaan, jolloin aineisto analysoidaan tutkimusta varten laaditun taulukkolaskentatyökirjan avulla. Sillä muodostetaan analyysivaiheen aikana erikseen määriteltävät vastausten jakaumat ja frekvenssit. Tuloksien esittämisessä käytetään kuvioita ja graafisia kaavioita, jotka kirjoitetaan auki.

Kvalitatiivisen analyysin kulkua kuvaavat Hirsjärvi & Hurme (2009, 144) ylöspäin suuntautuvalla spiraalilla, jossa analyysin vaiheet toisiaan seuraten nivoutuvat yhteen (kuvio 8).



KUVIO 8. Kvalitatiivisen analyysin vaiheet (muokattu lähteestä Hirsjärvi & Hurme 2009)

Kerätty aineisto kannattaa ensin lukea huolellisesti läpi, jotta se tulee tutkijalle riittävän tutuksi analyysiä varten. Aineistoa lukiessa kannattaa panna aineistosta merkille seikkoja, jotka nousevat esille erilaisina yksityiskohtina ja palata niihin myöhemmissä analyysin vaiheissa. Tässä tutkimuksessa aineisto koostuu strukturoidun haastattelun vastausaineistosta, joka perustuu vastaajilla olleeseen asteikkoon. Näin ollen yksittäisten vastausten tulkinnassa ei tutkimuksen rakenteesta johtuen voi käyttää esimerkiksi avainsanojen litterointiin perustuvaa toimintamallia, kuten esimerkiksi strukturoimattomassa haastattelututkimuksessa on mahdollista. Tämä yksinkertaistaa vastausten analysointia ja jättää vähemmän tilaa tulkinnalle.

Aineiston kuvailussa pyritään kartoittamaan tapahtumien tai kohteiden ominaisuuksia tai niiden ominaispiirteitä. Kuvailua voidaan tehdä monella tavalla ja sitä voidaan tarkastella suhteessa tutkijan tapaan kuvata aineistoa ilman tulkintaa. Kuvauksen tarkkuusvaatimusta tulee tarkastella tutkimuksen tarkoituksen näkökulmasta käsin ja pohtia, mitä seikkoja tutkimuksesta on tarpeen kuvata ja miten yksityiskohtainen kuvauksen tulee olla. Kuvauksessa on hyvä nostaa esille tutkittavan ilmiön kannalta merkitykselliset asiat siten, että ne saadaan selkeästi esille kerätyn aineiston joukosta. Lisäksi kuvauksessa tulee tutkittavat ilmiöt sitoa tutkimuksen kohderyhmän kontekstiin, jotta voidaan ymmärtää niiden laajempi merkitys. (Hirsjärvi &Hurme 2009, 146.)

Aineiston luokittelu synnyttää perustan haastatteluaineiston myöhemmälle tulkinnalle. Luokittelun avulla jäsennetään tutkittavaa ilmiötä. Luokittelussa tehdään päät-

telyä, jonka pääkriteerinä on tutkimusongelma sekä sen alakohtina tutkimuskysymykset. Tässä tutkimuksessa olen valmistautunut luokitteluun jo tutkimushaastattelun rakenteen ja kysymyslomakkeen suunnitteluvaiheessa siten, että haastattelukysymykset ryhmiteltiin kysymyssarjoiksi tutkimuskysymysten mukaan.

Aineiston yhdistelyssä on tarkoituksena löytää luokkien välille säännönmukaisuuksia tai toisaalta poikkeavia tapauksia. Yhdistelyllä on mahdollista löytää korrelaatioita eri luokkien ja eri ilmiöiden välille. Tavoitteena olisi pyrkiä tutkimusaineiston avulla saamaan ilmiöstä riittävän laaja ymmärrys ja löytämään ainakin teoreettinen näkökulma, johon luokiteltu aineisto sopii. (Hirsjärvi & Hurme 2009, 150.)

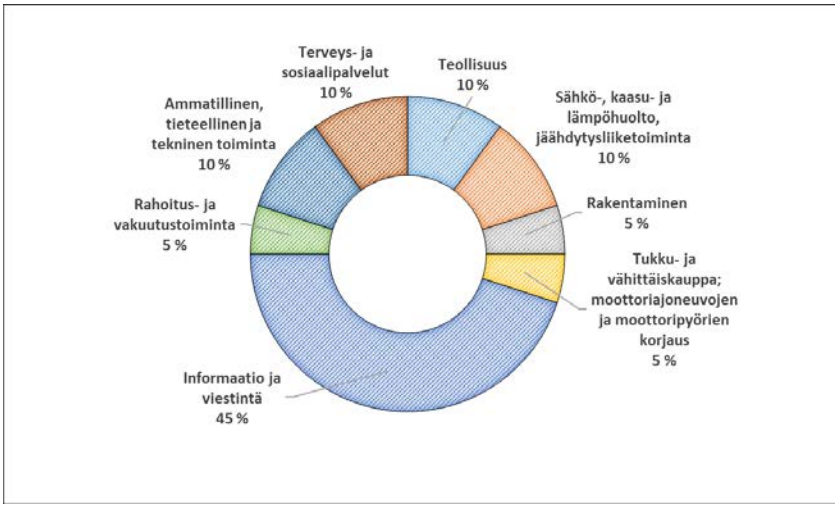
Haastatteluaineiston tulkinta on monitahoinen kysymys ja sitä tapahtuu tutkimuksen eri vaiheissa. Jo kysymysten laatija voi tehdä tulkintaa, minä jälkeen haastateltava tekee kysymyksestä ja ilmiöstä oman tulkintansa vastaustaan pohtiessaan. Tässä strukturoidussa haastattelussa ei sen sijaan haastattelijalle jäänyt mahdollisuutta tulkintaan, koska vastaukset kysymyksiin annettiin yksiselitteisinä vaihtoehtoina.

Aineiston tulkinnassa ilmiötä tarkastellaan koko kerätyn aineiston näkökulmasta, mikä mahdollistaa tulkita sekä yksittäisiä vastauksia tai luokkia että myös luokkien välisiä korrelaatioita. Tutkimusraportin lukija tekee lukiessaan omaa tulkintaansa, joka voi raportin olla erilainen kuin tutkija on asiaa tulosten perusteella tulkinnut.

6 TUTKIMUKSEN TULOKSET

6.1 TUTKIMUSAINEISTON KUVAUS

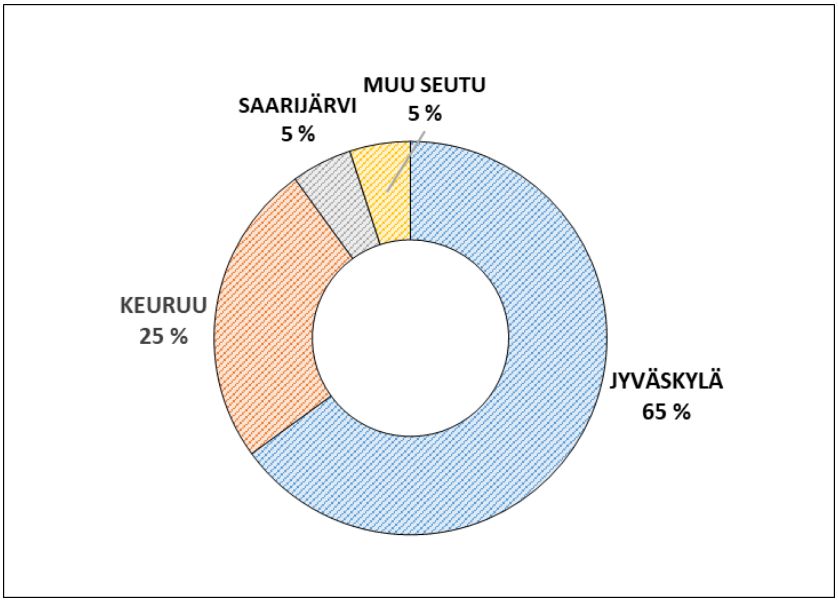
Haastattelututkimukseen osallistuneet 20 pk-yritystä jakautuivat yrityksen Y-tunnuksen perusteella Yritys- ja yhteisötietojärjestelmästä (Yritys- ja yhteisötietojärjestelmä YTJ 2016.) haetun tiedon mukaan kuvion 9 esittämille Tilastokeskuksen toimialaluokituksen (TOL 2008) pääluokkien mukaisille toimialoille (Toimialaluokitus 2008).



KUVIO 9. Haastateltujen yritysten toimialakohtainen jakauma TOL 2008:n mukaan (N=20)

Toimialoista ”informaatio ja viestintä” nousi esille suurimpana yksittäisenä toimialana. Todennäköisenä selityksenä ko. toimialan yritysten kiinnostukselle aihetta kohtaan on kyberturvallisuuden merkittävä rooli yritysten liiketoiminnalle. Tätä asiaa tarkastellaan lähemmin jäljempänä tuloksia tutkimuskysymyksittäin analysoitaessa.

Tutkimuksessa haastateltiin yhteensä kahtakymmentä pääasiassa Keski-Suomen alueella toimivan pk-yrityksen edustajaa. Yritykset jakautuivat seutukunnittain neljälle eri seutukunnalle, joista kolme sijaitsee Keski-Suomen maakunnassa ja yksi Pirkanmaan maakunnassa. Yritysten seutukohtainen jakauma on näkyvissä kuviossa 10.



KUVIO 10. Haastateltujen yritysten maantieteellinen jakauma (N=20)

Strukturoidun tutkimushaastattelun toteuttamista varten rakensin haastattelukysymyksistä Microsoft Excel –työkirjan, jossa jokaiselle yritykselle oli oma välilehtensä. Välilehtien niminä käytin numeroita yhdestä kahteenkymmeneen. Tämä oli yksi keino varmistaa, ettei haastattelutilanteessa kukaan vastaajista näe muiden vastauksia eikä muiden haastattelututkimukseen osallistuneiden yritysten tietoja. Yksittäisten yritysten antamat vastaukset linkittyvät yhteenvetosivulle tulosten yhteenvetoa ja analysointia varten.

Strukturoitu tutkimushaastattelu koostui viidestä (5) kysymyssarjasta, jotka oli rakennettu tutkimuskysymysten ympärille. Vastaajilla oli käytössään viisiportainen Likert-asteikko, jonka mukaan he valitsivat kuhunkin kysymykseen senhetkistä tilannetta yrityksessä mielestään sopivimman vastausvaihtoehdon. Käytettävissä olevat vaihtoehdot olivat 1=ei lainkaan, 2=heikosti 3=kohtalaisesti 4=hyvin 5=erittäin hyvin. Lisäksi oli käytössä vaihtoehto 0= ei ole relevantti. Kysymyssarjoissa oli yhteensä 52 kysymystä, jotka olivat väittämän muodossa. Yhteensä numeraalisia vastauksia kysymyksiin kertyi 1040 kappaletta.

Lisäksi vastaajilla oli mahdollista antaa vapaamuotoinen kommentti/palaute tutkimukseen, sen teemaan tai oman yrityksensä tilanteeseen liittyen. Vapaamuotoisia kommentteja annettiin yhteensä 23 kappaletta. Tutkimuksen sisältöön tai sen toteuttamiseen liittyviä kommentteja esitettiin seitsemän ja yleisesti kyberturvallisuuteen tai yrityksen omaan nykytilaan kommentteja esitettiin yhteensä 16.

Haastatelluista henkilöistä naisia oli neljä ja miehiä 16. Vastaajia ja vastauksia oli tulosaineiston mukaan mahdollista analysoida yrityksittäin, toimialoittain, seutukunnittain sekä myös tarvittaessa vastaajan sukupuolen mukaan, mitä ei kuitenkaan anonymiteetin säilyttämisen vuoksi ole tehty.

6.2 TULOKSET TUTKIMUSKYSYMYKSIIN

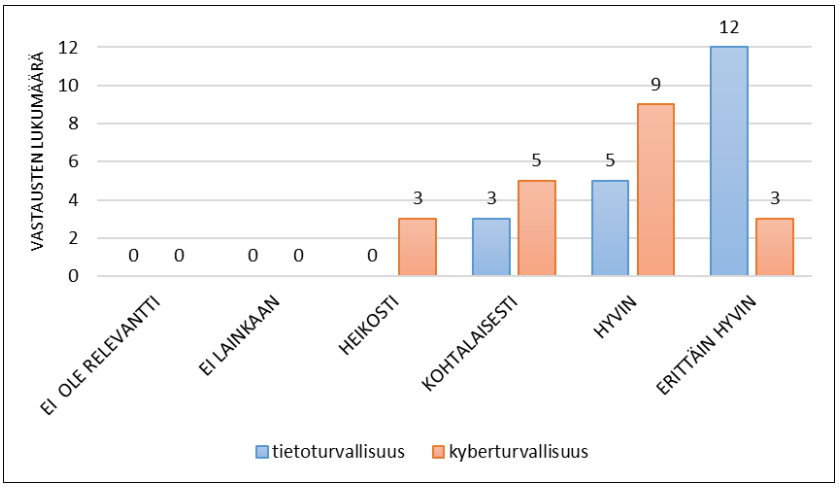
Analysoin strukturoidun tutkimushaastattelun tuloksia kysymyssarjoittain siten, että kukin kysymyssarja vastauksineen kohdentuu yhteen tutkimuskysymykseen. Kysymyksistä, jotka kohdistuvat hyvin läheisesti samaan asiaan, olen muodostanut kysymyspareja tai joissakin tapauksissa kolmen kysymyksen ryhmiä paremman kokonaiskäsityksen saamiseksi kysytystä asiasta. Vastausten jakaumia esittävissä graafisissa

kuvioissa olen joissakin kohdissa taivuttanut vastausasteikkoa eri sija- tai sanamuotoon, jotta se paremmin soveltuisi kulloiseenkin kysymykseen.

6.2.1 Tutkimuskysymys 1: Miten yritykset ymmärtävät kyberturvallisuuden käsitteenä ja millainen merkitys sillä on yritykselle?

Ensimmäisen kysymyssarjan työnimi on ”1. Käsitteet ja strategia näkökulma”. Haastatteluvaiheessa tähän kysymyssarjaan sisältyi yhteensä 11 kysymystä, joista analyysivaiheessa siirsin yhden kysymyksen kysymyssarjaan kaksi, johon se soveltui sisällöllisesti paremmin.

Haastattelun aluksi selvitettiin kysymysparilla termien ”tietoturvallisuus” ja ”kyberturvallisuus” selkeyttä yrityksen johdolle. Vastaajien mielestä termi ”tietoturvallisuus” oli tutumpi ja sisällöltään selkeämpi. Kahdestakymmenestä vastaajasta viisi (5) ilmoitti tuntevansa sen merkityksen hyvin ja 12 vastaajaa erittäin hyvin. Termi ”kyberturvallisuus” oli yhdeksän (9) vastaajan mielestä hyvin selkeä ja kolmen vastaajan mielestä erittäin selkeä. Kohtalaisen selkeänä ”kyberturvallisuutta” piti viisi vastaajaa ja ”tietoturvallisuutta” kolme vastaaja. Kyberturvallisuus oli terminä heikosti selkeä kolmen vastaajan mielestä. Kuvio 11 havainnollistaa haastateltujen antamat vastaukset tähän kysymyspariin. Siitä on selkeästi nähtävissä termin ”tietoturvallisuus” selkeys yritysten johdon mielestä.

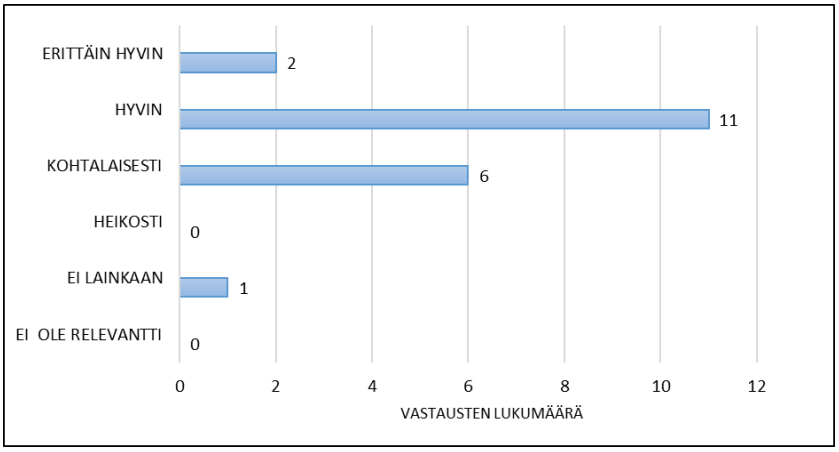


KUVIO 11. Termien ”kyberturvallisuus” ja ”tietoturvallisuus” selkeys yritysjohdolle (N=20)

Seuraavaksi kysyttiin missä määrin yrityksen strategiassa on otettu tieto- ja/tai kyberturvallisuus huomioon. Kaksi (2) vastaajaa kahdestakymmenestä valitsi vastauksen

”erittäin hyvin”, 11 vastaaja oli vastauksen ”hyvin” kannalla ja kuusi (6) vastaajaa valitsi vaihtoehdon ”kohtalaisesti”. Vastaajista yksi (1) ilmoitti, että tieto- tai kyberturvallisuus ei ole lainkaan asia, joka olisi otettu huomioon yrityksen strategiassa.

Kuvio 12 kuvaa vastausten jakaumaa ja siitä on selkeästi nähtävissä, että yli puolet vastaajista ilmoitti tieto- ja/tai kyberturvallisuuden olevan eräs yrityksen strategisesti merkittävistä tekijöistä.



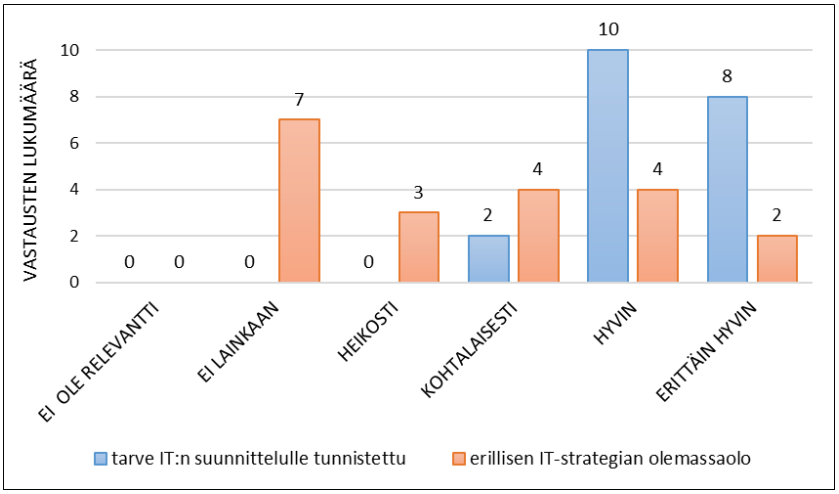
KUVIO12. Tieto- ja/tai kyberturvallisuuden huomioonottaminen strategiassa (N=20)

Informaatioteknologian merkitys yrityksen liiketoiminnalle selvitettiin kysymysparilla, jonka ensimmäisessä kysymyksessä haluttiin tietää, missä määrin yrityksessä on tunnistettu tarve strategiseen informaatioteknologiaan liittyvälle suunnittelulle liiketoiminnan tavoitteiden saavuttamiseksi. Toisella kysymyksellä haluttiin selvittää, onko yrityksellä olemassa erillinen it-strategia, joka on osana yrityksen kokonaisstrategiaa.

Vastausten mukaan 18 yritystä kahdestakymmenestä on tunnistanut ”hyvin” tai ”erittäin hyvin” tarpeen informaatioteknologian strategiselle suunnittelulle ja kaksi (2) yritystä ilmoittaa tarpeen olevan tunnistettu ”kohtalaisesti”. Erillistä IT-strategia ei ole lainkaan seitsemällä (7) yrityksellä, se on olemassa ”heikosti” kolmella (3) yrityksellä ja ”kohtalaisesti” neljällä (4) yrityksellä. Kahdella (2) yrityksellä kahdestakymmenestä erillinen IT-strategia on ”erittäin hyvin” ja neljällä (4) yrityksellä ”hyvin” olemassa.

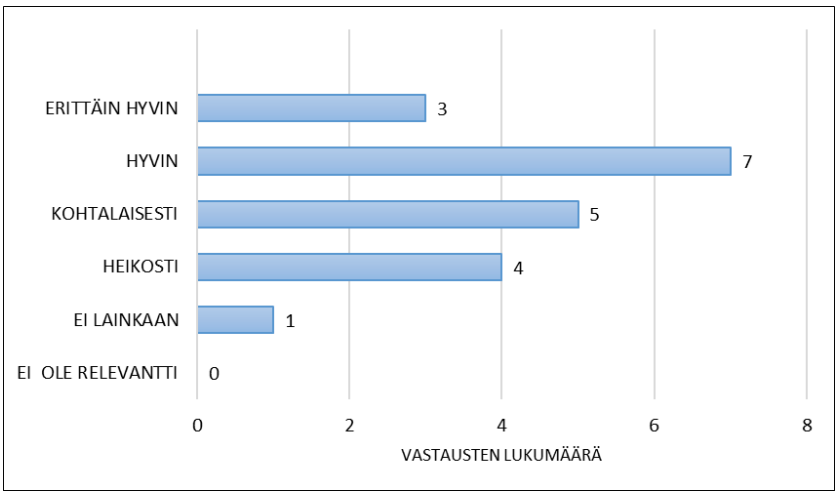
Kuviossa 13 on näkyvissä vastausten jakauma tähän kysymyspariin. Koska tarve informaatioteknologian strategiselle suunnittelulle on vahvasti tunnistettu, voidaan vas-

tauksista päätellä, että yksi tulevaisuuden toimenpiteistä suuressa osassa tutkimukseen osallistuneista yrityksistä tulee olemaan informaatioteknologian sen käytön strateginen suunnittelu ja mahdollisesti myös informaatioteknologian sisällyttäminen nykyistä vahvemmin yrityksen strategian tai jopa erillisen IT-strategia laatiminen.



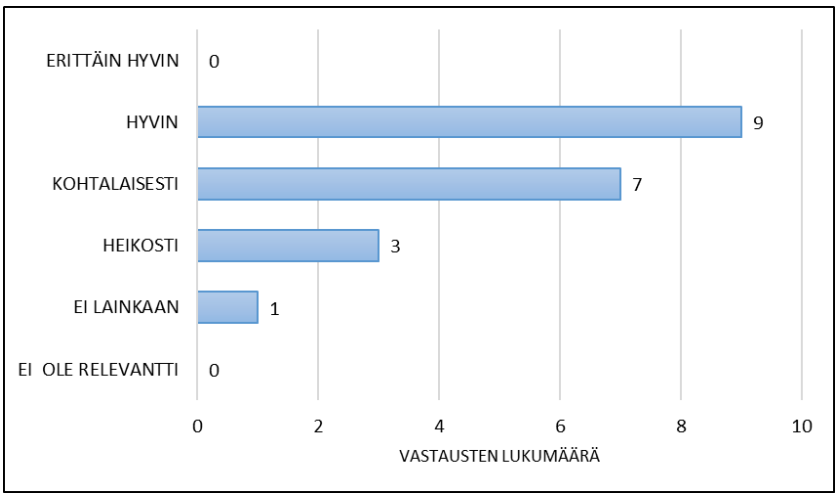
KUVIO 13. Informaatioteknologia rooli yrityksen strategisena tekijänä (N=20)

Mahdollisten tieto- ja kyberturvallisuusuhkien tunnistaminen ja niiden arviointi ovat yksi perusedellytys sille, että voidaan suunnitella ja ottaa käyttöön keinoja niitä vastaan suojautumiseksi. Haastateltavilta kysyttiin, missä määrin yrityksessä on tunnistettu ja arvioitu tietoon ja sen käsittelyn liittyvien epävarmuuksien ja epäonnistumisten (uhkien) vaikutuksia liiketoimintaan. Kolme (3) yritystä kahdestakymmenestä on paneutunut asiaan vastauksensa perusteella ”erittäin hyvin” ja seitsemän (7) yritystä ”hyvin”. Yksi (1) yrityksistä ei ole lainkaan tunnistanut ja arvioinut mahdollisia uhkia, neljä (4) yritystä on tunnistanut ja arvioinut niitä ”heikosti” ja viisi (5) yritystä ”kohtalaisesti”. Kun verrataan alla olevassa kuviossa 14 esitettyä vastausten jakaumaa kuvioon 12, voidaan päätellä, että useimmissa vastanneista yrityksessä on tiedostettu strateginen tarve tieto- ja kyberturvallisuudelle, mutta vaadittavat käytännön toimet ovat vielä osalla yrityksistä kesken.



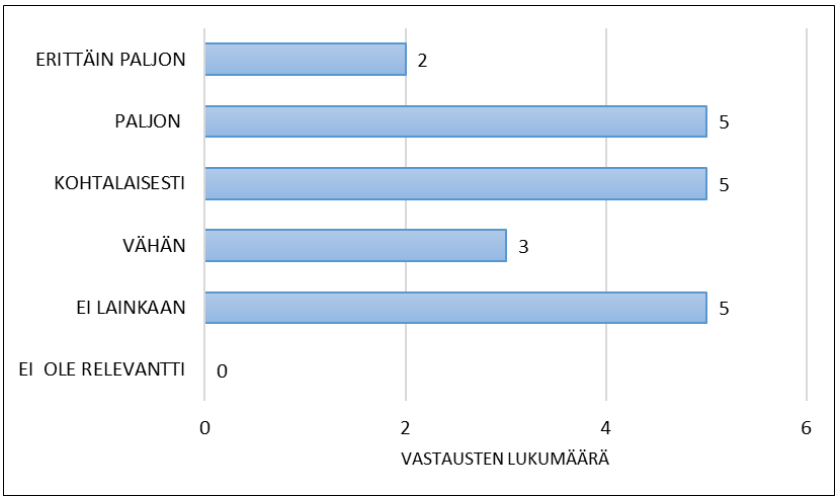
KUVIO 14. Uhkien tunnistamisen ja arvioinnin tilannekuva haastatteluajankohtana (N=20)

Ymmärrys omasta valmiudesta reagoida mahdollisiin kyberturvallisuusuhkiin ja -poikkeamiin on yrityksen kannalta tärkeä seikka. Haastateltavilta kysyttiin, miten yrityksessä on tiedossa oma valmius reagoida mahdollisen kyberturvallisuuspoikkeamaan. Kukaan kahdestakymmenestä vastaajasta ei ollut sitä mieltä, että tietoisuus valmiudesta olisi ”erittäin hyvällä” tasolla. Yhdeksän (9) vastaajaa vastasi valmiuden olevan ”hyvin” tiedossa ja seitsemän (7) vastaaja ilmoitti tietoisuuden tasoksi ”kohtalainen”. Valmius oli ”heikosti” tiedossa kolmessa (3) yrityksessä ja ”ei lainkaan” tiedossa yhdessä (1) yrityksessä. Vastausten jakaumasta kuviossa 15 voidaan nähdä, että tietoisuuden lisäämiseen on tehtävä yrityksissä toimenpiteitä. Niillä on todennäköisesti vaikutusta myös valmiuden kehittymiseen.



KUVIO 15. Tietoisuus valmiudesta reagoida kyberturvallisuuspoikkeamaan (N=20)

Yritysten ja organisaatioiden toiminnassa voi esiintyä tilanteita, jotka voidaan kokea uhkatilanteiksi tai niissä täytyy kriteerit, jotka yritys kokee riskiksi liiketoiminnan kannalta. Yrityksiltä kysyttiin missä määrin niissä on esiintynyt tilanteita, jolloin on käytännössä jouduttu arvioimaan kyberturvallisuuteen liittyviä riskejä sekä niiden vaikutuksia liiketoimintaan. Vastaukset jakautuivat siten, että viisi (5) yritystä ilmoitti, ettei kyseisen tyyppisiä tilanteita ole esiintynyt lainkaan ja kolmessa (3) yrityksessä niitä on esiintynyt ”vähän”. Viiden (5) yrityksen vastaus oli ”kohtalaisesti” ja viidessä (5) yrityksessä kyseessä olevia tilanteita on esiintynyt paljon ja kahdessa (2) yrityksessä erittäin paljon. Kuviossa 16 havainnollistetaan vastausten jakaumaa. Tässä yhteydessä on hyvä muistaa, että mikäli yrityksen valmiudet uhkatilanteiden tunnistamiseen eivät ole riittävää tasolla, niitä ei havaita. Tämä on omiaan vaikuttamaan vastausvaihtoehdon valintaan.



KUVIO 16. Uhkatilanteiksi tunnistettujen tapausten esiintyminen yrityksissä (N=20)

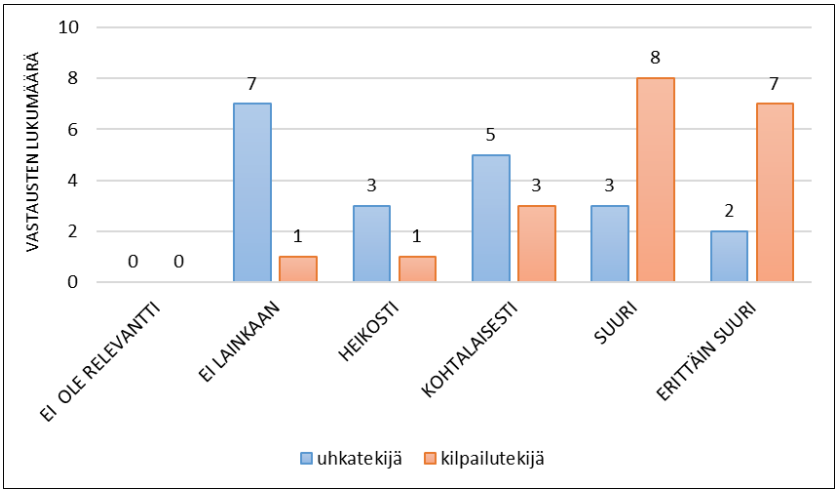
Kyberturvallisuus voidaan kokea yrityksessä monella eri tavalla. Joissakin yrityksissä se voidaan kokea yrityksen toimintaa haittaavana tekijänä ja uhkana, mutta toisten mielestä se voi olla mahdollistaja, joka hyvin hallittuna voi antaa kilpailuetua suhteessa muihin vastaavan alan yrityksiin.

Yrityksiltä kysyttiin mielipidettä siitä, koetaanko kyberturvallisuus uhkatekijänä vai kilpailutekijänä. Yhteensä seitsemän (7) yritystä kahdestakymmenestä vastasi, että kyberturvallisuus ei ole lainkaan uhkatekijä. Kolme (3) vastaajaa oli sitä mieltä, että se on ”heikosti” uhkatekijä ja viisi (5) vastaajaa piti sitä ”kohtalaisena” uhkatekijänä.

Kolmen (3) vastaajan mielestä kyberturvallisuus on suuri uhkatekijä ja kaksi (2) vastaajaa oli sitä mieltä, että se on erittäin suuri uhkatekijä.

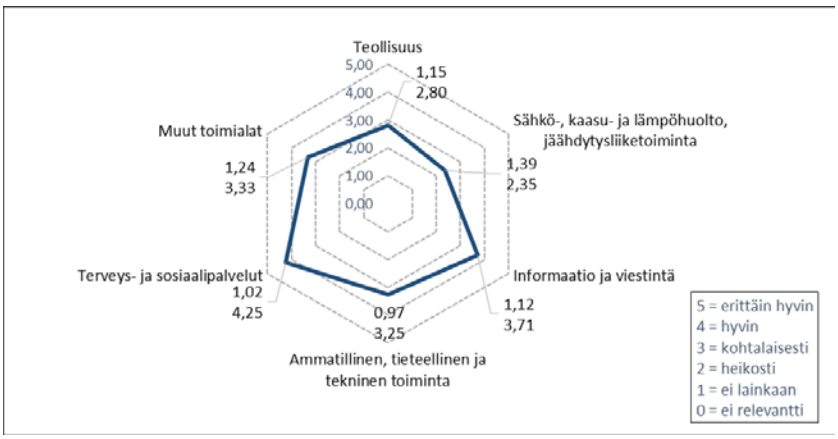
Kilpailutekijäksi kyberturvallisuutta ei yksi (1) yritys mieltänyt lainkaan ja yksi yritys vain ”heikosti”. Kolme (3) yritystä ajattelee kyberturvallisuutta ”kohtalaisena” kilpailutekijänä, kahdeksan (8) yritystä suurena kilpailutekijänä ja seitsemän (7) yritystä ”erittäin suurena” kilpailutekijänä.

Kuvio 17 havainnollistaa yritysten näkemystä kyberturvallisuuden roolista uhkatekijänä tai kilpailutekijänä. Tarkoituksellisen vastakkainasettelun vuoksi yritysten vastaukset tähän kysymyspariin ovat lähes kääntäen verrannolliset.



KUVIO 17. Kyberturvallisuuden rooli uhkatekijänä vs. kilpailutekijänä (N=20)

Kysymyssarjaan annettuja vastauksia voidaan kokonaisuutena tarkastella myös vastaajayritysten toimialan mukaisesti. Tässä tutkimuksessa olivat edustettuina Tilastokeskuksen toimialaluokituksen (TOL) mukaisesti seuraavat toimialat: C. Teollisuus (yritysten lukumäärä 2); D. Sähkö-, kaasu ja lämpöhuolto, jäähdytysliiketoiminta (2); F. Rakentaminen (1); G. tukku- ja vähittäiskauppa, moottoriajoneuvojen ja moottoripyörien korjaus (1); J. Informaatio ja viestintä (9); K. Rahoitus ja vakuutustoiminta (1); M. Ammatillinen tieteellinen ja tekninen toiminta (2) sekä Q. terveys ja sosiaalipalvelut (2). Koska yritysten lukumäärä rakentamisen, tukku- ja vähittäiskaupan sekä rahoitus ja vakuutustoiminnan toimialoilla oli tässä tutkimuksessa vain yksi, olen vastauksia analysoitaessa yhdistänyt ne samaan luokkaan nimellä ”Muut toimialat”. Näin vältytään siltä tilanteelta, että yksittäisen yrityksen vastaukset tulisivat suoraan esille.



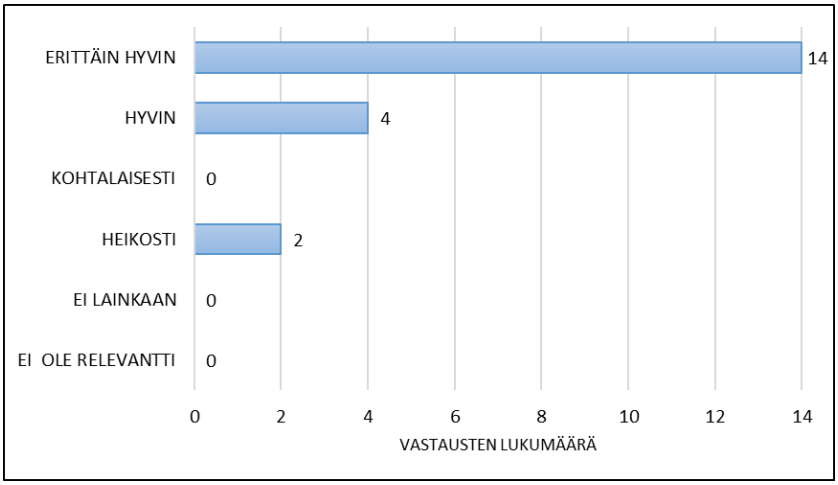
KUVIO 18. Kysymyssarjaan yksi annettujen vastausten toimialakohtaiset keskiarvot ja –hajonnat (N=200)

Kuvio 18 näyttää havainnollisesti miten eri toimialojen yritykset vastasivat kysymyssarjan yksi kysymyksiin. Verrattaessa vastauksia, niiden keskiarvoja sekä keskihajontoja eri toimialojen yritysten välillä on mukana kaikki annetut vastaukset mukaan lukien edellä mainitut kyberuhkiin liittyvät vastaukset. Koska vastauksia tarkastellaan kaikkien osallistuvien yritysten näkökulmasta samalla tavalla ovat ne sellaisenaan keskenään vertailukelpoisia. Suurin numeraalinen vastauskeskiarvo 4,25 (keskihajonta 1,02) saadaan terveys ja sosiaalipalvelujen toimialaa edustavilta yrityksiltä. ”Sähkö-, kaasu- ja lämpöhuolto, jäähdytysliiketoiminta” –toimialan yritykset puolestaan saavuttivat vastauskeskiarvokseen 2,35 (1,39), mikä antaa huomattavan eroon vertailtaessa eri toimialojen yrityksiä keskenään. Tarkastelussa on kuitenkin otettava huomioon se, että tutkimukseen osallistuneiden yritysten lukumäärä oli yhteensä 20 yritystä ja tuloksia analysoitaessa yksittäisen toimialan yritysten määrä on kaksi tai sitä enemmän. Tulokset ovat siten suuntaa antavia, mutta niiden perusteella ei voida vetää pitkälle meneviä johtopäätöksiä. Kuitenkin kuvio 18 osoittaa, että tutkimukseen osallistuvien yritysten kesken oli vastauksissa suuria eroja.

6.2.2 Tutkimuskysymys 2: Miten yritys on tunnistanut tiedon ja sen turvallisen käsittelyn merkityksen liiketoiminnalle?

Toisen kysymyssarjan työnimi on ”2. Tieto ja sen merkitys liiketoiminnalle”. Siihen sisältyi haastatteluvaiheessa 11 kysymystä. Analyysivaiheen aikana siirsin ensimmäisestä kysymyssarjasta yhden kysymyksen tähän sarjaan, johon se soveltui sisällöllisesti paremmin.

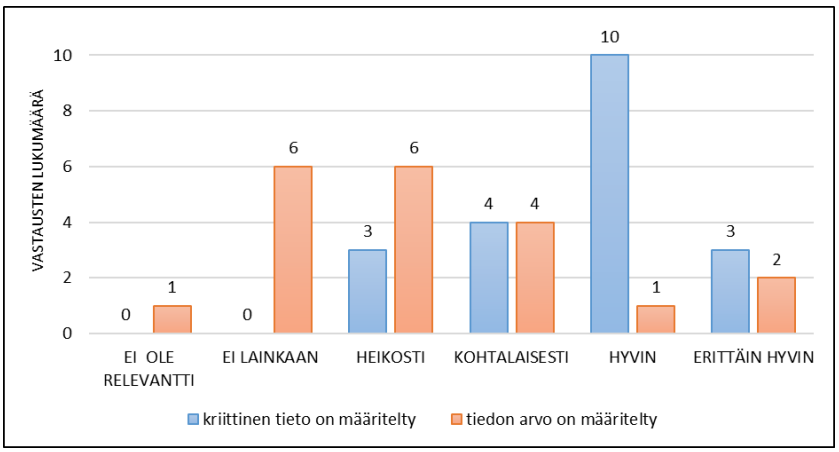
Toinen kysymyssarja aloitettiin väittämällä ”tieto on tunnistettu osaksi yrityksen omaisuutta”(asset). Kysymykseen vastasi 14 yritystä kahdestakymmenestä vaihtoehdolla ”erittäin hyvin” ja neljä (4) yritystä vastasi ”hyvin”. Jäljelle jääneet kaksi (2) yritystä valitsivat molemmat vaihtoehdon ”heikosti”. Kuvio 19 havainnollistaa jakauman yritysten vastauksista, joiden keskiarvoksi muodostuu koko haastattelututkimuksen korkein lukema 4,50.



KUVIO 19. Tiedon arvostaminen yrityksen omaisuutena (N=20)

Seuraavaksi pureuduttiin yrityksen hallussa olevan tieto-omaisuuden ja sen arvon määrittelyyn. Väittämän ”yrityksen liiketoiminnan kannalta kriittinen tieto omaisuus on määritelty” avulla pyrittiin selvittämään, missä määrin yritykset ovat analysoineet hallussaan olevaa tietoa ja onko sieltä löydetty liiketoiminnan kannalta kriittisiä osia. Kysymyspariin toisella kysymyksellä haluttiin selvittää, onko tieto-omaisuudelle määritelty arvo. Arvoa voidaan ajatella esimerkiksi taloudellisena arvona tai liiketoiminnallisena arvona eli hyötynä liiketoiminnalle.

Kuvio 20 osoittaa, että yhteensä 13 vastaajaa ilmoitti, että kriittisen tieto-omaisuuden määrittely on yrityksessä vähintään ”hyvällä” tasolla. Neljä (4) vastaajaa valitsi vaihtoehdon ”kohtalaisesti” ja kolme (3) vastaajaa päätyi vaihtoehtoon ”heikosti”. Tieto-omaisuuden arvon määrittelyssä yritykset ovat vastaustensa perusteella enemmän vielä alkutaipaleella. Kuusi (6) yritystä ei ollut määritellyt tieto-omaisuutensa arvoa lainkaan. Samoin kuusi (6) yritystä oli pohtinut asiaa ”heikosti” ja neljä (4) yritystä ”kohtalaisesti”. Yksi (1) yritys oli määritellyt tieto-omaisuutensa arvon ”hyvin” ja kaksi (2) yritystä ”erittäin hyvin”. Yhden vastaajan mielestä asia ei ollut relevantti yrityksen kannalta.

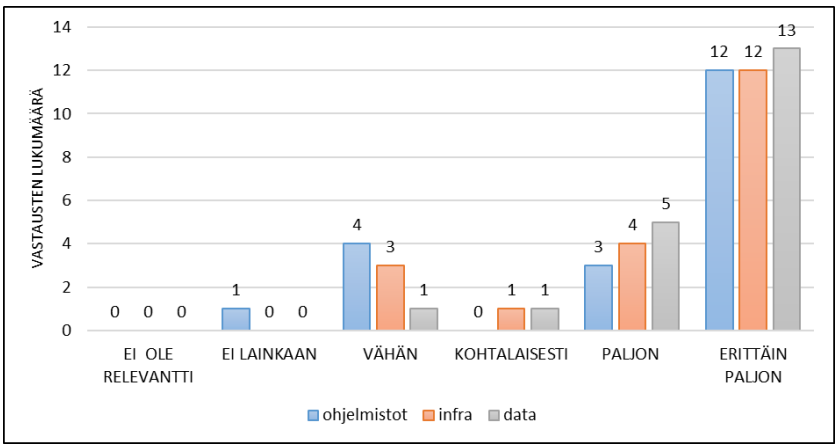


KUVIO 20. Tieto-omaisuuden ja sen arvon määrittelyn tilanne vastaajayrityksissä (N=20)

Kolmen kysymyksen sarjalla haluttiin selvittää, mistä osatekijöistä yrityksen liiketoiminnan kannalta kriittinen tieto-ominaisuus koostuu. Teema jaettiin kolmeen kysymykseen, koska tutkimustyön perusperiaatteiden vuoksi yhdessä kysymyksessä voidaan kysyä vain yhtä asiaa. Kolme tarkasteltavaa näkökulmaa olivat ohjelmistot, tietotekninen infrastruktuuri eli fyysiset koneet, laitteet ja järjestelmät sekä kolmantena näkökulmana oli tietojärjestelmiin tallennettu ja niissä käsiteltävä data. Kuvio 21 osoittaa havainnollisesti, että yritysten vastaukset näihin kolmeen kysymykseen olivat melko suuressa määrin samansuuntaisia. Ohjelmistoista koostuu tieto-omaisuus 12 yrityksillä ”erittäin paljon”, kolmella (3) yrityksellä ”paljon”, neljällä (4) yrityksellä vain vähän ja yhdellä (1) yrityksellä ei lainkaan.

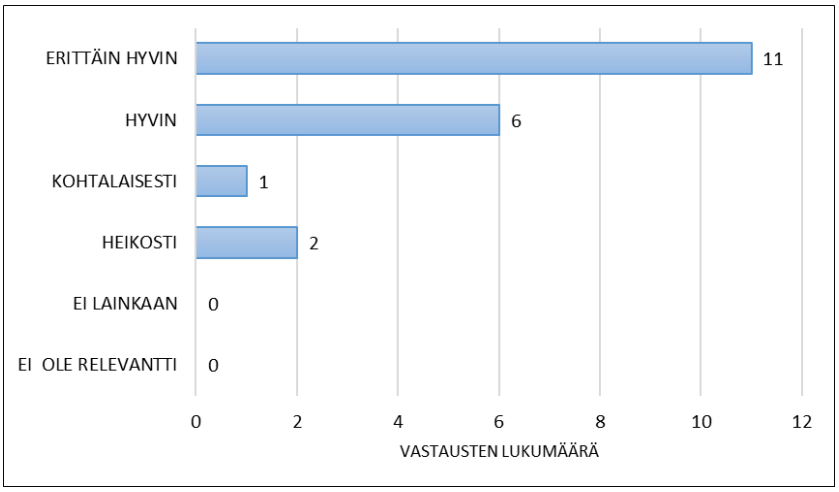
Yrityksen kriittiseen tieto-omaisuuteen sisältyy liiketoiminnan kannalta elintärkeää infraa 12 yrityksellä ”erittäin paljoin”, neljällä (4) yrityksellä ”paljon”, yhdellä (1) yrityksellä ”kohtalaisesti” ja kolmella yrityksellä ”vähän”. Yrityksen kriittiseen tieto-omaisuuteen sisältyy liiketoiminnan kannalta elintärkeää luottamuksellista tietoa/dataa yhteensä 13 yrityksellä ”erittäin paljon” ja viidellä yrityksellä paljon”. Yhdellä yrityksellä on hallussaan liiketoimintakriittiseksi luokiteltavaa dataa ”kohtalaisesti” ha yhdellä yrityksellä vain ”vähän”.

Vastaukset tähän kolmen kysymyksen sarjaan korreloivat melko hyvin edellä kuvioissa 19 ja 20 esitettyihin vastauksiin. Suurimmalla osalla vastanneista yrityksistä näyttäisi olevan kohtalaista parempi käsitys hallussaan olevasta liiketoimintakriittisestä tieto-omaisuudestaan.



KUVIO 21. Liiketoimintakriittisen tieto-omaisuuden koostumus (N=20)

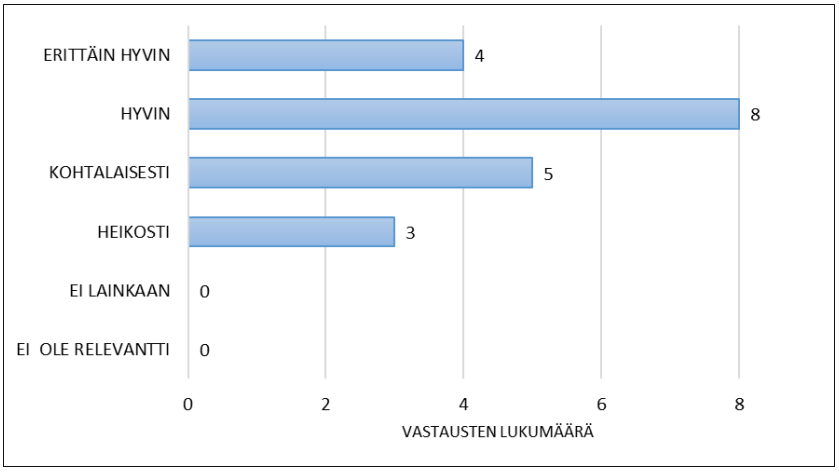
Koska edellisten kysymysten vastausten perusteella yritysten liiketoimintakriittiseen tieto omaisuuteen sisältyi suuressa määrin dataa, saattoi helposti olettaa, että tieto sekä sen käsittelyyn liittyvät riskit ovat merkittäviä yritysten liiketoiminnan kannalta. Tähän väittämään vastasi - kuten kuvio 22 osoittaa - yhteensä kuusi (6) yritystä siten, että riskit ovat ”hyvin” merkittäviä ja 11 yritystä, että riskit ovat ”erittäin hyvin” merkittäviä. ”Kohtalaisen” merkittävinä riskejä piti vain yksi (1) yritys ja ”heikosti” merkittävinä kaksi (2) yritystä. Merkillepantavaa on se, että jokaisessa yrityksessä koettiin tietoon ja sen käsittelyyn liittyvien riskien vaikuttavan toteutuessaan yrityksen liiketoimintaan.



KUVIO 22. Tietoon ja sen käsittelyyn liittyvien riskien merkittävyys liiketoiminnalle (N=20)

Yrityksen tieto-omaisuuden hallinnan merkitys korostuu erityisesti digitalisaation etenemisen myötä. Hallinnan tulee olla suunnitelmallista ja yrityksellä tulee olla selkeä käsitys siitä, miten tieto-omaisuutta säilytetään, suojataan, hyödynnetään, miten sen

arvoa ja merkitystä ymmärretään ja mitataan sekä siitä, miten tieto-omaisuuteen voidaan luottaa. Yrityksiltä kysyttiin, missä määrin niillä on selkeä käsitys siitä, miten tieto-omaisuutta tulee hallita nyt ja tulevaisuudessa. Viidesosa (4/20) yrityksistä vastasi omaavansa ”erittäin hyvän” käsityksen tieto-omaisuutensa hallinnasta. Kaksi viidesosaa (8/20) yrityksistä piti käsitystään ”hyvänä”, viisi (5) yritystä oli muodostanut mielestään ”kohtalaisen” käsityksen asiasta ja kolmella (3) yrityksellä käsitys oli vastauksensa perusteella vielä ”heikolla” tasolla. Kuten kuvio 23 osoittaa, painottuu yli puolet vastauksista vaihtoehtoihin ”hyvin” ja ”erittäin hyvin”. Tästä voidaan päätellä, että yritykset ovat keskuudessaan, mutta dokumentointia ei erikseen kysytty.

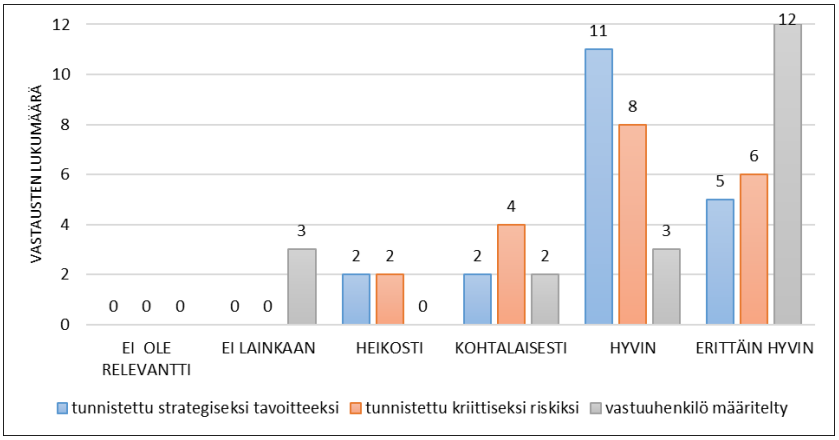


KUVIO 23. Yritysten käsityksen taso tieto-omaisuutensa hallinnasta nyt ja tulevaisuudessa (N=20)

Kyberturvallisuusuhkat saattavat toteutuessaan aiheuttaa vaaraa yrityksen liiketoiminnalle todennäköisesti sitä enemmän, mitä suurempi osuus yrityksen liiketoiminnasta perustuu digitalisaatioon. Digitaalisen jatkuvuuden hallinta on riskienhallinnan osa-alue, joka yrityksen tai muun organisaation on suunniteltava kyberturvallisuusuhkien toteutumisen varalle. Yrityksiltä kysyttiin digitaalisesta jatkuvuudenhallinnan nykytilaa kolmella eri kysymyksellä. Niistä ensimmäisessä saivat yritykset vastata siihen, missä määrin digitaalisen jatkuvuuden hallinta on tunnistettu yhdeksi strategiseksi tavoitteekseen yrityksessä. Seuraava väittämä sisälsi kysymyksen siitä, onko mahdollinen digitaalisen jatkuvuuden hallinnan menetys tunnistettu yhdeksi yrityksen kriittisistä riskeistä. Kolmantena teemaan liittyvänä asiana kysyttiin, onko yrityksessä määritelty vastuuhenkilö digitaalisen jatkuvuuden hallinnalle.

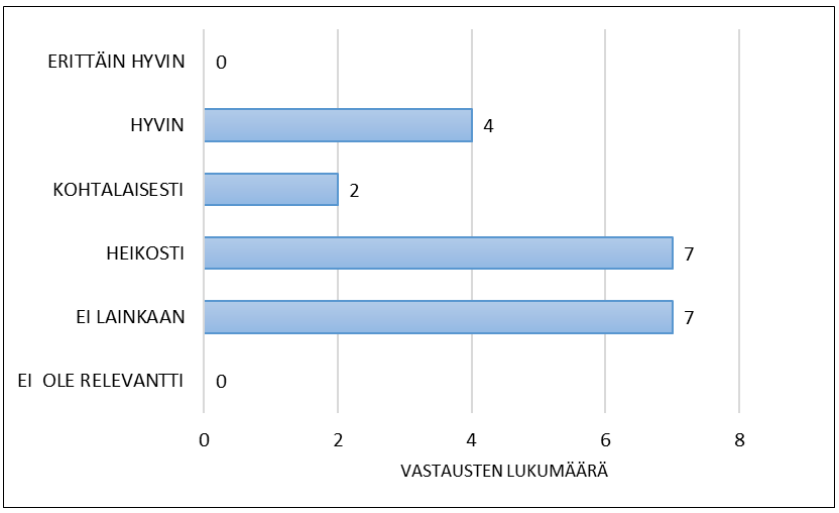
Yrityksistä viisi (5) ilmoitti vastauksessaan, että jatkuvuuden hallinta on tunnistettu strategiseksi tavoitteeksi ”erittäin hyvin”. Yksitoista (11) yritystä oli tunnistanut sen

tavoitteeksi ”hyvin”, kaksi (2) yritystä ”kohtalaisesti” sekä kaksi (2) yritystä ”heikosti”. Digitaalisen jatkuvuuden hallinnan menetys oli tunnistettu kuudessa (6) yrityksissä riskiksi ”erittäin hyvin”, kahdeksassa (8) yrityksessä hyvin, neljässä (4) yrityksessä kohtalaisesti ja kahdessa (2) yrityksessä heikosti. Digitaalisen jatkuvuuden hallintaa varten oli kaksitoista yritystä ilmaisi nimittäneenä vastuuhenkilön ”erittäin hyvin”, kolme (3) yritystä ”hyvin” ja kaksi (2) yritystä kohtalaisesti. Kolmessa (3) yrityksessä ei oltu vielä määritelty vastuuhenkilöä. Kuten kuvio 24 havainnollistaa, näkyvät kysymyksen keskinäiset riippuvuudet näkyvät yritysten antamissa vastauksissa. Vastausten perusteella voidaan myös todeta, että osa yrityksistä on ja alkanut käytännön toimenpiteisiin määrittelemällä vastuuhenkilön digitaalisen jatkuvuuden hallinnan turvaamiseksi.



KUVIO 24. Digitaalisen jatkuvuudenhallinnan merkitys yrityksille (N=20)

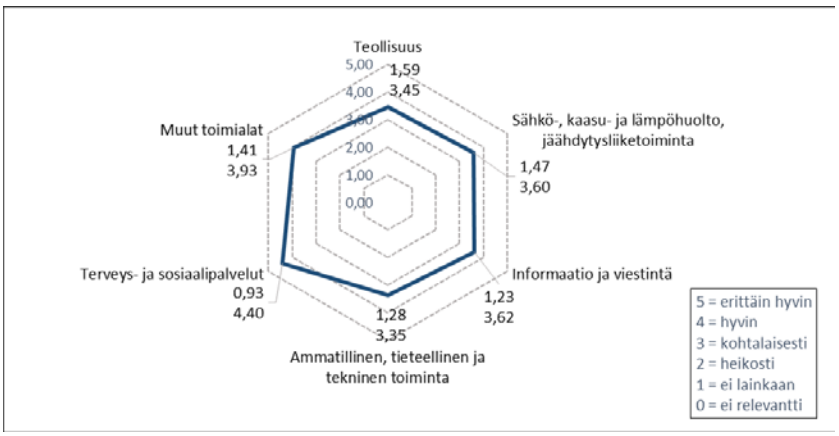
Palautumissuunnitelma kyberturvallisuusuhkan realisoitumisen varalle on yksi tärkeä osa digitaalisen jatkuvuuden hallintaa. Sen tulisi olla dokumentoitu kirjalliseen muotoon ja siihen liittyvät toimenpiteet ja vastuut tulisi olla selkeitä kaikille niille tahoille, joita asia koskettaa. Yrityksille esitettiin väittämä ”kyberturvallisuusuhkien varalta on dokumentoitu varautumissuunnitelma, jolla pyritään varmistamaan digitaalinen jatkuvuus”. Väittämään vastasi seitsemän (7) yritystä vaihtoehdolla ”ei lainkaan” ja sama määrä yrityksiä valitsi vaihtoehdon ”heikosti”. Kysymykseeni vastasi kaksi (2) yritystä ”kohtalaisesti” ja vaihtoehdon ”hyvin” valitsi neljä (4) yritystä. Yksikään yrityksistä ei valinnut vaihtoehtoa ”erittäin hyvin”. Kuvio 25 havainnollistaa yritysten antamien vastausten jakaumaa, jonka perusteella voidaan todeta, että tutkimukseen osallistuneilla yrityksille on vielä tehtävää digitaalisen jatkuvuuden hallinnan turvaamiseksi.



KUVIO 25. Dokumentoidun palautumissuunnitelman valmiustilanne yrityksissä (N=20)

Kysymyssarjaan ”2. Tieto ja sen merkitys liiketoiminnalle” annettuja vastauksia toimialakohtaisesti tarkasteltuna voidaan todeta, että toimialojen väliset erot olivat selkeästi pienempiä kuin kysymyssarjassa ”1. Käsitteet ja strategianäkökulma”.

Myös tässä kysymyssarjassa ”terveys ja sosiaalipalvelut” -toimiala erottui edukseen. Toimialan yritysten antamien kaikkien vastausten keskiarvo on 4,4 ja keskihajonta oli 0,93. Siitä huolimatta, että kysymyssarjan kysymykset painottuvat melko selkeästi perinteiselle ICT-toimialalle tuttuihin asioihin, ei ”informaatio ja viestintä” -toimialan yritysten vastausten keskiarvo nouse lähellekään ”terveys ja sosiaalipalvelut” -toimialan yritysten antamien vastausten keskiarvoa, kuten kuvio 26 havainnollisesti esittää.

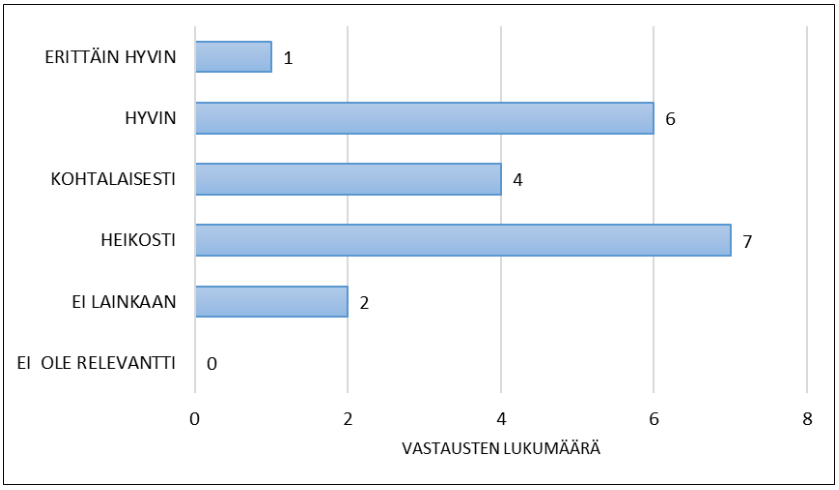


KUVIO 26. Kysymyssarjaan kaksi annettujen vastausten toimialakohtaiset keskiarvot ja –hajonnat (N=240)

6.2.3 Tutkimuskysymys 3: Miten yrityksen toimintaprosesseissa on otettu kyberturvallisuus huomioon?

Kolmannessa kysymyssarjassa työnimeltään ”3. Prosessit” haettiin vastauksia siihen, miten yritykset ovat toimintaprosesseissaan ottaneet kyberturvallisuuden huomioon. Kysymyssarja koostuu 15 kysymyksestä, jotka käsittelevät yrityksen toimintaa käytännön tasolla.

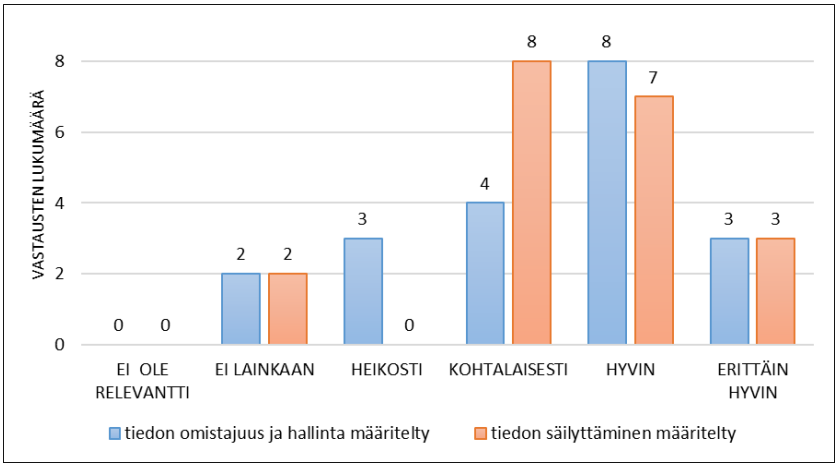
Sarjan ensimmäisenä kysymyksenä yritykselle esitettiin väittämä ”yrityksessä on määritelty ja dokumentoitu turvallisuuteen liittyvät vastuut ja päätösvalta”. Kysymykseen vastasi vaihtoehdolla ”erittäin hyvin” vain yksi (1) yritys. Asia oli kuuden (69 yrityksen mielestä ”hyvällä” tasolla ja neljän (4) vastaajan mielestä kohtalaisella tasolla. Asian määrittely oli toteutunut ”heikosti” seitsemän (7) vastaajan yrityksessä, eikä sitä oltu tehty lainkaan kahden (2) vastaajan yrityksessä. Kuvio 27 kuvaa vastausten jakaumaa, joka on edellisten kysymyssarjojen vastaukset huomioon ottaen huomattavan paljon painottunut vastauksiin ”heikosti” ja ”ei lainkaan”. Lähes puolet (9/20) yrityksistä kuvaa tilannettaan niillä vaihtoehdoilla, mihin todennäköisesti vaikuttaa kysymyksessä esitetty dokumentointivaade.



KUVIO 27. Turvallisuuteen liittyvien vastuiden määrittely ja dokumentointi yrityksissä (N=20)

Turvallisuuteen liittyvien vastuiden lisäksi yrityksessä on hyvä määritellä tiedon hallintaan ja omistajuuteen liittyvät käytänteet. Edelleen on tarpeen määrittää, missä ja miten yrityksen liiketoimintakriittistä tietoa säilytetään. Näitä asioita kysyttiin yrityksiltä kysymysparilla, joista ensimmäinen väittämä kuului ”tiedon omistajuus ja hallinta on määritelty yrityksessä jollekin henkilölle tai henkilöille”. Yrityksistä kolme (3)

vastasi väittämään vaihtoehdolla ”erittäin hyvin” ja kahdeksan (8) yritystä vastasi vaihtoehdolla ”hyvin”. Siis yli puolet yrityksistä olivat vastausten perusteella hoitaneet asiaan hyvin. Neljä (4) yritystä valitsi vaihtoehdon kohtalaisesti, kolme (3) yritystä oli keskittynyt asiaan ”heikosti” ja kaksi (2) yritystä ”ei lainkaan”. Toisena kysymyksenä yritykset saivat vastata väittämään ”yrityksessä on määritelty ja dokumentoitu, missä ja miten yrityksen liiketoimintakriittistä tietoa säilytetään”. Tähän kysymykseen valitsi kolme (3) yritystä vaihtoehdon ”erittäin hyvin” ja seitsemän (7) yritystä vastasi vaihtoehdolla ”hyvin”. Kahdeksan (8) yritystä oli hoitanut asiaa ”kohtalaisesti” mutta kaksi (2) yritystä ”ei lainkaan”. Kuvio 28 havainnollistaa yritysten vastaukset tähän kysymyspariin.

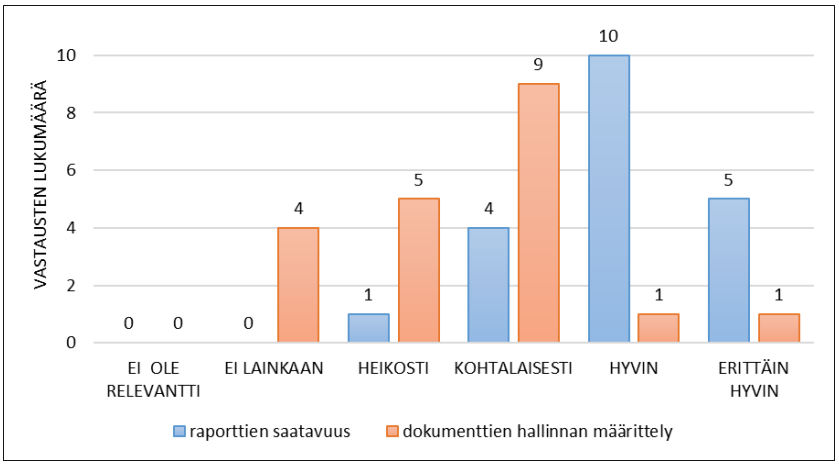


KUVIO 28. Liiketoimintakriittisen tiedon omistajuuden, hallinnan ja säilyttäminen määrittely (N=20)

Yksi osa liiketoimintakriittisen tiedon tuottamista ja käsittelyä on asiakirjahallinta sekä siihen liittyvät ohjeet ja käytänteet. Teemaan liittyvän kysymysparin ensimmäisessä kysymyksessä haettiin vastausta siihen, missä määrin yrityksen tietojärjestelmistä on saatavissa raportteja, jotka sisältävät liiketoiminnan kannalta käyttökelpoista, ajantasaista ja luotettavaa tietoa. Viisi (5) yritystä kahdestakymmenestä vastasi kysymykseen vaihtoehdolla ”erittäin hyvin” ja 10 yritystä valitsi vaihtoehdon ”hyvin”. Kolme neljäsosaa vastaajista oli siis sitä mieltä, että raporttien tuottaminen on vähintään hyvällä tasolla. Neljä (4) yritystä oli raportoinnin suhteen vaihtoehdon ”kohtalaisesti” kannalla ja yksi (1) yritys vastasi kysymykseen valitsemalla vaihtoehdon ”heikosti”.

Toisena kysymysparin osana esitettiin väittämä ”yrityksessä on määritelty ja dokumentoitu, miten nimetään ja kuvataan tietojärjestelmissä tuotettavat ja säilytettävät

dokumentit”. Neljä (4) yritystä vastasi, että kysytty asiaa ei ole tehty lainkaan. Viiden (5) vastaajan mielestä asia oli hoidettu ”heikosti” ja yhdeksän (9) vastaajaa oli sitä mieltä, että asia on järjestetty ”kohtalaisesti”. Yhteensä 18 vastaajaa kahdestakymmenestä oli sitä mieltä, että kysytyt toimenpiteet on tehty enintään ”kohtalaisella” tasolla. Yksi (2) yritys vastasi kysymykseen ”hyvin” ja yksi yritys ”erittäin hyvin”. Kuviosta 29 on nähtävissä havainnollisesti, miten yritysten vastaukset hajaantuvat tämän kysymysparin kohdalla.



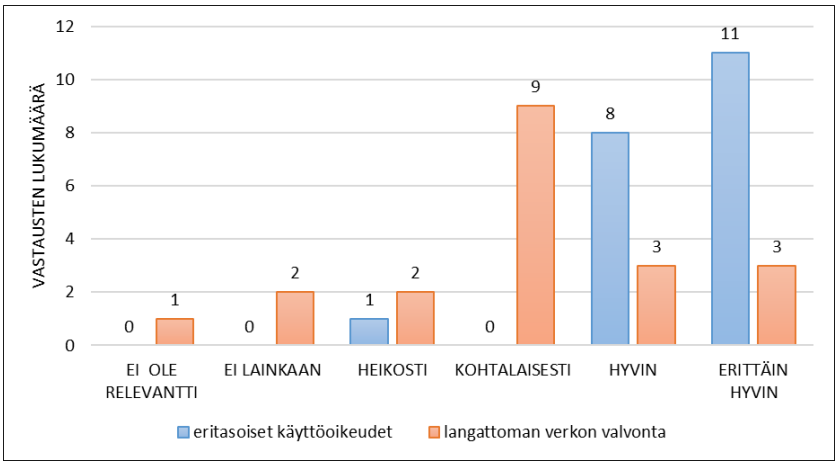
KUVIO 29. Liiketoiminnan raporttien tuottaminen ja dokumenttien hallinnan määrittely (N=20)

Käyttöoikeuksien hallinta muodostaa osan yrityksen tietoturvapolitiikasta. Siihen määriteltyjen periaatteiden avulla hallinnoidaan yrityksen tietojärjestelmien käyttöä ja ohjataan tietojen hallintaa. Melko yleisesti käytetään henkilökohtaisia tai tehtävä-/roolikohtaisia käyttöoikeuksia, jotka perustuvat työ- tai palvelussuhteeseen tai muuhun kirjalliseen työtehtävien kuvaukseen. Käyttöoikeuksia tietojärjestelmiin lisätään tai vähennetään työtehtävien muuttuessa.

Käyttöoikeuksien ja tietojärjestelmien pääsynhallintaan liittyen yrityksille esitettiin kysymyksen muotoinen väittämä ”yrityksen tietojärjestelmien pääsy on jaoteltu vähintäänkin niin sanotun etuoikeutetun käyttäjän ja tavanomaisen käyttäjän käyttöoikeuksiin”. Yli puolet vastaajista eli tässä tapauksessa 11 yritystä vastasi vaihtoehdolla ”erittäin hyvin”. Kahdeksan (8) yritystä valitsi vaihtoehdon ”hyvin” ja yksi (1) yritys valitsi vaihtoehdon ”heikosti”.

Kysymysparin toisena osana kysyttiin ”millä tavoin yrityksen langattomien verkkojen sisäänpääsyä valvotaan”. Yhdessä (1) yrityksessä kysymys ei ollut vastaajan mielestä relevantti. Kahdessa (2) yrityksessä valvontaa ”ei toteutettu lainkaan” ja kahdessa (2)

yrityksessä ”heikosti”. Yhdeksän (9) yritystä valvoo langattomien verkkojen sisäänpääsyä mielestään ”kohtalaisesti”, kolme (3) yritystä ”hyvin” ja kolme yritystä ”erittäin hyvin”. Kysymyspariin liittyviä vastauksia havainnollistetaan kuviossa 30, jossa on hyvin näkyvissä, että käyttöoikeuksien hallinta on yritysten vastausten mukaan kokonaisuudessaan hyvällä tasolla.



KUVIO 30.Roolipohjaisten käyttöoikeuksien ja langattoman verkon pääsynhallinta (N=20)

Pääsy liiketoimintakriittiseen tieto-omaisuuteen on asia, jota voidaan hallinnoida roolipohjaisilla käyttöoikeuksilla. Yhtenä hyvänä käytänteenä kullekin yrityksen tietojärjestelmälle nimetään omistajataho, joka on tietoinen siitä, kenellä on kyseiseen tietojärjestelmään pääsy ja minkä tasoiset käyttöoikeudet ovat kullakin käyttäjällä. Tietojärjestelmien käyttöoikeudet olisi myös syytä aika-ajoin katselmoida ja tehdä sen perusteella tarvittavat muutokset. Tätä seurantaa voidaan tehdä esimerkiksi tietoturvan omavalvontasuunnitelman avulla.

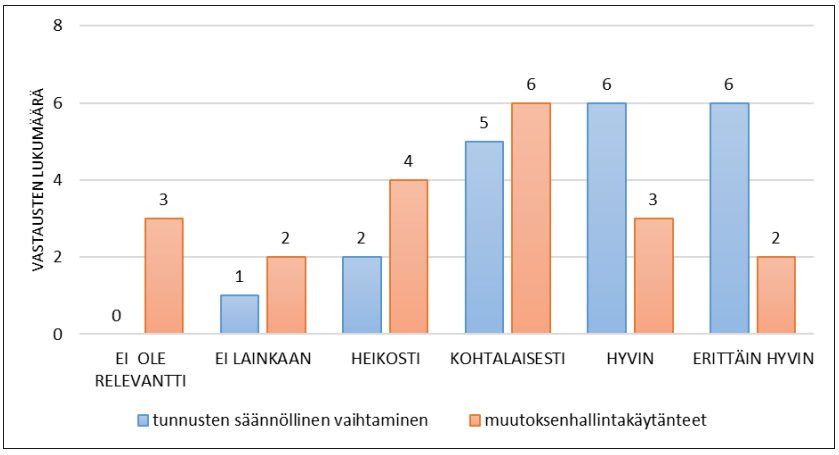
Yrityksille esitettiin kysymys liiketoimintakriittiseen tieto-omaisuuteen pääsyn seurannasta ja pääsyyn oikeuttavien tietojärjestelmien tunnusten säännöllisestä vaihtamisesta. Kysymykseen vastasi kuusi (6) yritystä vaihtoehdolla ”erittäin hyvin” ja kuusi (6) yritystä vaihtoehdolla ”kohtalaisesti”. Yrityksistä kaksi (2) vastasi vaihtoehdolla ”heikosti” ja yksi (1) yritys valitsi vaihtoehdoksi ”ei lainkaan”.

Tärkeä osa yrityksen tietoturva ovat muutoksenhallintakäytänteet, jotka voivat koskea muutosten tekemistä tietojärjestelmiin sekä niiden käyttöoikeuksiin ja niiden sisältämiin tietoihin. Tietojärjestelmien muutostenhallinta tulee perustua dokumentoituun suunnitelmaan. Kaikista muutoksista tulee jäädä dokumentti tai lokitieto, josta

voidaan tarvittaessa jälkikäteen todeta, kuka muutokset on tehnyt ja onko hänellä ollut siihen tarvittavat valtuudet.

Yrityksiltä kysyttiin, missä määrin niissä on määritelty sellaisia muutoksenhallintakäytänteitä, joilla voidaan estää luvattomien muutosten teko yrityksen kannalta kriittisen tietoon tai tietojärjestelmiin. Kaksi (2) yritystä vastasi muutostenhallinnan olevan ”erittäin hyvin” määritelty. Kolmen (3) vastaajan mielestä asia oli hoidossa ”hyvin” ja kuuden (6) vastaajan mielestä ”kohtalaisesti”. Neljässä (4) yrityksessä tilannetta kuvattiin vaihtoehdolla ”heikosti” ja kahdessa (2) yrityksessä vaihtoehdolla ”ei lainkaan”. Kolmen (3) vastaajan mielestä kysymys ei ollut heidän yrityksessä relevantti.

Alla olevasta kuviosta 31 voidaan havainnollisesti todeta yritysten kehityskaaren tämänhetkinen vaihe käyttöoikeuksien hallinnassa ja muutostenhallinta käytänteissä. Tietojärjestelmien käyttöön oikeuttavien tunnusten vaihtaminen on jo käytänteenä hyvällä tasolla, mutta muutostenhallinta käytänteiden suhteen on vielä työtä tehtävänä.



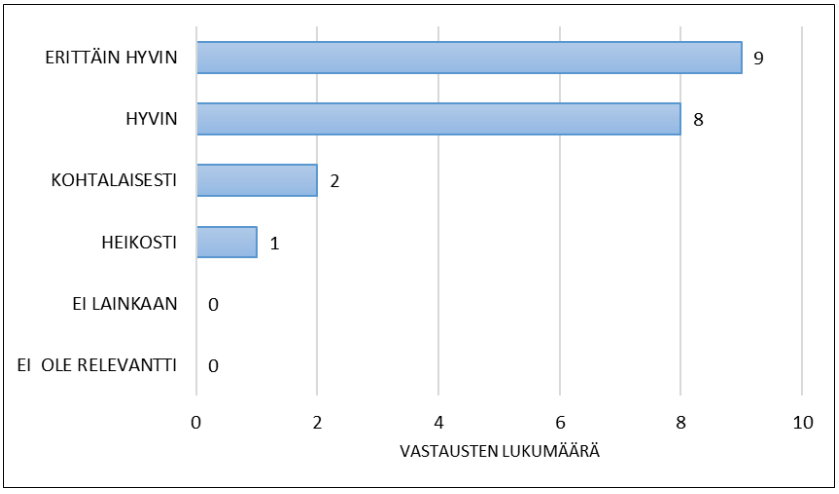
KUVIO 31. Pääsyyn oikeuttavien tunnusten säännöllinen vaihtaminen ja muutostenhallintakäytänteiden olemassaolo (N=20)

Osa yrityksen hallussa olevasta tiedosta on sen liiketoiminnan kannalta kriittistä tietoa ja se voi olla myös liikesalaisuudeksi luokiteltavaa tietoa. Liikesalaisuuden kannalta merkittävä uudistus on parhaillaan eduskunnan käsiteltävänä oleva Suomen hallituksen esitys liikesalaisuuslaiksi (HE 49/2018). Sillä on tarkoitus panna täytäntöön Euroopan parlamentin ja neuvoston liikesalaisuuksien suojaamista koskeva direktiivi, jolla pyritään parantamaan yritysten liikesalaisuuksiin liittyvää turvaa.

Lakiesityksen mukaan yrityksen liikesalaisuus on luonteeltaan salaista tietoa, joka ei ole julkisesti saatavissa eikä se ole yrityksen toimialalla yleisesti tunnettua. Liikesalaisuuden tunnusmerkkinä on myös se, että tiedolla on yrityksen elinkeinotoiminnan kannalta taloudellinen arvo, sikäli kun se pysyy salaisena. (Hallituksen esitys eduskunnalle liikesalaisuuslaiksi ja eräiksi siihen liittyviksi laeiksi. HE 49/2018 2018, 137.)

Jos tieto vuotaa luvattomiin käsiin, se heikentää yrityksen kilpailukykyä ja taloudellista asemaa. Tieto voi kuitenkin olla jaettua tietoa esimerkiksi toisen saman toimialan yrityksen kanssa. Liikesalaisuuden haltijan on pidettävä liikesalaisuudeksi määrittelemänsä tieto salassa ja ohjeistamaan tietoa käsitteleviä henkilöitä pitämään tiedon luottamuksellisena. Tiedon salassapitoon voidaan käyttää avuksi salassapitosopimuksia ja ottaa käyttöön tietojärjestelmiin sekä fyysisiin tiloihin vaikuttavia pääsynhallintaratkaisuja.

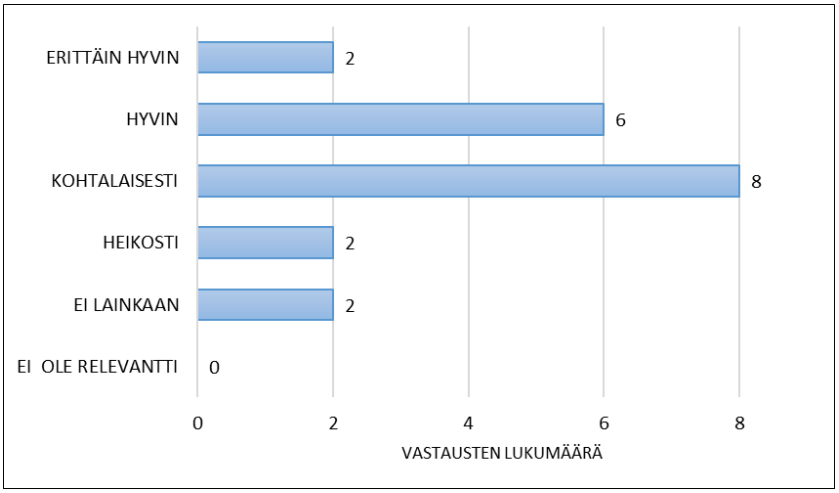
Tutkimushaastattelussa yrityksille esitettiin väittämä ”yrityksen kaikki ei-julkinen tieto on suojattu niin, että luvaton pääsy siihen käsiksi on estetty.” Yhdeksän (9) yritystä kahdestakymmenestä vastaajasta valitsi vastausvaihtoehdoksi ”erittäin hyvin”, kahdeksan (8) yritystä oli hoitanut asian mielestään ”hyvin”, kaksi (2) yritystä ”kohtalaisesti” ja yksi (1) yritys heikosti. Kuvio 32 osoittaa, että tiedon suojaamiseen on yrityksissä panostettu ja se on kokonaisuutena vastaajien keskuudessa vähintäänkin hyvällä tasolla.



KUVIO 32. Ei-julkisen tiedon suojaamisen aste tutkimukseen osallistuneissa yrityksissä (N=20)

Yritysten hallinnassa olevan tiedon määrä kasvaa koko ajan ja osa aikaisemmin analogisesta tiedosta muuttuu digitaaliseen muotoon. Tietojenkäsittelyn liittyviä prosesseja on tämän vuoksi tarpeen tarkastella ja tehdä niihin mahdollisia muutoksia, jotta pyrittäisiin tai kyettäisiin hyödyntämään hallussa oleva tieto kustannustehokkaasti ja samalla suojaamaan tiedon liiketoimintakriittinen osuus sekä varmistamaan tietosuojasta edellytettyjen vaatimusten täyttyminen.

Tähän liittyen yrityksille esitettiin väittämänä ”yrityksessä seurataan ja arvioidaan tietojenkäsittelyn liittyviä prosesseja ja niiden tehokkuutta”. Yrityksistä kaksi (2) vastasi kysymykseen vaihtoehdolla ”erittäin hyvin”, kuusi (6) yritystä suoriutuu tästä mielestään ”hyvin” ja kahdeksan (8) yritystä kohtalaisesti. Kahdessa (2) yrityksessä seurantaa ja arviointia tehdään ”heikosti” ja kahdessa (2) yrityksessä ei lainkaan. Kuvio 33 kuvaa vastausten jakauma osoittaen havainnollisesti, että tietojenkäsittelyn liittyvät prosessit eivät ole tutkimukseen osallistuneiden yrityksen vahvana prioriteettina: Tulos on sikäli mielenkiintoinen, että tutkimukseen osallistuneista yrityksistä yhdeksän yritystä kahdestakymmenestä sijoittuu informaatio ja viestintä –toimialalle.

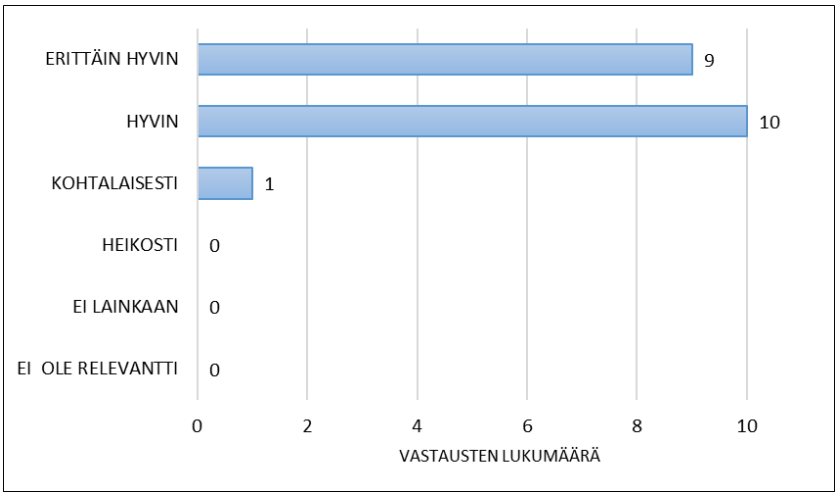


KUVIO 33. Tietojenkäsittelyyn liittyvien prosessien seuranta ja arviointi (N=20)

Riskienhallinta on keskeinen osa myös pk-yrityksen strategista johtamista. Digitalisaation myötä useilla yrityksillä on käytössään aikaisempaa enemmän informaatioteknologiaa, siihen liittyviä palveluja sekä liiketoiminnan kannalta merkittävää ja kriittistä tietoa.

Osana tutkimusta haluttiin yrityksiltä selvittää, missä määrin niissä on tunnistettu tarvetta käytössään olevaan informaatioteknologiaan ja -palveluihin liittyvien riskien

hallinnalle. Vastauksissaan yritykset olivat hyvin pitkälti yksimielisiä. Yhdeksän (9) yritystä oli tunnistanut tarpeen ”erittäin hyvin”. Puolet kaikista vastanneista eli kymmenen (10) yritystä oli tunnistanut riskienhallinnan tarpeen ”hyvin” ja ”kohtalaisesti” vain yksi (1) yritys. Kuviosta 34 on nähtävissä vaihtoehtoihin ”hyvin” ja ”erittäin hyvin” vahvasti painottunut yritysten vastausten jakauma.

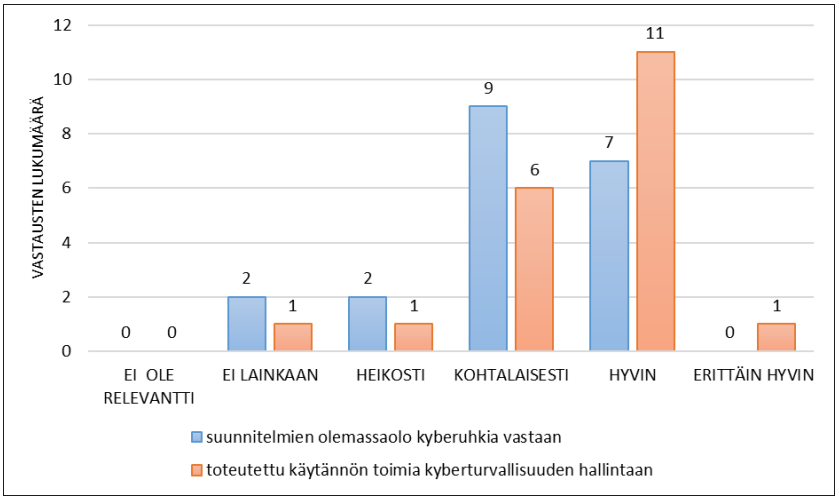


KUVIO 34. Yritysten tunnistama tarve informaatioteknologiaan liittyvien riskien hallinnalle (N=20)

Tässä prosesseihin liittyvässä kysymyssarjassa tarkasteltiin myös suoraan kyberturvallisuuteen liittyviä näkökulmia. Yrityksiltä haluttiin selvittää, missä määrin yritykset ovat suunnitelmatasolla ja toisaalta käytännön tasolla varautuneet kyberturvallisuusuhkiin. Kysymysparin ensimmäisessä kysymyksessä yrityksiltä kysyttiin sellaisten politiikkojen, prosessien, suunnitelmien tai menetelmien olemassaoloa, jotka auttavat niitä vastaamaan kyberturvallisuusuhkiin. Yrityksistä seitsemän (7) valitsi vastausvaihtoehdokseen ”hyvin” ja yhdeksän (9) yritystä vastasi ”kohtalaisesti”. Kahden (2) yrityksen vastaus oli ”heikosti” ja kahdella (2) yrityksellä ”ei lainkaan”. Missään yrityksistä ei ollut varauduttu kyberturvallisuusuhkiin suunnitelmatasolla ”erittäin hyvin”.

Kysymysparin toisessa osassa kysyttiin, missä määrin yrityksissä on käytännössä tehty kyberturvallisuuden hallintaan liittyviä toimenpiteitä. Yritysten vastausten jakauma noudattaa kysymysparin edellisen kysymyksen vastauksia. Yksi (1) vastanneista yrityksistä on tehnyt käytännön toimenpiteitä ”erittäin hyvin” ja 11 yritystä on toteuttanut niitä ”hyvin”. Yrityksistä kuusi (6) on toteuttanut käytännön toimenpiteitä ”kohtalaisesti”, yksi (1) yritys ”heikosti” ja yksi (1) yritys ”ei lainkaan”.

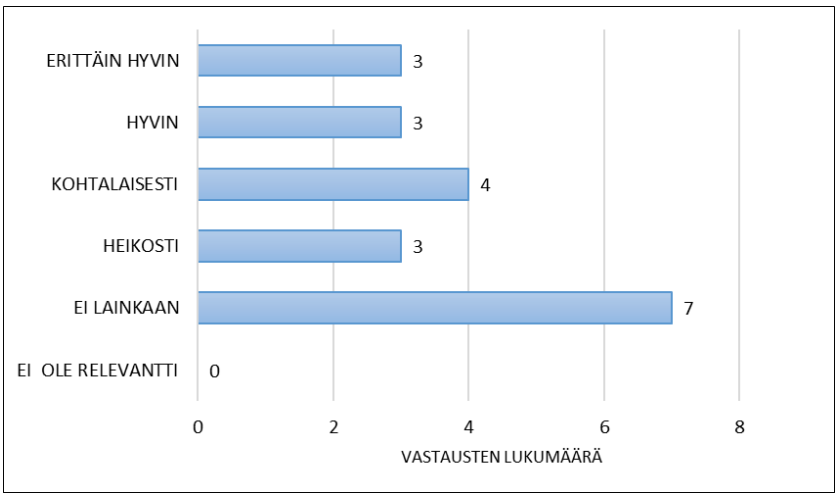
Vastausten jakaumaa osoittavassa kuviossa 35 kiteytyy karkealla tasolla yritysten nykytila kyberturvallisuuden suhteen. Positiivista on se, että toimenpiteitä on vastausten mukaan toteutettu käytännössä enemmän kuin niitä tukevia suunnitelmia on olemassa. Vastanneiden yritysten koko huomioon ottaen tämä on luonnollinen kehityssuunta, koska pienissä yrityksissä suunnitelmien laatimiseen ei useinkaan ole ajallisesti mahdollista riittävästi panostaa henkilöresurssien rajallisuuden vuoksi.



KUVIO 35. Yritysten varautuminen suunnitelmatasolla ja käytännön tasolla kyberuhkiin (N=20)

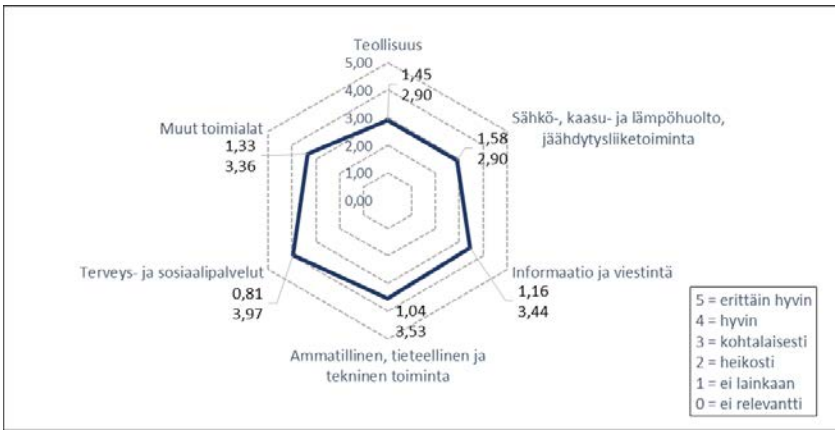
Vastauksissa aiempiin kysymyksiin on tullut selkeästi ilmi, että yritykset kokevat tietoon ja tietojärjestelmiin liittyvät riskit merkittäviksi yritysten liiketoiminnan kannalta. Tämän lisäksi yritykset ovat hyvin selkeästi tunnistaneet tarpeen informaatioteknologiaan liittyvien riskien hallinnalle. Yksi keino riskienhallintaan on vakuutuksen ottaminen kyberuhkien toteutumisen varalle. Yrityksiltä kysyttiin, onko niissä pohdittu kyberturvallisuuden liittyvien riskien pienentämistä vakuutusten avulla.

Kuvio 36 osoittaa, että kolme (3) yritystä oli pohtinut asiaa ”erittäin hyvin” ja kolme (3) yritystä ”hyvin”. Pohdintaa oli tehty ”kohtalaisesti” neljässä (4) yrityksessä ja ”heikosti” kolmessa (3) yrityksessä. Asia oli kokonaan miettimättä seitsemässä (7) yrityksessä kahdestakymmenestä vastaajasta. Tämä lienee osoitus myös siitä, että haastatteluhetkellä eivät suoraan kyberturvallisuusuhkiin keskittyneet vakuutustuotteet olleet monenkaan Suomessa toimivan vakuutusyhtiön tuotevalikoimissa ja niistä ei ollut yrityksillä riittävästi tietoa. Toisaalta vakuutukset liiketoiminnan keskeytymisen varalta ovat jo kauan olleet yrityksille suunnattuina vakuutustuotteina.



KUVIO 36. Pohdinnan taso kyberturvallisuusriskien pienentämisestä vakuutusten avulla (N=20)

Kuvion 37 avulla voidaan tarkastella, miten eri toimialojen yritykset vastasivat kysymyssarjan ”3. Prosessit” kysymyksiin. Suurimman numeraalisen vastauskeskiarvon 3,97 (keskihajonta 0,1) aikaansaavat edellisten kysymyssarjojen tavoin ”terveys- ja sosiaalipalvelujen” toimialaa edustavat yritykset. Pienimmän vastauskeskiarvon 2,90 saavuttavat sekä ”Sähkö-, kaasu- ja lämpöhuolto, jäähdytysliiketoiminta” –toimialan yritykset (keskihajonta 1,58) sekä ”teollisuus” –toimialan yritykset (keskihajonta 1,58). Kokonaisuutena ottaen toimialakohtaiset erot ovat samaa suuruusluokkaa kuin kysymyssarjassa ”2. Tieto ja sen merkitys liiketoiminnalle” ja kyberturvallisuuden huomioonottaminen yrityksen toimintaprosesseissa on tietoisuutta alhaisemmalla tasolla myös toimialakohtaisesti tarkasteltuna.



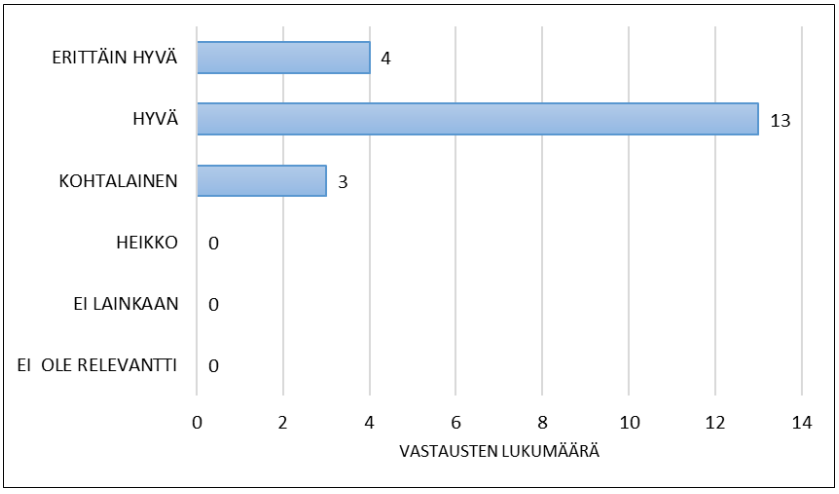
KUVIO 37. Kysymyssarjaan kolme annettujen vastausten toimialakohtaiset keskiarvot ja –hajonnat (N=300)

6.2.4 Tutkimuskysymys 4: Miten yritys on ottanut kyberturvallisuuden huomioon henkilöstön osaamisessa?

Kyberturvallisuuden yleinen ymmärrys, sekä tietoon ja tietojärjestelmiin liittyvien liiketoiminnan kriittisten tekijöiden tunnistaminen ja niiden suojaaminen kyberuhkia vastaan toimivilla prosesseilla ovat yrityksen kyberuhkien sietokyvyn peruspilareita. Niiden lisäksi tarvitaan yrityksen koko henkilöstöltä riittävä tietoisuus kyberuhkista sekä osaaminen niiden tunnistamiseen ja niitä vastaan suojautumiseen. Tutkimuksen neljäs kysymyssarja on työnimeltään ”4. Henkilöstön tietoisuus ja osaaminen” ja se koostuu kahdeksasta (8) kysymyksestä, joilla kartoitetaan sitä, miten yritys on ottanut kyberturvallisuuden huomioon henkilöstönsä osaamisessa.

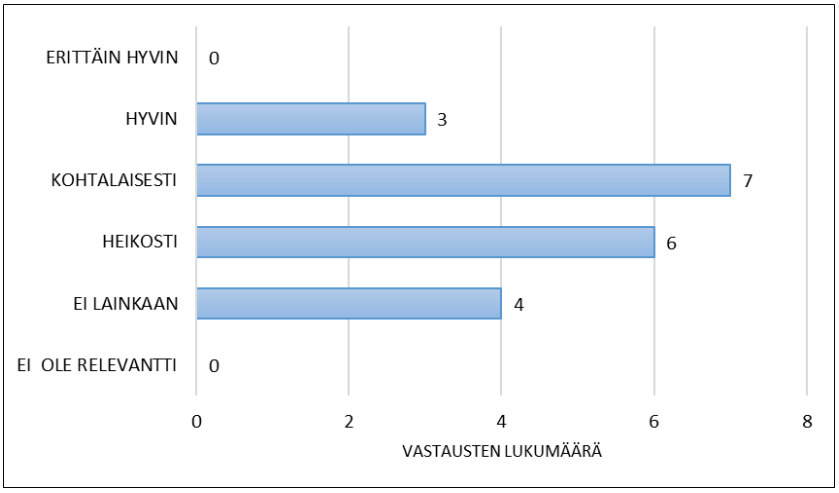
Kuten jo aikaisemmin on todettu, kyberturvallisuus on tekijä, jossa absoluuttista turvallisuutta on lähes mahdoton saavuttaa. Sen vuoksi on hyväksyttävä, että tietoon ja tietojärjestelmiin liittyvät riskit ovat aina olemassa ja niihin tulee varautua. Varautumisen tavat ja siihen käytettävät panokset on kunkin yrityksen itse määriteltävä ja suhteutettava liiketoimintaa uhkaaviin mahdollisiin kyberturvallisuusuhkiin.

Ensimmäisenä kysymyksenä selvitettiin yrityksen tietojärjestelmistä vastuullisen henkilön valmiuksia. Haastateltavilta kysyttiin, missä määrin yrityksen tietojärjestelmistä vastuullisella henkilöllä on riittävät valmiudet vastuullaan olevien riskien ymmärtämiseen ja hyväksyttävän riskitason määrittelyyn. Yrityksistä neljä (4) ilmoitti valmiuksien olevan ”erittäin hyvällä” tasolla. Kolmetoista (13) yritystä piti valmiuksia hyvinä ja kolmen (3) vastaajan mielestä valmiudet ovat ”kohtalaiset”. Kuviossa 38 näkyvä vastausten jakauma osoittaa tilanteen olevan kokonaisuudessaan hyvällä tasolla.



KUVIO 38. Tietojärjestelmistä vastuullisen henkilön valmiudet riskien ymmärtämiseen (N=20)

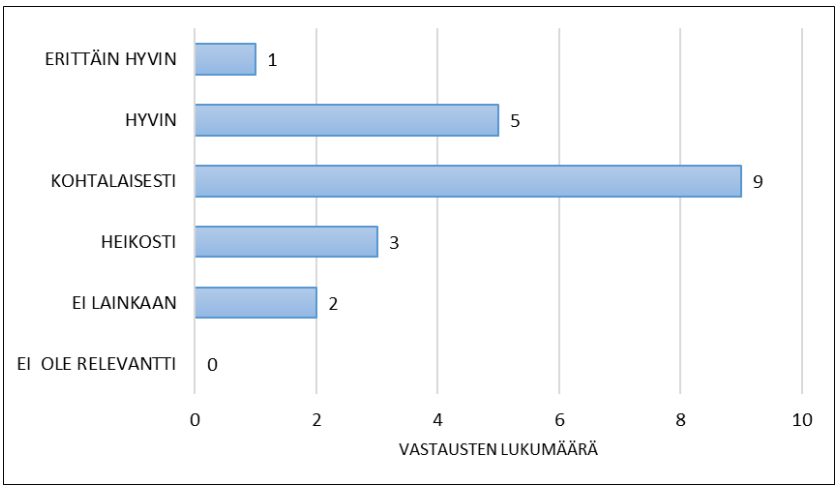
Laajennettaessa näkökulmaa vastuuhenkilön valmiuksista tarkastelemaan yrityksen koko henkilöstön valmiuksia, kysyttiin ”missä määrin yrityksessä on määritelty vaatimuksia sille, millainen kyvykkyys reagoida kyberturvallisuuspoikkeamaan tulee henkilöstöllä olla”. Yritysten antamien vastausten jakauma poikkeaa selkeästi edellisestä kysymyksestä. Vastaajista kolme (3) oli sitä mieltä, että kyvykkyysvaatimukset on määritelty ”hyvin”. Seitsemän (7) vastaajan mielestä yrityksessään on määritelty vaatimukset ”kohtalaisesti” ja kuuden (6) vastaajan mielestä ”heikosti”. Neljä (4) vastaajaa valitsi vaihtoehdon ”ei lainkaan”. Kuvio 39 näyttää havainnollisesti kokonaistilanteen, joka sijoittuu vaihtoehtojen ”heikosti” ja ”kohtalaisesti” välimaastoon. Tämä tarkoittaa sitä, että yrityksissä on tällä osa-alueella vielä tehtävää.



KUVIO 39. Henkilöstön kyvykkyysvaatimusten määrittelyn tilannekuva (N=20)

Jokaisella yrityksen henkilökunnasta tulee olla omalta osaltaan vastuu yritykseen liittyvästä turvallisuudesta. Vastuun kantamisen mahdollistava tekijä vastuiden määrittelyn lisäksi on myös se, että henkilöillä on riittävä osaaminen, jotta he pystyvät vastuunsa ottamaan. Tämä seikka koskee luonnollisesti kaikkia turvallisuuteen liittyviä vastuita, eikä rajoitu pelkästään kyberturvallisuuteen.

Haastateltavilta kysyttiin, ”ovatko yrityksen työntekijät saaneet riittävän koulutuksen, jotta he kykenevät kantamaan turvallisuuteen liittyvät vastuunsa”. Vastausten perusteella laadittu kuvio 40 osoittaa, että yksi (1) yritys on hoitanut koulutustehtävän mielestään ”erittäin hyvin” ja viisi (5) yritystä on hoitanut asia ”hyvin”. Lähes puolet yrityksistä eli tässä tapauksessa yhdeksän (9) yritystä on hoitanut asiaa ”kohtalaisesti”. kolme (3) yritystä ”heikosti” ja kaksi (2) yritystä ”ei lainkaan”.



KUVIO 40. Yritysten henkilöstön saama koulutus turvallisuuteen liittyvien vastuiden kantamiseksi (N=20)

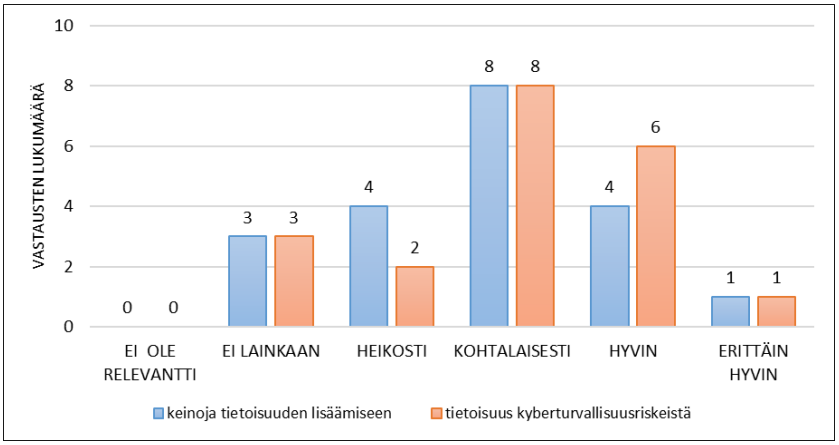
Yrityksessä työskentelee henkilöitä erilaisissa rooleissa ja työtehtävissä. Jokaisella henkilöllä tulisi olla työtehtäväänsä suhteutettuna riittävä tietoisuus ja ymmärrys kyberturvallisuudesta ilmiönä sekä niistä mahdollisista uhkista tai poikkeamista, jotka voivat vaikuttaa yrityksen toimintaan.

Henkilöstön perehdyttämiseen liittyviä seikkoja tarkasteltiin kysymysparilla, josta ensimmäisellä haluttiin selvittää, missä määrin yrityksillä on käytössään tapoja, menetelmiä tai materiaaleja, joilla työntekijät saatetaan tietoisiksi kyberturvallisuuteen liittyvistä riskeistä. Eli haluttiin selvittää, onko yrityksillä käytettävissä keinoja henkilöstön kyberturvallisuustietoisuuden lisäämiseen. Yksi (1) yritys vastasi keinoja olevan ”erittäin hyvin” käytössä ja neljällä (4) yrityksellä niitä oli ”hyvin” käytössä. Kahdeksan (8) yritystä vastasi keinoja olevan ”kohtalaisesti” ja neljän (4) yrityksen mielestä ”heikosti”. Kolmen (3) yrityksen mielestä heillä ei ollut lainkaan käytössä keinoja henkilöstön tietoisuuden lisäämiseen.

Sitä seikkaa, missä määrin yritysten työntekijöitä on perehdytetty kyberturvallisuusasioihin, kysyttiin väittämällä ”kaikki yrityksen työntekijät on saavutettu tietoisiksi mahdollisesta kyberturvallisuusriskeistä, jotka voivat vaikuttaa yrityksen liiketoimintaan”. Vastaukset jakautuivat lähes samaan tapaan kuin kysymysparin toisessa osassa, jossa kysyttiin perehdytyskeinojen olemassaoloa. Yksi (1) yritys vastasi perehdyttäneensä saa kaikki yrityksen työntekijät ”erittäin hyvin”. Kuuden (6) yrityksen mielestä asia oli ”hyvin” hoidettu ja kahdeksan (8) yrityksen mielestä ”kohtalaisesti” hoidettu. Näin ollen kolme neljäsosaa tutkimukseen osallistuneista yrityksistä ilmoitti

lisänneensä henkilöstönsä kyberturvallisuustietoisuutta vähintään kohtalaisesti. Kaksi (2) yrityksistä vastasi kysymykseen vaihtoehdolla ”heikosti” ja kolme (3) yritystä ei ollut lisännyt henkilöstön tietoisuutta lainkaan.

Kuvio 41 osoittaa yritysten vastausten jakaumaa henkilöstön kyberturvallisuustietoisuuden lisäämiseen liittyvässä kysymysparissa. Keinojen olemassaolo korreloi melko hyvin myös niiden käyttöasteeseen.



KUVIO 41. Keinojen olemassaolo ja niiden käyttäminen henkilöstön tietoisuuden lisäämiseksi (N=20)

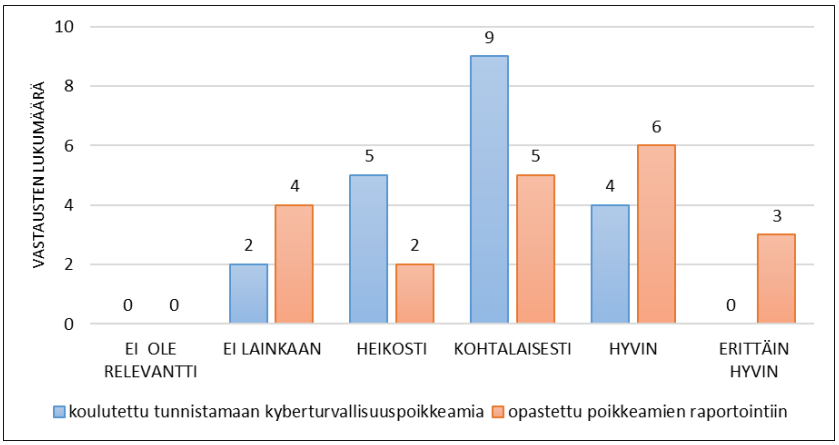
Pelkästään tietoisuuden lisääminen ei kuitenkaan riitä yritykselle kyberturvallisuusuhkien sietokyvyn varmistamiseksi. Yritysten henkilöstön tulee kyetä tunnistamaan poikkeamatilanteita sekä toimimaan niin, että mahdollista poikkeamista aiheutuva haitta rajoittuu minimiin ja yrityksessä kyetään mahdollisimman pian turvaamaan liiketoiminnan jatkuvuus sekä palauttamaan toiminta vähintään poikkeamaa edeltäneelle tasolle. Lisäksi yrityksessä tulee olla prosesseja tai mekanismeja, joiden avulla mahdollisista kyberturvallisuuspoikkeamista raportoidaan sekä yrityksen johdolle, mahdollisille tietojärjestelmiin liittyville palveluntuottajille, että tarvittaessa myös Viestintäviraston Kyberturvallisuuskeskukselle.

Näistä valmiuksista kysyttiin yrityksiltä kysymysparilla, joista ensimmäisessä haluttiin tietää, missä määrin ”yrityksen henkilöstöä on koulutettu tunnistamaan ja käsittelemään kyberturvallisuuspoikkeamia”. Yritysten vastaukset jakautuivat kuvion 46 mukaan. Neljässä (4) yrityksessä oli henkilöstö koulutettu kyberturvallisuuspoikkeamien tunnistamiseen ja käsittelemiseen ”hyvin”. Yhteensä yhdeksän (9) yritystä vastasi tähän koulutuksen tasoa käsittelevään kysymykseen vaihtoehdolla ”kohtalaisesti” ja

viisi (5) yritystä valitsi vaihtoehdon ”heikosti”. Yrityksistä kaksi (2) ei ollut toteuttanut koulutusta lainkaan.

Kysymysparin toisena osana yrityksille esitettiin kysymyksenä ovatko ”kaikki yritykset työntekijät opastettu raportoimaan mahdollista ja epäilyttävistä kyberturvallisuus poikkeamista”. Edelliseen kysymykseen verrattuna vastausten jakauma kuviossa 42 näyttää yritysten kyberturvallisuuden kannalta hieman paremmalta. Kolme (3) yritystä ilmoitti, että opastus on toteutettu ”erittäin hyvin”, kuusi (6) yritystä ilmoitti opastuksen toteutuneen ”hyvin” ja viisi (5) yritystä valitsi vaihtoehdon ”kohtalaisesti”. Kaksi (2) yritystä oli opastanut työntekijöitä raportoinnissa mielestään ”heikosti” ja peräti neljä (4) yritystä oli vastauksen ”ei lainkaan” kannalla.

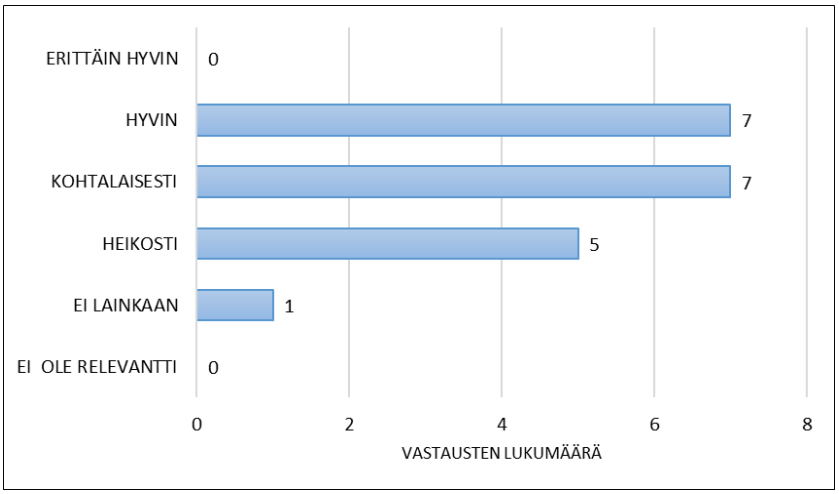
Yritysten tähän kysymyspariin antamien vastausten perusteella voidaan vetää selkeästi se johtopäätös, että yritysten henkilöstölle tarvittaisiin lisää perehdytystä kyberturvallisuuspoikkeamien tunnistamiseen ja niiden käsittelyyn.



KUVIO 42. Yritysten arvio henkilöstön saamasta koulutuksesta kyberturvallisuuspoikkeamien tunnistamiseen, käsittelyyn ja raportointiin (N=20)

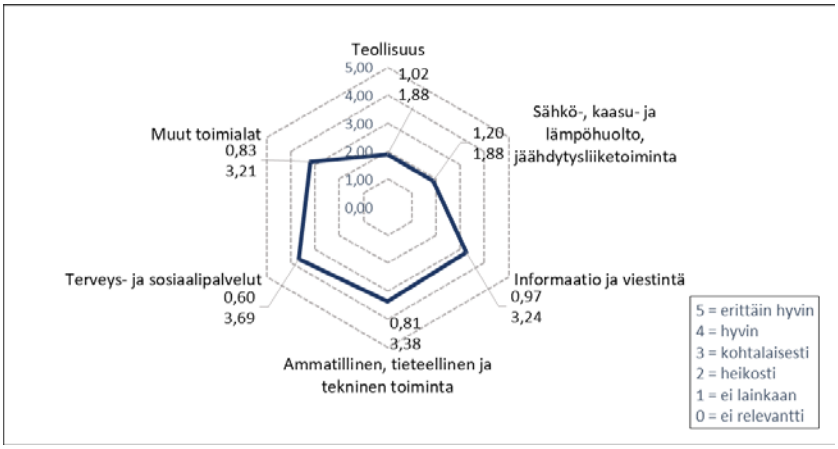
Jotta yritysten tietoisuutta kyberturvallisuudesta, siihen liittyvistä uhkista sekä yritysten mahdollisuudesta varautua uhkien toteutumiseen voisi lisätä, tulisi siihen liittyvää puolueetonta ja kansantajuista tietoa ja hyviä käytänteitä olla yritysten saatavissa. Luonnollisesti tähän teemaan keskittyneitä konsulttipalveluja on korvausta vastaan saatavissa, mutta erityisesti pienempien yritysten mahdollisuudet konsulttipalvelujen hankkimiseen ovat rajallisia.

Yrityksille käyttökelpoisen tiedon saatavuutta selvitettiin väittämällä ”kansantajuista tietoa yleisistä kyberturvallisuuteen liittyvistä ohjeista ja hyvistä käytänteistä on saatavilla yrityksen ulkopuolelta”. Seitsemän (7) yrityksen mielestä tietoa on saatavissa ”hyvin” ja samoin seitsemän (7) yritystä vastasi vaihtoehdolla ”kohtalaisesti”. Viiden (5) yrityksen mielestä tietoa on saatavissa ”heikosti” ja yhden (1) yrityksen mielestä ”ei lainkaan”. Kuvio 43 osoittaa, että tutkimukseen osallistuneiden yritysten mielestä niille käyttökelpoisen kyberturvallisuuteen liittyvän tiedon saatavuutta tulisi lisätä.



KUVIO 43. Kyberturvallisuuteen liittyvän tiedon ja hyvien käytänteiden saatavuus yrityksen ulkopuolelta (N=20)

Kysymyssarjaan ”4. Henkilöstön tietoisuus ja osaaminen” annettuja vastauksia toimialakohtaisesti kuvion 44 avulla havainnollistettuna toistuu aiemmin tarkastelluissa kysymyssarjoissa havaittu ilmiö. ”Terveys- ja sosiaalipalvelujen” toimialaa edustavien yritysten antamien vastausten numeraalinen keskiarvo 3,69 (keskihajonta 0,6) on toimialaryhmien suurin. Pienimmän vastauskeskiarvon 1,88 saavuttavat sekä ”Sähkö-, kaasu- ja lämpöhuolto, jäähdytysliiketoiminta” –toimialan yritykset (keskihajonta 1,88) sekä ”teollisuus” –toimialan yritykset (keskihajonta 1,88). Suurimman ja pienimmän keskiarvon erotukseksi muodostuu siten peräti 1,81. Luku on kysymysryhmien sisäisistä eroista suurin. Muut tutkimuksessa edustettuina olleet toimialat sijoittuvat keskenään lähes yhtäläisillä keskiarvoilla vastausvaihtoehdon ”kohtalaisesti” yläpuolelle.



KUVIO 44. Kysymyssarjaan neljä annettujen vastausten toimialakohtaiset keskiarvot ja –hajonnat (N=160)

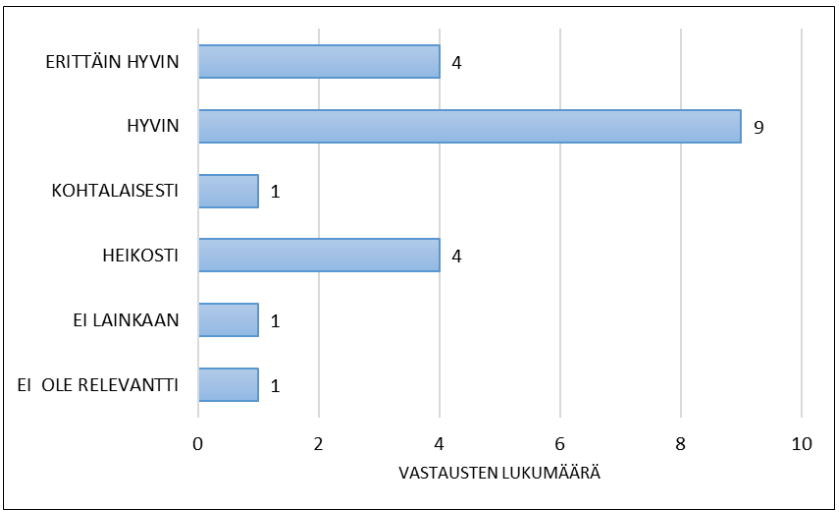
6.2.5 Tutkimuskysymys 5: Miten kyberturvallisuus on otettu huomioon yrityksen fyysisessä ympäristössä?

Kyberturvallisuus pitää sisällään tietoperustaisen omaisuuden, jota tallennetaan tai siirretään ICT:n avulla sekä tietoon perustumattoman omaisuuden, joka on haavoittuvainen ICT:n kautta tuleville uhkille. Näin ollen fyysinen turvallisuus on yksi huomioon otettavista kyberturvallisuuteen vaikuttavista tekijöistä.

Viides kysymyssarja tutkimuksessa on nimetty työnimellä ”5. Fyysinen turvallisuus” ja se koostuu seitsemästä (7) kysymyksestä, joiden avulla selvitetään yrityksiltä, miten ne ovat ottaneet huomioon fyysisen turvallisuuden toimitiloissaan ja niiden varustuksessa.

Fyysiseen turvallisuuteen pätee sama periaate kuin useimpiin muihinkin seikkoihin yritystoiminnassa; siitä tulee jonkun kantaa vastuu. Kysymyssarja aloitettiin väittämällä ”fyysinen turvallisuus on jonkun tietyn henkilön vastuulla kaikissa niissä tiloissa, joissa käytetään tai jonne on sijoitettu tietojärjestelmiä”.

Kuvion 45 esittämien vastausten perusteella vastuun määrittely fyysisestä turvallisuudesta on yrityksissä hyvällä tasolla, sillä neljä vastaajaa valitsi vaihtoehdon ”erittäin hyvin” ja yhdeksän (9) vastaaja valitsi vaihtoehdon ”hyvin”. Vastuuttaminen on toteutettu ”kohtalaisesti” yhdessä (1) yrityksessä, ”heikosti” neljässä (4) yrityksessä ja ”ei lainkaan” yhdessä (1) yrityksessä. Yhden vastaajan mielestä kysymys ei ollut heidän tapauksessaan relevantti.



KUVIO 45. Fyysisen turvallisuuden vastuuttaminen yrityksissä (N=20)

Tietojärjestelmien ja tiedon tallennusvälineiden säilyttämiseen liittyviä seikkoja kysyttiin neljällä (4) erillisellä kysymyksellä, joihin annetut vastaukset on koottu kuvioon 46. Ensimmäinen kysymys/väittämä toteaa, että ”yrityksen kannettavia tietokoneita, tabletteja ja muita kannettavia atk-laitteita säilytetään turvallisessa paikassa. Luonnollisesti vastaajalla oli mahdollisuus vastausta antaessaan mielessään määritellä, mitä sana ”turvallinen” hänen mielestään tarkoitti.

Kaksi (2) yritystä vastasi atk-laitteitaan säilytettävän ”erittäin hyvin” turvallisessa paikassa ja kymmenen (10) vastaajan mielestä säilytyspaikka oli ”hyvin” turvallinen. Viisi (5) vastaajaa oli sitä mieltä, että säilytyspaikka on ”kohtalaisesti” turvallinen, kahden (2) vastaajan mielestä säilytyspaikka oli vain ”heikosti” turvallinen ja yksi (1) vastaaja totesi, ettei säilytyspaikka ollut lainkaan turvallinen. Yhden vastaajan mielestä kysymys ei ollut relevantti.

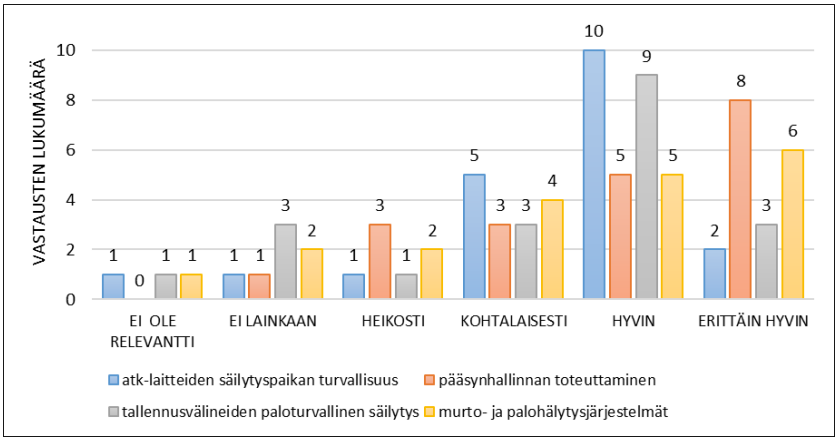
Fyysisiä pääsynhallintaratkaisuja on käytettävissä sekä perinteisen tyyppisiä mekaanisia lukitusjärjestelmiä, että sähköisiin avaimiin ja digitaalisiin lukkoihin perustuvia järjestelmiä. Olennaista on kuitenkin se, että kaikkien niiden lukituksen avaamiseen tarvitaan avain joka voi olla myös esimerkiksi näppäiltävä pääsykoodi.

Seuraavaksi yrityksille esitettiin väittämä ”avain tai jokin muu sisäänpääsyn oikeuttava väline tarvitaan kaikkiin niihin tiloihin, joissa tietokoneita, -järjestelmiä tai tallennusvälineitä säilytetään”. Kahdeksan (8) yritystä vastasi pääsynhallinnan olevan kunnossa ”erittäin hyvin” ja viisi (5) yritystä ilmoitti sen olevan ”hyvin” hoidettu. Kolmen

(3) yrityksen mielestä asia oli ”kohtalaisesti” hoidossa ja samoin kolmen (3) vastaajan mielestä ”heikosti” hoidettu. Yksi (1) yritys vastasi, että asia ei ole lainkaan hoidettu.

Tallennusvälineiden kapasiteetin kehityksen myötä on niiden koko pienentynyt merkittävin harppauksin. Lisäksi on tullut uusia mahdollisuuksia tiedon tallentamisen muun muassa matkapuhelimien kehityksen myötä. Keveitä liikuteltavia välineitä uhkaa paitsi murtautumisen vaara myös palovaara. Yrityksiltä kysyttiin, missä määrin ”yrityksen liiketoimintakriittistä tietoa sisältävät tallennusvälineet säilytetään tarkoitukseen soveltuvissa paloturvallisissa kaapeissa tai tiloissa”. Kysymykseen vastasi kolme (3) yritystä vaihtoehdolla ”erittäin hyvin” ja yhdeksän (9) yritystä valitsi vaihtoehdon ”hyvin”. Kolmessa (3) yrityksessä paloturvallisuus toteutuu ”kohtalaisesti”, yhdessä (1) yrityksessä ”heikosti” ja kolmessa (3) yrityksessä asiaan ei kiinnitetä lainkaan huomiota. Yhden vastaajan mielestä kysymys ei ollut relevantti.

Neljäntenä toimitilojen turvallisuuteen liittyvänä kysymyksenä yrityksiltä kysyttiin missä määrin ”ne tilat, joissa tietokoneita, -järjestelmiä tai tallennusvälineitä säilytetään ovat varustettu ajanmukaisin murto- ja palohälytyslaittein”. Hälytysjärjestelmät olivat vastaajien mielestä kunnossa kuudessa (6) yrityksessä ”erittäin hyvin”, viidessä (5) yrityksessä ”hyvin” ja neljässä (4) yrityksessä ”kohtalaisesti”. Kahden (2) yrityksen valitsema vaihtoehto oli ”heikosti” ja kahdella (2) yrityksellä ei hälytysjärjestelmiä ollut käytössään lainkaan. Yhden vastaajan mielestä kysymys ei ollut heille relevantti.

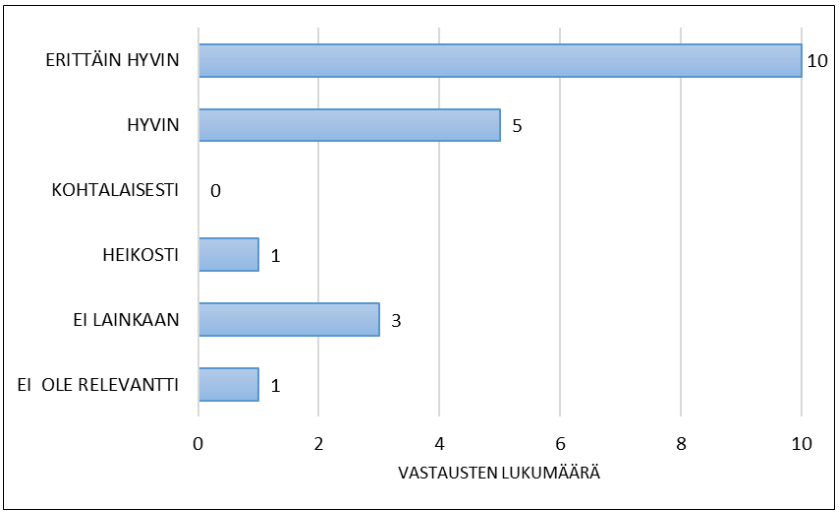


KUVIO 46. Yritysten fyysisen ympäristön kybervarautumisen tilannekuva eri osa-alueilla (N=20)

Luonnonilmiöiden aiheuttamat sähkökatkot voivat aiheuttaa pitkiäkin keskeytyksiä yritysten toiminnalle. Myös ihmisen aiheuttamat tahalliset tai tahattomat sähkökat-

kot aiot samalla tavoin aiheuttaa poikkeustilanteita yritysten toimintaan. Sähkövirrasta riippuvaisten tietojärjestelmien energiansaanti tulisi varmistaa riittävässä määrin myös poikkeustilanteissa, jotta järjestelmissä oleva tieto saadaan varmistettua niin, että se ei häviä pidemmänkään sähkökatkon aikana.

Tähän liittyen yrityksiltä kysyttiin, missä määrin ”yrityksen tietojärjestelmät ovat varustettu katkeamattomalla virransyötöllä tai varavoimalaitteella sähkökatkojen varalta”. Kymmenellä (10) yrityksellä sähköenergian saanti tietojärjestelmille oli ”erittäin hyvin” turvattu myös sähkökatkojen aikana. Viisi (5) yritystä ilmoitti asian olevan ”hyvin” järjestetty ja yksi (1) yritys totesi asian olevan ”heikosti” hoidettu. Kolmella (3) yrityksellä ei varavoimajärjestelyjä oltu tehty lainkaan ja yhden (1) vastaajan mielestä kysymys ei ollut heidän yritykselleen relevantti. Alla oleva kuvio 47 osoittaa, että jopa kolme neljäsosaa yrityksistä on varautunut sähkökatkoihin vähintäänkin ”hyvin”.

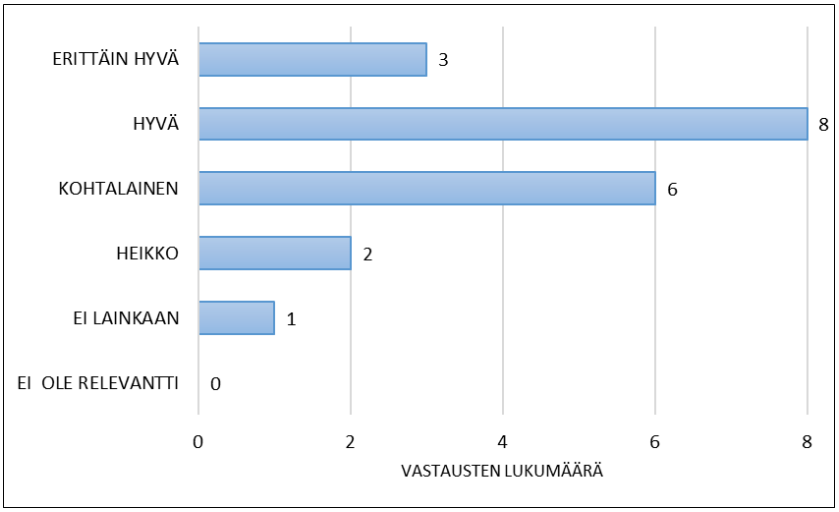


KUVIO 47. Yritysten varustautuminen varavoimalaittein sähkökatkojen varalta (N=20)

Henkilötietoihin liittyvä tietosuoja on noussut vahvasti esille johtuen erityisesti EU:n yleisestä tietosuoja-asetuksesta, jonka siirtymäaika päättyi 25.toukokuuta 2018. Se velvoittaa kaikkia rekisterinpitäjiä suojaamaan hallussaan olevia henkilötietoja.

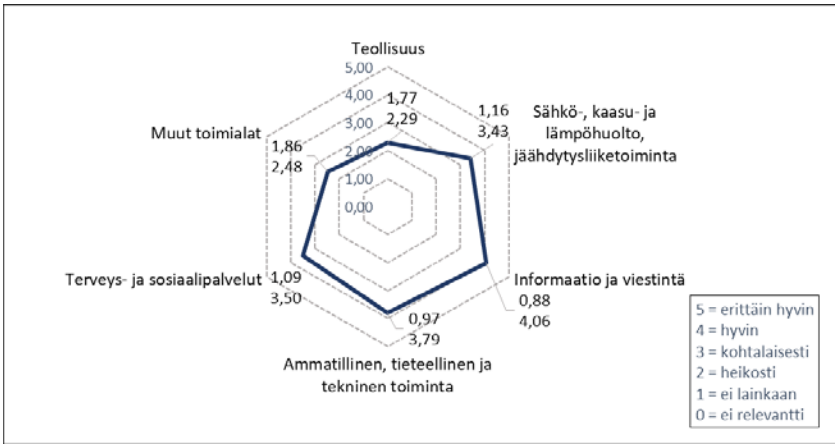
Tämä näkyy käytännön toimenpiteinä myös yritysten arjessa. Erityisesti asiakaspalveluun käytettävissä tiloissa voi esiintyä tilanteita, joissa yrityksen ulkopuolinen henkilö pääsee kosketuksiin yrityksen hallussa olevan arkaluontoisen tiedon tai henkilötiedon kanssa. Tätä mahdollisuutta kartoittava yrityksille esitetty väittämä kuului: ”il-

man asianmukaisia käyttöoikeuksia olevien henkilöiden pääsy työasemien näyttöpäätteille on estetty”. Kuviosta 48 näkyy vastausten jakauma, jonka mukaan näyttöpäätteet on suojattu ulkopuolisilta kolmessa (3) yrityksessä ”erittäin hyvin”, kahdeksassa (8) yrityksessä ”hyvin” ja kuudessa (6) yrityksessä ”kohtalaisesti”. Tilanne oli kahden (2) vastaaja mielestä ”heikko” ja yhdessä (1) yrityksessä suojausta ei oltu tehty lainkaan.



KUVIO 48. Näyttöpäätteiden suojaus ilman käyttöoikeuksia olevilta henkilöiltä (N=20)

Vertailtaessa kysymyssarjaan ”5. Fyysinen turvallisuus” annettuja vastauksia haastattelussa edustettuina olleiden toimialojen kesken, voidaan todeta, että toimialojen keskinäiset suhteet poikkeavat aikaisemmista neljästä kysymyssarjasta. Kuten kuvio 49 osoittaa, toimialoista korkeimman vastauskeskiarvon 4,06 (keskihajonta 0,88) saa tässä kysymyssarjassa ”informaatio ja viestintä” -toimialaa edustavat yritykset. Seuraavaksi korkein vastaus keskiarvo 3,79 (0,97) on ”ammatillinen tieteellinen ja tekninen toiminta” -toimialaa edustavilla yrityksillä. Muissa kysymysryhmissä korkeimmat vastauskeskiarvot saavuttaneet ”terveys ja sosiaalipalvelut” –toimialan yritykset saavat kolmanneksi suurimmaksi vastauskeskiarvoksi 3,50 (1,09). Alhaisimman vastausten keskiarvon 2,29 (1,77) saavuttivat tässä kysymysryhmässä ”teollisuus” –toimialaa edustavat yritykset.



KUVIO 49. Kysymyssarjaan viisi annettujen vastausten toimialakohtaiset keskiarvot ja –hajonnat (N=140)

6.3 VAPAAMUOTOISET KOMMENTIT

Haastatelluilla oli mahdollisuus jokaisen kysymyssarjan läpikäynnin jälkeen antaa siihen liittyviä vapaamotoisia kommentteja. Niitä ei kuitenkaan tuotu esille minkään yksittäisen kysymyssarjan yhteydessä. Vastaava mahdollisuus ”vapaaseen sanaan” tarjottiin siinä, vaiheessa kun kaikki strukturoidut kysymykset oli käyty läpi.

Vapaamuotoisia kommentteja annettiin yhteensä 23 kappaletta. Niistä seitsemän (7) kohdistui tutkimukset sisältöön, rakenteeseen tai toteutustapaan seuraavasti:

- *”Kysymykset ovat relevantteja teeman kannalta.”*
- *”Fyysiseen turvallisuuteen liittyvät tekijät nousevat hyvin esille.”*
- *”Asteikon olisi hyvä vaihdella.”*
- *”Sähköinen kysely voisi olla parempi, jolloin voisi verrata kysymyksiä toisiinsa ja tarkastella miten on aikaisemmin vastannut.”*
- *”Kysymyksissä oli sekä laajoja että yksityiskohtaisia kysymyksiä.”*
- *”Kysymykset ja niiden rajaus suhteessa oman organisaation ympäristöihin ovat vaikeita, kun huomioidaan kysymysten yleinen (geneerinen) taso. Kysymykset sinällään ovat hyviä.”*
- *”Yleisellä tasolla kysely on hyvä ja toi esille, että on paljon tekemistä.”*

Saadut kommentit olivat hyödyllisiä ja ne tukivat omaa pohdintaani tutkimuksen toteuttamisesta ja mahdollisista parannuskohteista.

Yleisesti tutkimuksen aihepiiriin tai vastaajayrityksen omaan tilanteeseen kyberturvallisuusuhkiin varautumisen suhteen annettiin yhteensä 16 vapaamuotoista kommenttia seuraavasti:

- *”Asiakastuotteiden kyberturvallisuus on joko omalla tai palveluntuottajan vastuulla ja se on vähintäänkin kohtuullisella tasolla.”*
- *”Tuotekehitykseen ja muuhun toimintaan liittyen on vielä kehitettävää ja sillä osa-alueella on asiakkaiden aiheuttamat riskit ovat myös merkittävä tekijä kyberturvallisuuden kannalta.”*
- *”Haittaohjelmien leviäminen on hallitsematon riski monessa yrityksessä.”*
- *”Kyberturvallisuus-termin määrittely on haasteellista.”*
- *”Digitalisaatio on edennyt ja palveluja on mahdollista siirtää pilveen.”*
- *”Internet-sivustolla on kävijöitä eri maista.”*
- *”Osallistuimme KESKI-15 harjoitukseen.”*
- *”Riskitason määrittäminen on kunkin yrityksen sisäinen asia.”*
- *”Sähköpostin turvallisuuteen luotetaan yrityksissä aivan liikaa.”*
- *”Puhuttaessa liiketoimintakriittisen tiedon säilyttämisestä on huomattava, että tietoa tallennetaan myös pilveen. Näin ollen yksiselitteisen vastauksen antaminen on hankalaa. On huomattava, että suurin riski tiedon käsittelyssä on asiakkaan tiedon menettäminen.”*
- *”Dokumentaatiota täytyy lisätä.”*
- *”Tiedostan, että on paljon tehty asioita, mutta koskaan ei tulla valmiiksi. Esimerkiksi henkilöstön koulutuksen osalta olemme toimialalla kohdassa 5.”*
- *”Asia on paljon laajempi kuin voisi ajatella.”*
- *”Tietoturvallisuus- ja kyberturvallisuuskyvykkyyksiä kehitettäessä on törmätty ongelmaan, ettei tahdo löytyä sellaisia kumppaneita, jotka auttavat ymmärtämisessä ja tuottamisessa (erityisesti liittyen mobiliteettisovelluksiin).”*
- *”Luulen että vastauksemme eroavat useimpien yritysten vastauksista, koska meillä yrityksen tieto on tärkein yrityksen omaisuus. Yrityksen metadatan arvo säilyy ja tulevaisuudessa siitä todennäköisesti osataan analysoida uusia ulottuvuuksia ja tarkempaa uutta tietoa. Meillä on minimaalinen dokumentaatio, jonka koemme olevan yritykselle sekä heikkous että vahvuus. Tavoittelemme yrityksessä*

ketteryyttä ja liian raskas ylläpidettävä dokumentaatio ei näin ollen puolla paikkaansa. Kyseessä on siis tiedostettu, valittu toimintatapa."

- *"Kyberturvallisuus on laaja-alainen asia ja se vaatii huomattavan paljon työtä. Ei pidä tuudittautua siihen, että jotkut järjestelmät toimivat."*

Haastateltavien antamat vapaamuotoiset kommentit ovat samansuuntaisia strukturoituihin kysymyksiin annettujen vastausten kanssa ja kuvaavat hyvin kohdejoukon nykytilaa ja ajatuksia kyberturvallisuuden suhteen. Niistä ilmenee, että haastattelu nosti esille kyberturvallisuusilmiön laajuutta ja kompleksisuutta. Lisäksi niistä näkyy, että joissakin yrityksissä havaittiin uusia kehittämiskohteita kyberturvallisuuden lisäämiseksi. Tämä oli havaittavissa myös aistinvaraisesti "ahaa-ilmiöinä" haastattelutilanteissa.

6.4 TULOSTEN VERTAILU SAMAN AIHEPIIRIN TUTKIMUKSIIN

Yritysten tietoturvaan liittyen on tehty useita tutkimuksia sekä Suomessa että ulkomailla. Halusin verrata tässä haastattelututkimuksessa saatuja tuloksia relevantteihin samaa aihepiiriä käsitteleviin tutkimuksiin ja erityisesti sellaisiin, joissa kohderyhmänä on ollut pieniä ja keskisuuria yrityksiä.

Tarkoituksena oli löytää verrokkitutkimuksiksi alueellinen tutkimus, kansallinen tutkimus sekä kansainvälinen tutkimus. Koska tarkoituksena ei ollut mitata aikaan sidottuja kehitystrendejä, oli tavoitteena löytää mahdollisimman lähelle oman tutkimustyön ajankohtaan sopivia tutkimuksia, koska tutkittavat ilmiöt sinänsä voivat olla luonteeltaan nopeasti muuttuvia, vaikka kohderyhmän muutos olisikin hitaampaa. Poimin kustakin verrokkitutkimuksesta sellaisia kysymyksiä, jotka sisällöllisesti sopivat verrattaviksi tekemäni tutkimuksen kysymysten kanssa.

6.4.1 Alueellinen verrokkitutkimus

Alueelliseksi verrokiksi valikoitui Jarmo Nevalan ja Jouni Ahon tekemä ja vuonna 2016 julkaistu tutkimus nimeltään "Keskisuomalaisten yritysten kyberturvallisuus". Kyselytutkimus oli toteutettu Jyväskylän koulutuskuntayhtymän hallinnoimassa "Toisen asteen kyber" –nimisessä hankkeessa. Teen seuraavassa tutkimusten vertailua niiltä osin, joissa tutkimuksissa esitettyjen kysymysten sisältö tai kysymyksenasettelu on lähes kokonaan tai osittain samankaltainen. (Nevala & Aho 2016, 6.)

Saateviesti ja linkki Digium Enterprise kyselyohjelmistolla toteutettuun kyselyyn oli lähetetty sähköpostitse 2276 keskisuomalaiselle yritykselle ja siihen vastasi yhteensä 201 yritystä. Vastaajista oli 74 % alle 10 henkilöä työllistäviä yrityksiä ja yli 10 henkilön yrityksiä oli 26 %. (Nevala & Aho 2016, 9.)

Lähes kolmannes vastaajista sijoittui palvelualoille, teollisuuden toimialalle sekä kaupan toimialalle sijoittui molemmille 15 % vastaajista, teknologia -toimialalle 10 % ja rakentamisen toimialalle 9 %. Loppuosa yrityksistä eli noin 20 % sijoittui ryhmään muut toimialat. Koska kyselyn analyysissä ei ole käytetty Tilastokeskuksen toimialaluokitusta (TOL) ei toimialakohtaisia vastauksia voi suoraan verrata omaan tutkimukseeni. (Nevala & Aho 2016, 14.)

Vastaajien taustatietojen lisäksi tutkimuksen kohteina olivat 1) tietoturvan huomioiminen, 2) asenteet, 3) toteutuneet uhat ja 4) yrityksen koulutusnäkökulma. (Nevala & Aho 2016, 16.)

Tietoturvan huomioimisen osa-alueilla kysymykset koskivat muun muassa tietoisuutta EU lainsäädännöstä, internetiin kytkeytyviä laitteita ja omien laitteiden käyttöä työasioiden hoitamiseen. Oman tutkimukseni kanssa lähinnä samankaltainen kysymys koski henkilöstön perehdyttämistä tunnistamaan liiketoiminnan kannalta luottamukselliset tiedot. Vastausvaihtoehdot olivat kyllä / ei / en tiedä. Vastaajista 73,6 % prosenttia vastasi ”kyllä”, vastauksen ”ei” antoi 20,4 % ja 6 % vastasi ”en tiedä”. (Nevala & Aho 2016, 15.)

Saman tyyppinen kysymys omassa tutkimuksessani oli kysymysryhmään ”4. Henkilöstön tietoisuus ja osaaminen” sisältynyt väittämä ”kaikki yrityksen työntekijät on saatettu tietoisiksi mahdollisista kyberturvallisuusriskeistä, jotka voivat vaikuttaa yrityksen liiketoimintaan”. Kysymykseen vastasi kahdeksan (8) yritystä vaihtoehdolla ”kohtalaisesti”, kuusi (6) yritystä ”hyvin” ja yksi (1) yritys ”erittäin hyvin”. Nämä vastaukset muodostavat yhteensä 75 % kaikista vastauksista, joka on samaa suuruusluokkaa kuin Nevalan & Ahon verrokkitutkimuksessa. Tutkimuksissa käytettyjen vastausasteikkojen erilaisuudesta johtuen ei vastauksia voi tietenkään aivan suoraan verrata keskenään.

Seuraava konkreettisesti vertailukelpoinen asia liittyy häiriötilanteisiin varautumiseen. Nevalan & Ahon tutkimuksen mukaan 67 prosenttia vastanneista yrityksistä on

varautunut sähkökatkoihin. Omassa tutkimuksessani 75 prosentilla vastanneista yrityksistä on tietojärjestelmät varustettu katkeamattomana virransyötöllä tai varavoimalaitteella sähkökatkojen varalta. (Nevala & Aho 2016, 20.)

Kyberuhkiin liittyvän tiedon riittämättömyyden kokee lähes 60 % vastanneista verrokkitutkimuksessa vähintään “melko suureksi” esteeksi tehokkaan kyberturvallisuuden toteuttamiseksi yrityksessä (Nevala & Aho 2016, 23). Omassa tutkimuksessani 14 vastaajaa kahdestakymmenestä eli 60 % oli sitä mieltä, että kansantajuista tietoa yleisistä kyberturvallisuuteen liittyvistä ohjeista ja hyvistä käytänteistä on saatavilla yrityksen ulkopuolelta. Vastauksia voidaan pitää lähes saman sisältöisinä.

Kysyttäessä tärkeimpiä yrityksen kyberturvallisuuden kehittämiskohteita, verrokkitutkimuksessa 71 % vastaajista piti yrityksen omistajan/yrittäjän tietoturvaosaamisen kehittämistä tärkeimpänä kehittämiskohteena. Lisäksi henkilökunnan osaamisen kehittämistä painotti noin 46 % vastaajista. (Nevala & Aho 2016, 25.)

Omassa tutkimuksessani ei suoraan kysytty kehittämistarpeita. Sen sijaan useampaan kysymykseen sisältyi arvio tämänhetkisestä tietoisuudesta tai osaamisesta, mikä oli vastaajien mielestä keskimäärin ”kohtalaisella” tasolla, Tästä voidaan vetää se johtopäätös, että yrityksissä olisi molempien tutkimusten mukaan olemassa tarve kyberturvallisuusosaamisen kehittämiseen.

6.4.2 Kansalliset verrokkitutkimukset

Kansallisia verrokkitutkimuksia ei luonnollisestikaan löytynyt saman sisältöisenä kuin tässä työssä tehty tutkimus oli. Olennaista kuitenkin oli löytää tutkimusajankohdaltaan yhtäläinen pk-yrityksiin (erityisesti pienyritykset) suuntautunut tutkimus, jonka osana on selvitetty myös yritysten varautumista kyberuhkiin. Valitsin verrokeiksi kaksi tutkimusta, joista molemmista poimin kolme omaan tutkimukseeni asiasisällöllisesti verrattavissa olevaa teemaa.

Ensimmäisenä verrokkina tarkastelen ”Yrityksiin kohdistuvat kyberuhat 2016” -tutkimusta, joka on tehty lokakuussa 2016 osana DigiCyber -hanketta. Siinä Taloustutkimus toteutti Helsingin seudun kauppakamarin toimeksiannosta kyselyn, johon vastasi 754 suomalaista yritystä. Pk-yritysten kokoluokkaan kuului vastanneista yrityksistä lähes 90%. Kyselyyn vastanneista henkilöistä 83 % toimi yrityksen päätöksentekijänä. (Yrityksiin kohdistuvat kyberuhat 2016, 5.)

Kyberuhkiin varautumiseen liittyen yritykseltä kysyttiin *”Mitkä ovat kolme suurinta estettä tehokkaan kyberturvallisuuden toteuttamisessa?*” Alle 50 henkilöä työllistävistä vastaajayrityksistä (N=563) 39 % oli sitä mieltä, että suurin este on käyttäjien piittaamattomuus tietoturvallisuudesta ja kyberuhkista. Reilu kolmasosa (35 %) vastaajista oli sitä mieltä, että yritysten riittämätön tieto kyberuhkista on merkittävä este kyberturvallisuudelle. Kolmanneksi merkittävämpänä (30 %) seikkana yritykset pitivät vaikeutta ylläpitää kyberturvallisuuteen liittyvää henkilökunnan tietotaitoa. (Yrityksiin kohdistuvat kyberuhat 2016, 13.)

Vastaukset tukevat oman tutkimukseni kysymyssarjaan ”4. Henkilöstön tietoisuus ja osaaminen” annettuja vastauksia. Molemmat tutkimukset osoittavat, että yritysten henkilöstön kyberturvallisuusosaaminen ei ole riittävällä tasolla, jotta se tukisi yritysten sietokykyä kyberuhkia vastaan. Tämän vuoksi olisi osaamisen kehittämiseen kyettävä panostamaan.

Helsingin seudun kauppakamarin teettämässä tutkimuksessa kysyttiin myös, että ”Tietääkö henkilökuntanne miten toimia, jos he epäilevät tunkeutumista tietojärjestelmiinne?” Tutkimukseen vastanneista alle 50 henkilöä työllistävistä yrityksistä (N=563) vastasi ”kyllä” 54 % vastaajista ja ”ei” hieman yli 22 prosenttia vastaajista. Jopa 23 % ei osannut sanoa, mikä olisi tilanne yrityksessä tunkeutumisepäilyn tultua ilmi. (Yrityksiin kohdistuvat kyberuhat 2016, 31.)

Vastausasteikkojen erilaisuuden vuoksi ei suoraa vertailua tutkimusten välillä voi tehdä. Omassa tutkimuksessani 65 % yrityksistä (N=20) ilmoitti, että henkilöstö on koulutettu vähintään ”kohtalaisesti” tunnistamaan kyberturvallisuuspoikkeamia ja 70 % ilmoitti, että henkilöstö on opastettu vähintään ”kohtalaisesti” poikkeamien raportointiin. Vastauksen ”ei lainkaan” tunnistamista koskevaan kysymykseen antoi 10 % vastaajista ja raportointia koskevaan kysymykseen 20 % vastaajista. Tutkimusten tulokset tukevat toisiaan ja niiden perusteellä näyttää siltä, että joka viidennessä yrityksessä on pahoissa aikeissa olevan tunkeutujan mahdollista toimia ilman, että tunkeutuminen tulee esille.

Molemmissa tutkimuksissa tarkasteltiin myös digitaalisen jatkuvuuden hallintaan liittyvien suunnitelmien olemassaoloa. Taloustutkimuksen esittämä kysymys kuului: ”Onko teillä käytössä käytännössä toimivia suunnitelmia tunkeutumisen varalle?” Alle 50 henkilöä työllistävistä yrityksistä (N=563) peräti 62% vastasi kysymykseen

kielteisesti ja neljäsosa vastaajista (25 %) ilmoitti suunnitelmien olevan olemassa. Loppuosa vastaajista (13 %) ei osannut sanoa asian tilaa. (Yrityksiin kohdistuvat kyberuhat 2016, 59.)

Omassa tutkimuksessani yrityksille (N=20) kysymyssarjassa ”2. Tieto ja sen merkitys liiketoiminnalle” esitetty väittämä kuului: ” Yrityksessä on dokumentoitu kyberturvallisuusuhkien varalta palautumissuunnitelma, jolla pyritään varmistamaan digitaalinen jatkuvuus.” Väittämään vastasi 35 % yritystä vaihtoehdolla ”ei lainkaan” ja niin ikään 35 % valitsi vaihtoehdon ”heikosti”. Kysymykseeni vastasi 10 % yritystä vaihtoehdolla ”kohtalaisesti” ja vaihtoehdon ”hyvin” valitsi 20 % vastaajista. Erilaiset vastausasteikot eivät mahdollista suoraa vertailua, mutta omassa tutkimuksessani ”kohtalaisesti” ja ”hyvin” vastanneet muodostavat 30 % kaikista vastaajista, mikä kuvaa samansuuntaista tilannetta kuin Helsingin seudun Kauppakamarin teettämässä kyselyssä.

Toisena kansallisena tutkimuksena tarkastelen teleoperaattori Elisa Oyj:n sekä Suomen Yrittäjät ry:n vuonna 2016 teettämää tutkimusta suomalaisten pk-yritysten digitalisaation asteesta, johon vastasi yhteensä 730 yrittäjää. Yrityksistä vain 17 kpl oli yli 50 henkilöä työllistäviä yrityksiä, joten tutkimuksen kohderyhmä soveltuu yritysten kokoluokan perusteella erinomaisesti verrokkitutkimukseksi. Tutkimuksen suomalaisten pk-yritysten digitalisaation asteesta toteutti käytännössä Prior Konsultointi Oy. Yhtenä osana tutkimusta tarkasteltiin tietoturvaa ja henkilötietojen käsittelyä yrityksissä. Kyse ei siis ollut varsinaisesti kyberturvallisuuteen liittyvästä tutkimuksesta. (Aitoa digitaalisuutta vai työsuhdekännyköitä? Tutkimus suomalaisten Pk-yritysten digitalisaation asteesta 2016, 4.)

Yrityksen varautumiseen tietoturvauhkia vastaan liittyen esitettiin Elisan teettämässä tutkimuksessa (N=730) vastaajille väittämä ”Meillä on tunnistettu mitkä ovat yrityksen elintärkeitä toimintoja ja mitkä ovat niihin liittyvät tietoturvariskit.” Vastaajista 54% vastasi kysymykseen vaihtoehdolla ”järjestelmällisesti”, 34% vastasi vaihtoehdolla ”satunnaisesti” ja 15% suunnitteli tekevänsä tunnistamista. Jäljelle jääneistä 6% oli sitä mieltä, että asia ei koske heitä ja 1% vastaajista ilmoitti, että tunnistamista ei ollut tehty ollenkaan. (Aitoa digitaalisuutta vai työsuhdekännyköitä? Tutkimus suomalaisten Pk-yritysten digitalisaation asteesta 2016, 18.)

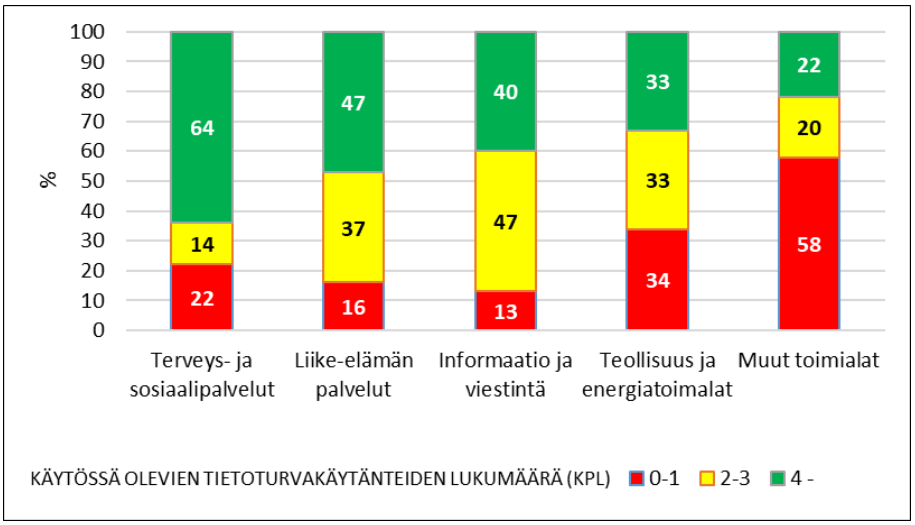
Omassa tutkimuksessani (N=20) vastaavaa aihetta käsiteltiin väittämässä ”Tietoon ja sen käsittelyyn liittyvät riskit ovat merkittäviä yrityksen liiketoiminnan kannalta.” Väittämän taustaoletuksena on se, että vastaajalla on riskit siinä määrin tiedossa ja hän vastatessaan pystyy arvioimaan niiden merkittävyyttä liiketoiminnan kannalta. Yrityksistä 55 % vastasi riskien olevan ”erittäin hyvin” merkittäviä ja 30 % vastasi ”hyvin” merkittäviä. ”Kohtalaisesti” –vastauksia oli 5 % ja ”heikosti” vastasi 10% yrityksistä. Vastausvaihtoehtojen erilaisuudesta huolimatta nähdään molemmista tutkimuksista, että yli 80 % yrityksistä oli tunnistanut tietoturvaan liittyviä riskejä ja niiden merkittävyyttä liiketoiminnalle ja yli puolet kaikista vastanneista oli tehnyt sitä muita perusteellisemmin.

Yrityksen tietoturvakäytänteisiin liittyvänä kysymyksenä esitettiin verrokkitutkimuksessa väittämä ”Salasanat päivitetään säännöllisesti”. Siihen vastasi vaihtoehdolla ”järjestelmällisesti” yhteensä 29% yrityksistä. Noin puolet (51%) valitsi vaihtoehdon ”satunnaisesti” ja 13% ilmoitti asian olevan suunnitteluasteella. Vastaajista 2 % ilmoitti vastauksekseen vaihtoehdon ”ei ollenkaan” ja kolme prosenttia oli sitä mieltä, että asia ”ei koske yritystäni”. (Aitoa digitaalisuutta vai työsuhdekännyköitä? Tutkimus suomalaisten Pk-yritysten digitalisaation asteesta 2016, 18.)

Omassa tutkimuksessani vastaavaa asiaa lähestyttiin kysymyssarjan ”3. Prosessit” väittämällä Liiketoimintakriittiseen tieto-omaisuuteen pääsyä seurataan ja pääsyyn oikeuttavat tunnukset tietojärjestelmissä vaihdetaan säännöllisesti. Vastaajista 30% valitsi vaihtoehdon ”erittäin hyvin” samoin 30% vastasi vaihtoehdolla ”hyvin”. Vaihtoehdon ”kohtalaisesti” valitsi 25% yrityksestä vaihtoehdon ”heikosti” 10% yrityksestä ja ”ei lainkaan” 5% yrityksestä.

Mikäli tutkimusten vastausvaihtoehdoista ”järjestelmällisesti” ja erittäin hyvin” arvotetaan toisiaan vastaaviksi vaihtoehdoiksi, on kyseiset vaihtoehdot valinneiden yritysten suhteellinen osuus lähes yhtä suuri. Vastaavanlainen vertailutulos saadaan, mikäli oman tutkimukseni vaihtoehdot ”hyvin” ja ”kohtalaisesti” arvioidaan olevan verrattavissa verrokkitutkimuksen vaihtoehtoon ”satunnaisesti”. Hieman yli puolet vastaajista valitsi tutkimuksissa nämä vaihtoehdot. Tässäkin tapauksessa vastausasteikkojen erilaisuus vaikeuttaa vertailua.

Kolmantena verrokkitutkimuksen vertailukohteena on tietoturvakäytäntöjen olemassaolo ja niiden lukumäärä eri toimialoilla. Tarkastelen tuloksia kuvion 50 avulla vastaavien toimialojen näkykulmasta kuin omassa tutkimuksessani oli edustettuina.

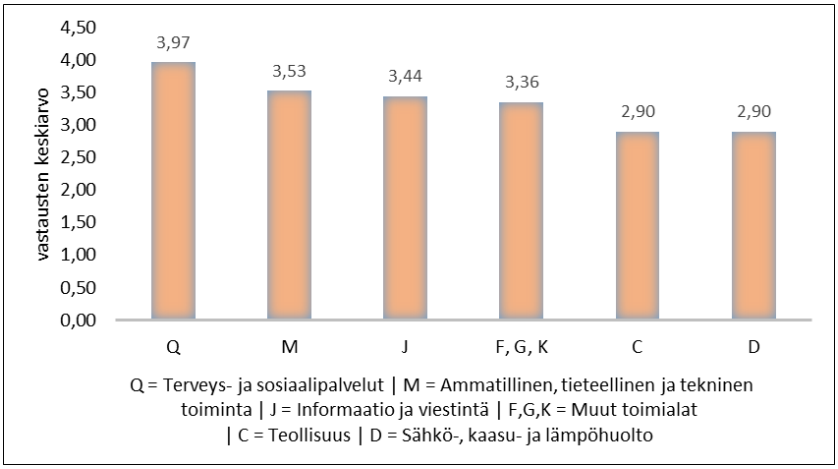


KUVIO 50. Tietoturvakäytänteitä omaavien yritysten suhteelliset osuudet toimialoittain vastanneista yrityksistä (Prior Konsultointi 2016)

Tutkimuksen mukaan parhaiten tietoturvasta huolehtii ”terveys ja sosiaalipalvelut” -toimialan yritykset (N=31), joista lähes kahdella kolmasosalla (64 %) oli käytössään ”4 tai enemmän” tietoturvakäytäntöjä. Toimialoista ”paremmuusjärjestyksessä” seuraavana oli ”Liike-elämän palvelut” –toimialaksi nimetty ryhmä yrityksiä (N= 71, vastaa tässä TOL:n mukaista toimialaa ”Ammatillinen, tieteellinen ja tekninen toiminta”), joilla hieman vajaalla puolella (47 %) oli käytössään vähintään neljä käytännettä. ICT-alan ammattilaisia edustava ”Informaatio ja viestintä” –toimiala (N=46) sijoittui tutkimuksen vertailussa kolmannelle sijalle. Sillä toimialla 47 yrityksistä oli käytössään 2-3 tietoturvakäytännettä. Neljänneksi sijoittui yhdistetty ”Teollisuus” ja ”Sähkö-, kaasu- ja lämpöhuolto, jäähdytysliiketoiminta” toimialat ja huonoimmin vertailussa menestyi ryhmä ”Muut toimialat”. (Aitoa digitaalisuutta vai työsuhdekännyköitä? Tutkimus suomalaisten Pk-yritysten digitalisaation asteesta 2016, 19.)

Kun tarkastellaan kuviossa 51 havainnollistettuja verrokkitutkimuksen tuloksia suhteessa oman tutkimukseni kysymyssarjasta ”3. Prosessit” saatuihin tuloksiin, voidaan todeta, että ”paremmuusjärjestys” on kolmen tietoturvastaan parhaiten huolta pitävien toimialojen välillä täsmälleen sama. Erot omassa tutkimuksessani ovat pieneh-

köjä mutta selviä. ”Terveys- ja sosiaalipalvelujen” –toimiala erottuu edukseen molemmissa tutkimuksissa ja omassa tutkimuksessani lisäksi myös kysymyssarjoissa 1, 2 ja 4. Perustellulla syyllä Prior Konsultointi Oy toteaakin verrokkitutkimuksen tuloksia esitellessään, että *”sosiaali- ja terveyspalvelut ovatkin ainoa toimiala joka huolehtii tietoturvasta”*. (Aitoa digitaalisuutta vai työsuhdekännyköitä? Tutkimus suomalaisten PK-yritysten digitalisaation asteesta 2016, 19.)



KUVIO 51. Toimialakohtaiset vastauskeskiarvot kysymyssarjassa kolme ”3. Prosessit”

6.4.3 Kansainvälinen verrokkitutkimus

Kansainvälisen pk-yrityksiä koskevan verrokkitutkimukseen löytäminen osoittautui haasteelliseksi. Useimmissa kaupallisten toimijoiden tekemissä yritysten kyberturvallisuutta ja siihen varautumista koskevissa kansainvälisissä tutkimuksissa on vastaajina pääasiassa keskikokoisia ja suuria yrityksiä ja pienten yritysten osuus on yleensä hyvin vähäinen.

Onnistuin kuitenkin löytämään verrokiksi osana Iso-Britannian National Cyber Security Program -ohjelmaa toteutetun määrällisen ja laadullisen tutkimuksen, jonka teetti Department for Culture, Media and Sport. Tutkimuksen toteutti Ipsos MORI Social Research Institute yhteistyössä University of Portsmouth:in yksikön Institute for Criminal Justice Studies kanssa. (Klahr ym. 2016, 3.)

Tutkimuksessa haastateltiin puhelimen välityksellä 1008 sattumanvaraisesti valittua Iso-Britanniassa toimivaa yritystä pääasiassa joulukuun 2015 ja tammikuun 2016 aikana. Haastatelluista yrityksistä oli 28 % mikroyrityksiä (2-9 työntekijää), 17 % pien-

yrityksiä (10-49), 35 % keskisuuria yrityksiä (50-249) ja 20 % suuryrityksiä (250 +). Tutkimukseen osallistuneiden yrityksen profiilia suhteessa kyberturvallisuuden haasteisiin kuvaa hyvin se, millaisen osan online-palvelut muodistavat yrityksen ydinpalvelutarjonnasta. Vastaajista 14 % ilmoitti online-palveluja olevan suuressa määrin, 39 % jossakin määrin ja lähes puolella (47 %) ei lainkaan. (Klahr ja muut 2016, 9.)

Mikroyrityksistä 17 % ja pienyrityksistä 33 % ilmoitti haastattelussa olleensa kybertuvallisuuteen liittyvän tietomurron tai hyökkäyksen kohteena viimeksi kuluneiden 12 kuukauden aikana haastattelun ajankohdasta lukien. Kaikkien vastanneiden keskiavo oli 24 %. (Klahr ym. 2016, 34.) Kyberturvallisuutta piti tärkeänä 37 % (fairly high priority) tai erittäin tärkeänä 33 % (very high priority) kaikista vastaajista (Klahr ym. 2016, 15).

Verrokkitutkimuksen mukaan 16 % mikroyrityksistä ja 47 % pienyrityksistä on kyberturvallisuusriskit dokumentoituna osaksi liiketoiminnan jatkuvuussuunnitelmaa, sisäisiä auditointeja sekä riskienhallintaa. Kaikilla tutkimukseen osallistuneista vastaava luku oli 29 %. Toimialoista paras tilanne (49 %) oli rahoitus- ja vakuutusalalla, koulutusalalla sekä terveys- ja sosiaalipalvelujen alalla. (Klahr ym. 2016, 25.)

Tutkimukseni kysymyssarjassa ”2. Tieto ja sen merkitys liiketoiminnalle” yrityksille esitettyyn väittämään ”kyberturvallisuusuhkien varalta on dokumentoitu varautumissuunnitelma, jolla pyritään varmistamaan digitaalinen jatkuvuus” vastasi yrityksistä 20 % vaihtoehdolla ”hyvin” ja 10 % vaihtoehdolla ”kohtalaisesti”. Yrityksistä 35 % valitsi vaihtoehdon ”heikosti” ja saman suuruinen osuus (35 %) vastaajista vastasi vaihtoehdolla ”ei lainkaan”. Toimialoista ”Ammatillinen, tieteellinen ja tekninen toiminta” oli valmistautunut vastausten perusteella parhaiten.

Mikäli näiden lukujen valossa tarkastellaan verrokkitutkimuksen kuvaamaa tilannetta Iso-Britanniassa ja verrataan sitä tähän Keski-Suomessa tehtyyn tutkimukseen, voidaan todeta varautumistilanteen olevan melko samankaltainen toimialakohtaisia eroja lukuun ottamatta. Oletuksena on, että paikalliseen tutkimukseen vastanneet tarkoittavat vaihtoehdoilla ”hyvin” ja ”kohtalaisesti” sitä, että kyberturvallisuusuhkat sisältävä varautumissuunnitelma on olemassa.

Verrokkitutkimuksessa yrityksiltä kysyttiin, onko yritysten hallituksen jäsenenä henkilöä, jolle kyberturvallisuus on vastuutettu. Mikroyrityksistä 21% ja pienyrityksistä

37% ilmoitti vastuutuksen olevan tehty. Kaikista vastaajista 28% oli järjestänyt asian kysymyksen ilmaisemalla tavalla. (Klahr ym. 2016, 27.) Tutkimukseni kysymyssarjassa ”3. Prosessit” esitettiin yrityksille väittämä ”yrityksessä on määritelty ja dokumentoitu turvallisuuteen liittyvät vastuut ja päätösvalta”. Vastaajista 30 % valitsi vaihtoehdon “hyvin” ja 20 % valitsi vaihtoehdon kohtalaisesti. Tutkimuksissa käytettyjen termien eroavaisuuksista huolimatta tilanne näyttää olevan molempien tutkimusten perusteella se, että kyberturvallisuuden vastuuttaminen mikro- ja pienyrityksissä on yli puolella yrityksistä tekemättä. Tästä johtuen on mahdollista, että siihen ei olla kovin helposti valmiita panostamaan, koska asia ei ole erityisesti kenenkään henkilön vastuulla.

Verrokkitutkimuksessa käsiteltiin myös henkilöstön kyberturvallisuusosaamisen kehittämistä. Haastattelussa kysyttiin, ”onko henkilöstöä osallistunut kyberturvallisuutta koskevaan sisäiseen tai ulkoiseen koulutukseen, seminaariin tai konferenssiin viimeisen 12 kuukauden aikana.” Mikroyrityksistä 12% vastasi kysymykseen myönteisesti ja 22% pienyrityksistä oli panostanut aiheeseen. Kaikista vastaajista 17% vastasin kysymykseen ”kyllä”. (Klahr ym. 2016, 24.)

Tutkimukseni kysymyssarjassa ”4. Henkilöstön tietoisuus ja osaaminen” yritykset vastasivat väittämään ”Yrityksen henkilöstöä on koulutettu tunnistamaan ja käsittelemään kyberturvallisuuspoikkemia.” Vastauksista 20 % edusti vaihtoehtoa ”hyvin” ja 45 % oli vaihtoehdon ”kohtalaisesti” kannalla. ”Heikosti” oli asiaa hoitanut 25 % yrityksistä ja vastauksen ”ei lainkaan” valitsi 10 % vastanneista.

Kysymykset tutkimuksissa olivat jossakin määrin erilaisia johtuen siitä, että verrokkitutkimuksessa oli mukana aikaulottuvuus ja vastausvaihtoehtoina vain ”kyllä” tai ”ei”, joka sinänsä se antaa selkeämmän kuvan tilanteesta kuin omassa tutkimuksessani käytetty viisiportainen asteikko Likert –asteikko. Tutkimusten eroavaisuuksista huolimatta on molempien tutkimusten mukaan selvää, että mikro- ja pienyritykset eivät ole - muiden yritysten tavoin - paljoa panostaneet henkilöstönsä kyberturvallisuusosaamisen kehittämiseen, sillä vain joka viides yritys ilmoitti asian olevan kunnossa.

Lisäksi verrokkitutkimus sisälsi monia mielenkiintoisia kysymyksiä koskien konkreettisia kyberuhkia sekä kysymyksiä, jotka liittyivät Iso-Britannian valtion tekemiin panostuksiin kyberturvallisuuden lisäämiseksi. Yksi tutkimuksessa esiin tullut seikka oli

FINCSC® -sertifiointimalliin rakentamisessa benchmarkatut Cyber Essentials ja Cyber Essentials Plus arviointimallit, joiden käyttöä alihankkijoita valittaessa kysyttiin yrityksiltä. Kaikista vastaajista (N=241) Cyber Essentials -mallia tai sen noudattamista edellytti 8% päämiehistä. Cyber Essentials Plus –mallin kohdalla vastaava luku oli 5%. (Klahr ym. 2016, 30.)

7 JOHTOPÄÄTÖKSET, POHDINTA JA TULOSTEN HYÖDYNTÄMINEN

7.1 KESKEISET TULOKSET

Tämän tutkimuksen päätavoitteena oli tuottaa tietoa Keski-Suomessa toimivien pk-yritysten kyberturvallisuustietoisuuden ja kyberuhkiin varautumisen nykytilasta eri osa-alueilla. Tietoa hyödynnetään pk-yritysten kyberturvallisuustietoisuuden ja -osaamisen kehittämisessä sekä FINCSC®-sertifiointijärjestelmän kehittämisessä.

Tutkimusmenetelmäksi valikoitui strukturoitu haastattelututkimus, joka oli osana Cyber Scheme Finland –pilottiprojektissa tehtyä sertifiointimallin pilotointivaihetta, johon osallistui pääosin Keski-Suomen alueella toimivia pk-yrityksiä.

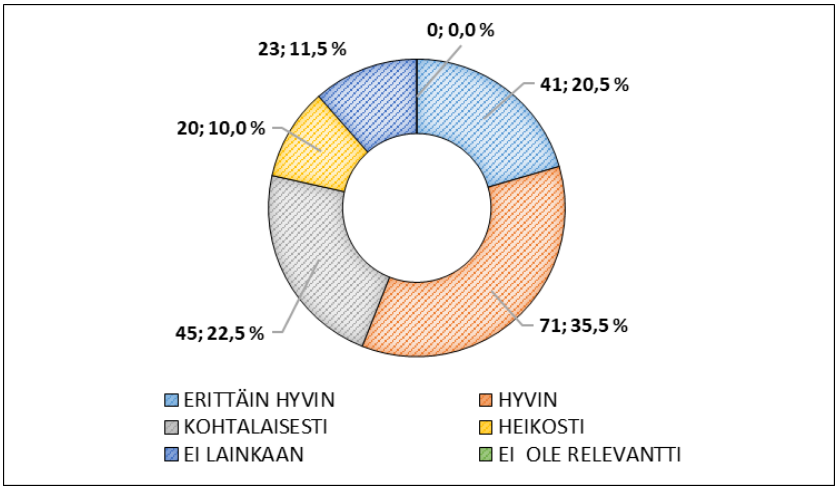
Tutkimus jakautui viiteen tutkimuskysymykseen, joita jokaista varten kokosin teemasta riippuen 7-15 kysymystä käsittäneen kysymyssarjan. Vastaajilla on haastattelutilanteessa käytössään viisiportainen sanalliset vastausvaihtoehdot sisältänyt Likert –asteikko.

Tarkastelen seuraavassa tutkimuksen keskeisiä tuloksia tutkimuskysymyksittäin.

Tutkimuskysymys 1: Miten yritykset ymmärtävät kyberturvallisuuden käsitteenä ja millainen merkitys sillä on yritykselle?

Tutkimuskysymykseen haettiin vastauksia kysymyssarjan ”1. Käsitteet ja strategia näkökulma” avulla. Analysoitavia vastauksia kertyi yhteensä 200. Kuviossa 52 on nähtävissä annettujen vastausten lukumäärät ja eri vastausvaihtoehtojen suhteelliset prosenttiosuudet kaikista vastauksista. Vastaukset jakautuivat prosentuaalisesti siten, että vaihtoehto ”5 erittäin hyvin” muodostaa noin viidesosan vastauksista. Vaihtoehto ”4 hyvin” on valittu reiluun kolmasosaan vastauksista. Vaihtoehtoa ”3 kohtalaisesti” on käytetty reilussa viidesosassa vastauksista. Vaihtoehtoa ”2 heikosti” vastauksia on kymmenesosa ja ”1 ei lainkaan” -vastauksia on hieman yli kymmenesosa.

Kaikki tämän kysymyssarjan kysymykset olivat yritysten mielestä relevantteja kysymyksiä heidän toimintansa näkökulmasta ajatellen.



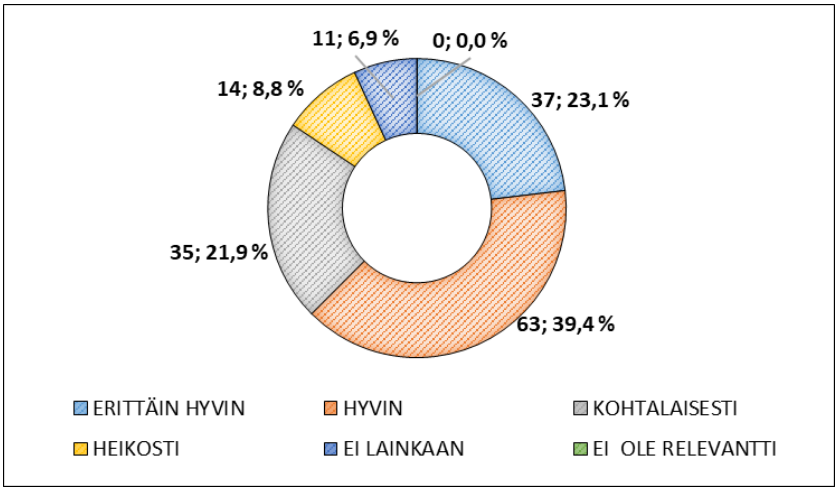
KUVIO 52. Kaikkien vastausten määrällinen ja suhteellinen jakauma kysymyssarjassa yksi (N=200)

Kuviossa 16 esitettyä ”uhkatilanteiden esiintymistä” ja kuviossa 17 esitettyä ”kyberturvallisuus uhkatekijänä” –kysymyksiä lukuun ottamatta muut kahdeksan kysymyssarjan kysymystä ovat muotoiltu niin, että tilanne kyberturvallisuuden kannalta on sitä parempi mitä suuremman numeraalisen arvon ja sitä kautta positiivisemman vaihtoehdon vastaaja valitsee. Näin ollen kyseisiin kysymyksiin annetut vastaukset hieman vääristävät kaikkien annettujen vastausten lukumäärään perustuvaa tarkastelua.

Kun jätetään vastauksista pois edellä mainittuihin kahteen kysymykseen annetut vastaukset, tulee vastausten määräksi yhteensä 160. Vastausten jakauma esitetään alla olevassa kuviossa 53. Vastauksista 100 eli lähes kaksi kolmasosaa edustaa vaihtoehtoja ”hyvin” tai ”erittäin hyvin”. ”Kohtalaisesti” -vastauksia on yhteensä 35 eli suhteellisesti hieman yli viidesosa vastauksista. Vastauksia ”heikosti” tai ”ei lainkaan” on yhteensä 25 eli suhteellisesti ottaen hieman vajaa kuudesosa annetuista vastauksista.

Vastausten jakauman perusteella voidaan vetää se johtopäätös, että haastatteluun osallistuneet yritykset ovat ymmärtäneet keskimäärin hyvin kyberturvallisuuden merkityksen ja ottaneet sitä myös huomioon yrityksen strategiaa suunnitellessaan. Myös asennoituminen kyberturvallisuuteen ja sen hallintaan on pääosin myönteistä

ja kyberturvallisuus koetaan yrityksissä huomattavasti vahvemmin mahdollisuutena kuin uhkana.

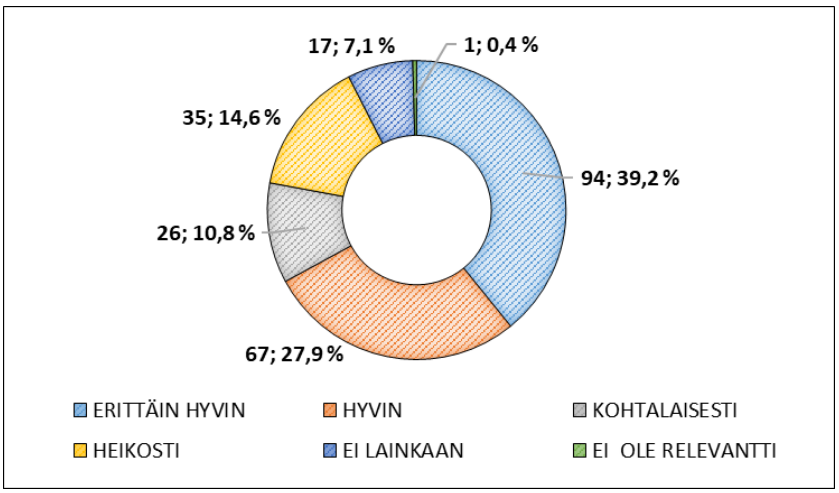


KUVIO 53. Vastausten jakauma ilman ”uhkatilanteet” ja ”uhkatekijä”-kysymyksiin liittyviä vastauksia N=160

Tutkimuskysymys 2: Miten yritys on tunnistanut tiedon ja sen turvallisen käsittelyn merkityksen liiketoiminnalle?

Kysymyssarjaan ”2. Tieto ja sen merkitys liiketoiminnalle” annettiin yhteensä 240 vastausta. Kuviosta 54 on nähtävissä annettujen vastausten lukumäärät ja eri vastausvaihtoehtojen suhteelliset prosenttiosuudet kaikista vastauksista. Vastausten perusteella voidaan muodostaa käsitys siitä, miten yritykset ovat tunnistaneet tiedon ja sen turvallisen käsittelyn merkityksen liiketoiminnalleen. Lähes 40 % vastauksista on vaihtoehtoa ”erittäin hyvin” ja yhdessä ”hyvin” –vastausten kanssa ne muodostavat vastauksista yli kaksi kolmasosaa (67,1 %). Siinä mielessä tilanne näyttää hyvältä. Toisaalta yli viidesosa (21,7 %) vastauksista ovat vaihtoehtoja ”heikosti” tai ”ei lainkaan” ja kymmenesosa (10,7 %) vastauksista on vaihtoehtoa ”kohtalaisesti”. Vaihtoehto ”ei relevantti” esiintyy vastausten joukossa vain yhden (1) kerran.

Kuten edellä yksittäisiin olevassa yksittäisiin kysymyksiin annettujen vastausten analyysistä kävi ilmi, on yrityksillä vastaustensa mukaan hyvällä tasolla olevasta tiedon arvostuksesta huolimatta kuitenkin vielä paljon työtä tehtävänään, jotta tunnistetut kehittämistarpeet muuttuisivat konkreettisiksi toimenpiteiksi ja sitä kautta lisääntyneeksi sietokyvyksi kyberturvallisuusuhkia vastaan.

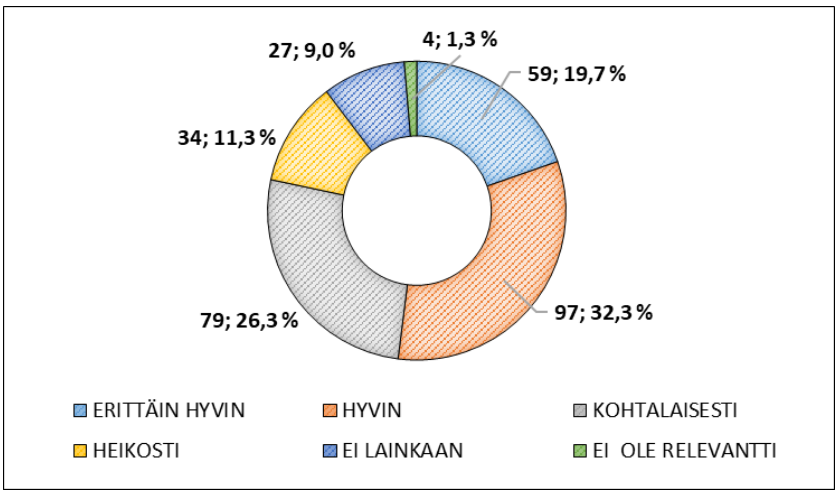


KUVIO 54. Annettujen vastausten määrällinen ja suhteellinen jakauma kysymyssarjassa kaks (N=240)

Tutkimuskysymys 3: Miten yrityksen toimintaprosesseissa on otettu kyberturvallisuus huomioon?

Kysymyssarja ”3. Prosessit” on kysymysten lukumäärältään laajin tämän tutkimuksen viidestä kysymyssarjasta sisältäen yhteensä 15 kysymystä. Kysymyksiin annettiin yhteensä 300 vastausta, joiden lukumääräinen jakauma sekä eri vastausvaihtoehtojen suhteelliset prosenttiosuudet kaikista vastauksista ovat nähtävissä kuviossa 55. Hieman yli puolet eli 50,2 % vastauksista edustaa vaihtoehtoja ”hyvin” tai ”erittäin hyvin”. Reilu neljännes vastauksista eli 26,3 % on vaihtoehtoa ”kohtalaisesti”. ”Heikosti” vastauksia on 11,3 % ja ”ei lainkaan” vastauksia on vajaa kymmenesosa eli 9,0 % kaikista kysymyssarjaan annetuista vastauksista. Vastausvaihtoehtoa ”ei relevantti” on käytetty neljässä vastauksessa.

Siitä huolimatta, että eri kysymyssarjoihin annettuja vastauksia ei voi suoraan vertailla kysymyssarjojen välillä, voidaan saatujen vastausten perusteella todeta, että kyberturvallisuuden huomioonottaminen yrityksen toimintaprosesseissa on alhaisemmalla tasolla kuin siihen liittyvien tarpeiden tiedostaminen kysymyssarjassa 2. Tiedostaminen on hyvä lähtökohta ja tämä on tavanomainen kehityspolku, joka etenee yrityskohtaisesti sen mukaan mitä kukin yritys liiketoiminnassaan painottaa ja millaisia toimenpiteitä on resurssien näkökulmasta mahdollista ja järkevää lähteä toteuttamaan.



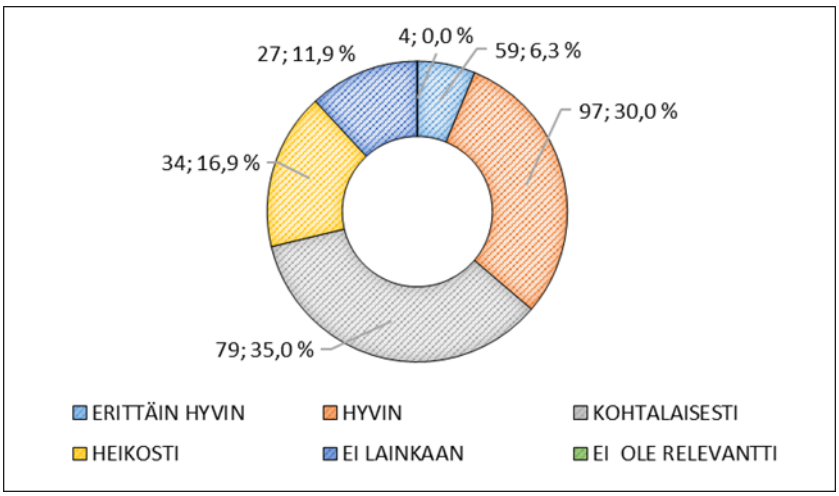
KUVIO 55. Annettujen vastausten määrällinen ja suhteellinen jakauma kysymyssarjassa kolme (N=300)

Tutkimuskysymys 4: Miten yritys on ottanut kyberturvallisuuden huomioon henkilöstön osaamisessa?

Kysymyssarjan ”4. Henkilöstön tietoisuus ja osaaminen” kahdeksaan kysymykseen annettiin yhteensä 160 vastausta. Niiden lukumääräinen jakauma sekä eri vastausvaihtoehtojen suhteelliset prosenttiosuudet kaikista vastauksista ovat nähtävissä kuviossa 56. Hieman yli kolmannes eli 36,3 % vastauksista edustaa vaihtoehtoja ”hyvin” tai ”erittäin hyvin”. Lähes yhtä suuri osuus vastauksista eli 35,0 % on vaihtoehtoa ”kohtalaisesti”. ”Heikosti” vastauksia on 16,9 % ja ”ei lainkaan” vastauksia on hieman yli kymmenesosa eli 11,9 % kaikista kysymyssarjaan annetuista vastauksista. Vastausvaihtoehtoa ”ei relevantti” käytettiin neljässä (4) vastauksessa.

Tähän mennessä läpikäydyistä neljästä kysymyssarjasta on yritysten tilanne tähän kysymyssarjaan liittyvällä osa-alueella heikoimmalla tasolla, vaikka annettuja vastauksia ei voikaan suoraan vertailla kysymyssarjojen kesken.

Sekä yksittäisiin kysymyksiin saatujen vastausten, että niiden yhteenvedon perusteella voidaan todeta, että yritysten henkilöstön kyberturvallisuustietoisuuden ja –osaamisen lisääminen on selkeästi yksi teema yritysten tulevaisuuden agendalla kyberturvallisuuden sietokyvyn kehittämiseksi.

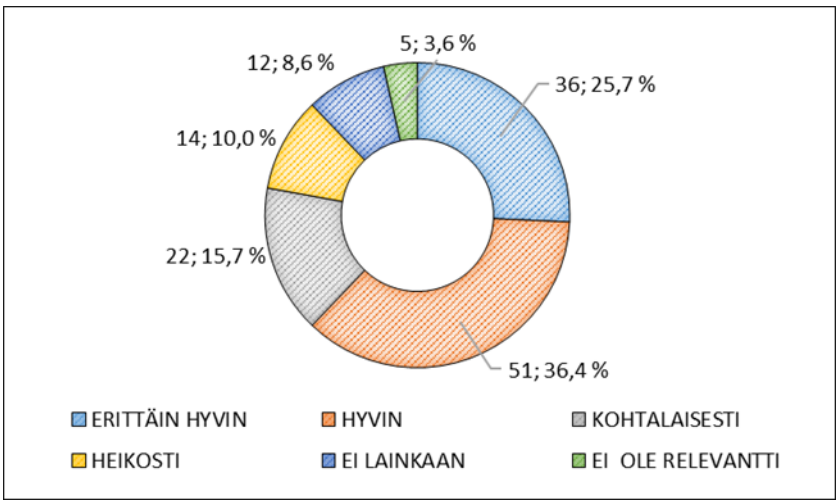


KUVIO 56. Annettujen vastausten määrällinen ja suhteellinen jakauma kysymyssarjassa neljä (N=160)

Tutkimuskysymys 5: Miten kyberturvallisuus on otettu huomioon yrityksen fyysisessä ympäristössä?

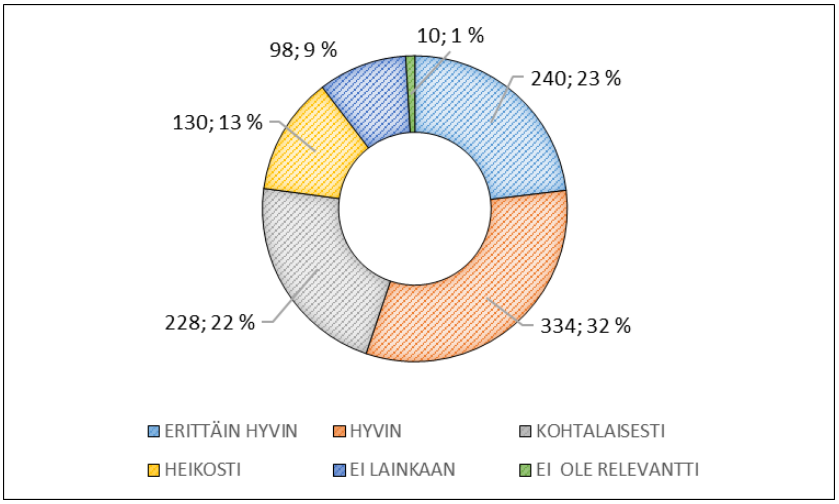
Kysymyssarjan ”5. Fyysinen turvallisuus” seitsemään kysymykseen kertyi yhteensä 140 vastausta. Niiden lukumääräinen jakauma sekä eri vastausvaihtoehtojen suhteelliset prosenttiosuudet kaikista vastauksista ovat nähtävissä kuviossa 57. Hieman yli neljäsosa (25,7 %) annetuista vastauksista edustaa vaihtoehtoa ”erittäin hyvin” ja reilu kolmannes (36,4 %) vastauksista on vaihtoehtoa ”hyvin”. Yhteensä nämä kaksi parhainta vaihtoehtoa muodostavat 62,1 % kaikista kysymyssarjaan annetuista vastauksista. Vajaa kuudesosa (15,7 %) vastauksista vaihtoehtoa ”kohtalaisesti”. ”Heikosti” vastauksia on 10,0 % ja ”ei lainkaan” vastauksia on alle kymmenesosa (8,6 %) annetuista vastauksista. Vastausvaihtoehtoa ”ei relevantti” käytettiin viidessä (5) vastauksessa.

Kysymyssarjaan ”5. Fyysinen turvallisuus” annettujen vastausten jakauma osoittaa, että kysytyt asiat olivat yrityksissä melko hyvällä tasolla. Osa kysymyksistä - kuten lukitukset ja toimitilojen pääsynhallinta –kohdentuivat seikkoihin, jotka tulisi luontaisesti olla kunnossa myös tiloissa, joissa ei käytetä tai säilytetä lainkaan tietojärjestelmiä, laitteita tai tietoa. Haastattelutilanteissa aistinvaraisesti tekemieni havaintojen perusteella osa kysymyksistä ”herätteli” vastaajia huomaamaan, että yksittäiset ja jopa arkipäiväisiltä tuntuvat asiat voivat olla seikkoja, joilla yrityksen kyberturvallisuutta voidaan parantaa.



KUVIO 57. Annettujen vastausten määrällinen ja suhteellinen jakauma kysymyssarjassa viisi (N=140)

Tutkimuksen 52 kysymykseen annettiin yhteensä 1040 vastausta. Ne jakautuivat eri vastausvaihtoehtojen välillä alla olevan kuvion 58 mukaisesti. Hieman yli puolet vastauksista (55 %) edustaa vaihtoehtoja ”hyvin” tai ”erittäin hyvin”. Vastaavasti vaihtoehtoja ”heikosti” tai ”ei lainkaan” on vastauksista reilu viidennes (22 %) eli yhteensä saman verran kuin vastauksia ”kohtalaisesti”. Vaihtoehtoa ”ei relevantti” on käytetty vain kymmenessä vastauksessa (1 %).



KUVIO 57. Kaikkien tutkimukseen saatujen vastausten määrällinen ja suhteellinen jakauma (N=1040)

Tutkimuksen tuloksia kokonaisuutena voidaan tarkastella myös kuvion 58 avulla. Se on koottu kuhunkin kysymyssarjaan annetuista vastauksista osoittaen kysymyssarjakohtaisten - ja samalla myös tutkimuskysymyskohtaisten - vastausten keskiarvoa ja

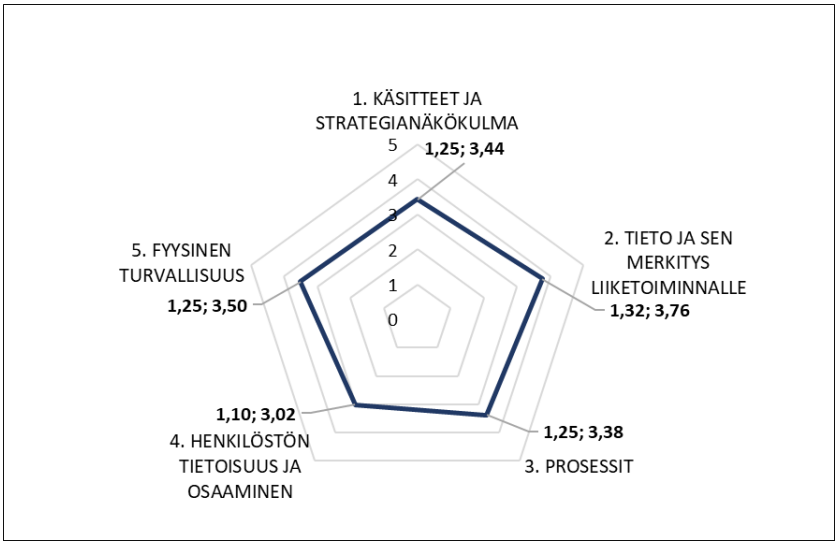
keskihajontaa. Näin ollen se edustaa tutkimukseen osallistuneiden yritysten antamien vastausten perusteella saatavaa keskimääräistä tilannetta kunkin kysymysryhmän osalta.

Ottaen huomioon se, mitä aiemmin on todettu kysymys- ja kysymysryhmäkohtaisista tuloksista, voidaan koko tutkimuksen keskeiset tulokset kiteyttää seuraaviin johtopäätöksiin, joita kuvion 58 osaltaan havainnollistaa.

1. Ymmärrys kyberturvallisuudesta ja sen monista ulottuvuuksista oli vastaajille jossakin määrin epäselvä, vaikka se terminä tunnistettiinkin. Sen sisällyttäminen yrityksen strategiaan oli vain tasoa ”kohtalainen”, mikä oli tuloksena samansuuntainen verrokkitutkimusten kanssa. Luonnollista on, että etenkin mikroyrityksillä on päivittäisen liiketoiminnan parissa niin paljon tehtävää, että aika ei millään riitä keskittymään muihin kuin strategisiksi tunnistettuihin asioihin. Positiivista oli se, että useimmat yritykset näkivät kyberturvallisuuden olevan hyvin hoidettuna yritykselle kilpailutekijä. Saatu tulos tukee tietoperustassa esiintuotuja seikkoja kyberturvallisuus -käsitteen laajuudesta ja kompleksisuudesta.
2. Tiedon ja sen käsittelyssä käytettävien välineiden ja ohjelmistojen kriittinen merkitys liiketoiminnalle tunnistettiin yritysten keskuudessa hyvin. Tiedon arvon ja sen liiketoiminnalle tuottaman hyödyn määrittely oli suurimmalla osalla vastaajista alkutekijöissään. Digitaalisen jatkuvuuden menettäminen tunnistettiin mahdolliseksi riskiksi hyvin, mutta dokumentoitu palautumissuunnitelma löytyy vain harvasta vastaajayrityksestä. Terveys- ja sosiaalipalvelujen toimialan yritykset erottuvat joukosta positiivisesti. Toimialla vaadittava tietosuojan taso on edellyttänyt yrityksiltä toimenpiteitä, jotka vaikuttavat kyberturvallisuuteen.
3. Tutkimuksessa esillä olleista prosesseista on parhaiten kunnossa tietojärjestelmiin liittyvä pääsynhallinta. Vastuukysymyksiin ja muutoksenhallintaan liittyvän ohjeistuksen ja dokumentaation vähäisyys nousee vastauksista selkeänä kehityskohteena. Samoin on laita myös suoraan kyberturvallisuuden suunnitelmalliseen hallintaan liittyvien toimenpiteiden kohdalla.
4. Tutkimuksen viidestä osa-alueesta huonoimman tuloksen tuottivat henkilöstön kyberturvallisuustietoisuuteen ja osaamiseen liittyvät vastaukset, joiden mukaan yrityksissä ei ole asiaan juurikaan panostettu. Huonoin tilanne tällä osa-alueella

on teollisuuden sekä sähkö-, kaasu- ja lämpöhuolto/jäähdytysliiketoiminnan toimialoja edustavissa yrityksissä, mutta kaikilla toimialoilla on parantamisen varaa riittävästi. Kansainvälinen verrokkitutkimus osoitti vastaavantyyppisen tilanteen vallinneen tutkimusajankohtana myös Iso-Britanniassa.

5. Fyysisen turvallisuuden osa-alue on tutkituissa yrityksissä kokonaisuudessaan kohtuullisen hyvällä tasolla. Osa tutkimuksessa esillä olleista asioista – kuten esimerkiksi fyysinen pääsynhallinta - on turvallisuuteen liittyvää ”perusasiaa”, joka on yleisen tietämyksen mukaan yrityksissä vähintään kohtuullisesti järjestetty. Tietojen käsittelyyn ja tallentamiseen käytettäviä laitteita varten on useimmilla yrityksillä vastaustensa perusteella palo- ja murtosuojatut säilytysolosuhteet, mikä niiltä osin mahdollistaa liiketoimintakriittisen tiedon säilymisen vahingoittumattomana.



KUVIO 58. Kaikkien tutkimukseen saatujen vastausten keskihajonnat ja -arvot kysymysryhmittäin jaoteltuina (N=1040)

Yhteenvetona tutkimuksesta voidaan todeta, että se toi selkeästi esille yrityksessä vallitsevaa tilannetta varautumisesta kyberturvallisuusuhkia vastaan sekä siihen liittyviä kehittämiskohteita. Näin ollen tutkimuksella saavutettiin haluttu tarkoitus ja saatiin vastaukset tutkimuskysymyksiin. Varsinaisesti uutta teoreettista antia tutkimus ei tuottanut, mutta tämä ei ollut tutkimuksen tarkoituksenakaan. Vapaamuotoisten kommenttien perusteella voidaan myös todeta, että tutkimushaastattelu toimi osalla yrityksistä ”herättelijänä” ja silmien avaajana, mikä osaltaan auttoi yrityksiä valmistautumaan FINCSC® -sertifiointimallin pilotointiin.

7.2 TUTKIMUKSEN LUOTETTAVUUDEN ARVIOINTI

Tutkimuksen luotettavuuden arvioinnissa keskeisiä käsitteitä ovat *reliabiliteetti* sekä *validiteetti*. Reliabiliteetilla tarkoitetaan tutkimuksen kykyä antaa samoja tai samanlaisia tuloksia myös tutkimusta toistettaessa. Tutkimusmenetelmää voidaan sanoa reliaabeliksi esimerkiksi tilanteessa, jossa kaksi tai useampi tutkijaa päätyy samaan tutkimus tulokseen eri tutkimuskerroilla kyseistä menetelmää käyttäen.

Tutkimuksen *validiteetilla* tarkoitetaan tutkimusmenetelmän kykyä mitata sitä asiaa tai niitä ilmiöitä, joita sillä on tarkoitus mitata. Validiteetti ilmaisee tutkimusmenetelmän soveltuvuutta instrumenttina kyseisen tyyppisen tutkimuksen tekemiseen. (Hirsjärvi ym. 2000, 213.)

Tutkimuksen ja sen tulosten luotettavuuden varmistamiseksi kiinnitettiin tutkimuksen suunnittelun ja toteuttamisen aikana huomiota seuraaviin seikkoihin:

- Koska oli etukäteen tiedossa, että kyberturvallisuus käsitteenä on suurelle yleisölle ainakin jossakin määrin epäselvä asia, pyrin tutkimusmenetelmän valinnassa siihen, että epätietoisuus käsitteistä vaikuttaisi mahdollisimman vähän tutkimuksen tuloksiin. Tämä seikka sekä luvussa 6.2 mainitut muut seikat yhdessä vaikuttivat siihen, että menetelmäksi valikoitui strukturoitu haastattelututkimus.
- Tutkimuksen kysymysten selkeyttä ja ymmärrettävyyttä pyrin lisäämään etukäteen pyytämällä kollegoilta kommentteja kysymysten muotoon ja sisältöön sekä toteuttamalla koehaastattelun pk-yrityksessä. Sen perusteella tein joitakin muutoksia kysymyksiin ymmärrettävyyden lisäämiseksi.
- Kaikille haastateltaville lähetettiin saman sisältöinen ennakkotiedote haastattelusta ja kysymyksiin vastaamisen tapa sekä vastausten kirjaaminen käytiin läpi kunkin vastaajan kanssa haastattelutilanteen alussa.
- Kysymykset esitettiin kaikille haastateltaville sanatarkasti juuri samassa muodossa eli sama kysely toistettiin tässä tutkimuksessa 20 kertaa. Kaikilla haastateltavilla oli haastattelutilanteessa käytössään sama viisiportainen Likert-asteikko sanallisine vastausvaihtoehtoineen ja niitä vastaavine numeroineen paperille tulostettuna. Vastaus määräytyi sen mukaan, minkä vastausvaihtoehdon mukaiseksi vastaaja koki tilanteen yrityksessään haastatteluhetkellä olevan.

Tutkimuksen tuloksiin liittyy myös epävarmuustekijöitä, jollaisiksi olen tunnistanut seuraavat haastateltaviin henkilöihin liittyvät seikat:

- Huolimatta siitä, että pyrin saamaan kysymyksistä mahdollisimman yksiselitteisiä ja kansantajuisia on aina mahdollista ymmärtää kysymys toisin kuin mitä haastattelija on sen tarkoittanut. Ymmärryksen vaikuttaa myös haastateltavan taustatieto tutkittavasta aiheesta sekä kyky että halu arvottaa asioita. Jokin asia saattaa olla toisen haastateltavan mielestä ”erittäin hyvin”, mutta toisen mielestä ”hyvin” tai ehkä vain ”kohtalaisesti”. Vastaushetkellä kunkin vastausvaihtoehdon todellisen merkityksen määrittää haastateltava.
- Toisena epävarmuustekijänä on haastateltavan objektiivisuus. Haastateltava saattaa kysymyksen kuultuaan yhtäkkiä huomata, että kysymys koskee asiaa joka pitäisi olla kunnossa, mutta todellisuudessa ei sitä ole. Haastateltavalla on vastausvaihtoehtoa valitessaan mahdollisuus ”pyöristää” todellista tilannetta ylöspäin positiivisempaan suuntaan, mutta toki myös negatiivisempi suuntakin on mahdollinen. Tutkimuksessa käytetty Likert-asteikko mahdollistaa objektiivisuuden heikentyessä ”vähemmän väärin vastaamisen” helpommin kuin pelkkä kyllä / ei -asteikko. Mikäli vastausvaihtoehdot olisivat olleet kyllä / ei, olisi haastattelun tulos ollut varmasti erilainen. Sitä, olisiko se objektiivisuuden näkökulmasta ollut parempi vai huonompi, on mahdoton sanoa, mutta joka tapauksessa se olisi mustavalkoisuudessaan heikentänyt tutkimuksen validiteettia.
- Kolmantena epävarmuustekijä tuloksissa on mahdollinen haastateltavan tietämättömyys. Kyselyssä on saattanut tulla esiin seikkoja, joihin haastateltava ei ole tiennyt oikeaa vastausta, vaikka sellainen olisi ollutkin olemassa. Koska vastaus vaihtoehtona ei ollut vaihtoehtoa ”en tiedä”, oli vastaajan valittava joku esillä olleista vaihtoehdoista. Näin ollen vastaajalla on ollut mahdollisuus antaa vastauksensa tietämättä asian oikea laitaa, vaikka vain arvaukseen perustuen. Näkemykseni mukaan tässä haastattelussa kyseinen epävarmuustekijä on kuitenkin hyvin vähäinen, koska haastateltavana henkilöinä oli useimmissa tapauksissa yrityksen omistaja/yrittäjä, joka tyypillisessä mikro- tai pienyrityksessä pitää kaikkia lankoja käsissään.

Jokaisella tutkimusmenetelmällä on myös omat rajoitteensa. Tiukasti strukturoitu haastattelututkimus, joka halutaan toistaa täsmälleen samanlaisena jokaisen haastateltavan kohdalla, ei periaatteessa mahdollista kysymysten tai vastausten laajempaa avaamista haastattelutilanteessa. Toisaalta se parantaa tutkimuksen validiteettia, koska vastauksiin ei sisälly sekä haastateltavan että haastattelijan mahdollista tulkintaa.

Tässä tutkimuksessa käytettiin kaikissa kysymyksissä vain yhtä, sanamuodoltaan tarkkaan harkittua arviointiasteikkoa. Haastattelujen aikana huomasin, että asteikko olisi joiden kysymysten kohdalla ollut kysymykseen sopivampi jossakin toisessa taivutusmuodossa. Tutkimuksen toistettavuuden vuoksi en kuitenkaan halunnut muuttaa sanamuotoja kesken haastattelujen. Sen sijaan tutkimuksen raportointivaiheessa käytin joissakin graafisissa kuvaajissa ja niitä selittävissä teksteissä joiltakin osin alkuperäisestä asteikosta muunnettua sanamuotoa, jotta se kielellisesti soveltuisi paremmin vastaukseksi. Varsinaisiin tutkimuksen tuloksiin tällä ei ollut vaikutusta. Vastaavanlaisessa tilanteessa voisi jatkossa käyttää tarvittaessa muuntuvaa sanamuotoa numeraalisten vaihtoehtojen rinnalla.

Tutkimuksessani suunnitteluvaihe ja tutkimushaastattelut sijoittuivat ajallisesti lähekkäin ilman mainittavia viiveitä tutkimusprosessin kulussa. Sen sijaan haastattelujen toteuttamisen ja tulosten analysoinnin ja raportoinnin välille aiheutui vajaan kahden vuoden mittainen ajanjakso. Koska kaikki tutkimuksen suunnitteluun ja käytännön tutkimustyön toteuttamiseen liittyvä aineisto oli dokumentoitu ja tallennettu sähköiseen muotoon, oli se käytettävissä täsmälleen samassa muodossa kuin se oli viimeisen tutkimushaastattelun toteuttamisen jälkeen. Mikään seikka ei ollut muistini varassa ja kaikki tarvittava tieto oli dokumentoitu. Mielestäni haastattelujen ja raportoinnin välillä olleella viiveellä ei ole ollut ainakaan negatiivista vaikutusta tutkimuksen tulosten analysointiin ja raportointiin.

Kokonaisuutena ottaen tutkimusmenetelmä tuotti tutkimuksesta halutun tiedon ja saadut tulokset ovat edellä mainitut rajoitteet ja epävarmuustekijät huomioiden sinänsä luotettavia. Tässä tutkimuksessa kohdejoukkona oli 20 mikro- ja pk-yritystä, joiden antamia saadut tulokset edustavat. Kohdejoukko valikoitui toisaalta yritysten oman kiinnostuksen perusteella sekä toisaalta tutkimuksen taustalla olevan projektin

näkökulmasta, koska siinä tehtyyn sertifiointimallin pilotointiin tarvittiin yrityksiä eri toimialoilta. Tästä johtuen otoksessa on valintamenetelmästä aiheutuvaa vinoumaa.

Lisäksi otoskoko (N=20) oli kooltaan niin pieni, että tutkimuksen tulosten yleistettävyyttä ei voida laajamittaisesti tehdä. Myös toimialojen välisessä vertailussa on otettava huomioon, että toimialakohtaisia ryhmissä oli yritysten määrissä vaihteluja ryhmien välillä ja osa ryhmistä oli pieniä. Toimialojen välinen vertailu on siten myös suuntaa antava. Otoskokoa kasvattamalla ja haastateltavien satunnaisvalinnalla olisi ollut mahdollista lisätä tutkimuksen ulkoista validiteettia.

7.3 TUTKIMUKSEN EETTISYYDEN VARMISTAMINEN

Tutkimustyön eettisyyden huomioonottamiseksi tein seuraavat toimenpiteet:

- Suunnittelin haastattelulomakkeen ja vastausvaihtoehdot siten, että haastateltavien ei tarvinnut muodostaa vastausta omin sanoin. Tällöin kaikki vastaajat olivat suhteessa vastaamistapaan samanarvoisia riippumatta siitä, millaiset heidän taustatietonsa tutkittavasta asiasta olivat.
- Haastattelutilanteessa yrityksille kerrottiin mihin tarkoitukseen tutkimustietoja kerätään ja mitä tietoja tutkimuksesta julkaistaan. Erityisesti mainittiin, että yksittäistä ei voida julkistettavien tietojen perusteella tunnistaa.
- Tuloksia analysoitaessa käytin vastausvaihtoehdoista niiden numeraalista muotoa, mikä takasi jokaiseen kysymykseen annetuille vastauksille yhtäläisen käsittelyn ilman tulkintamahdollisuutta.
- Tulosten analysoinnissa ja raportoinnissa käytettiin yrityksistä koodinumeroa, jolloin yrityksen nimen ei tarvinnut olla näkyvissä. Vaikka osa yrityksistä oli tutkijalle tuttuja, ei sillä ollut vaikutusta analysoituihin tuloksiin.
- Yritysten anonymiteetti ja yrityskohtaisen tiedon luottamuksellisuuden varmistamiseksi tutkimukseen osallistuneiden rakentamisen, tukku- ja vähittäiskaupan sekä rahoitus- ja vakuutustoiminnan toimialoille sijoittuvien yritysten vastaukset yhdistettiin toimialakohtaisessa tarkastelussa ”muut toimialat” nimiseen ryhmään. Kyseiset yritykset olivat tutkimuksessa ainoita toimialaansa edustaneita yrityksiä ja yhdistämisen avulla varmistettiin, ettei yksittäisen yrityksen vastaukset tulleet näkyviin.

- Vastaajien sukupuolijakaumaa ei ole esitetty yritysten tietoihin sidottuna, jotta yrityksiä ja niiden antamia vastauksia ei voi tunnistaa sen mukaan.
- Tutkimuksen tulosaineisto säilytetään sähköisessä muodossa tutkijan hallussa viisi vuotta haastattelututkimuksen toteuttamisajankohdasta lukien.
- Tutkimuksen tulokset ja niihin liittyvät vastaukset on raportoitu totuudenmukaisina ja siinä muodossa kuin haastateltavat ovat ne antaneet.
- Työssä käytetyt lähteet ja niihin liittyvät lähdeviitteet on tuotu raportissa esille opinnäytetyön raportointiohjeen mukaisesti.

7.4 TULOSTEN HYÖDYNTÄMINEN

Tutkimusta suunniteltaessa oli perustuen aikaisempiin keskusteluihin ja tiedonhankintaan olemassa ennakkokäsitys siitä, millainen kyberturvallisuuden taso mikro- ja pk-yrityksillä on. Tutkimus antoi mahdollisuuden syventää käsitystä ja esille uutta tietoa siitä, missä kohdin yrityksissä on pullonkauloja kyberturvallisuuden parantamiseksi. Tutkimus osoitti, että yritysten ja toimialojen välillä on yritysten välillä olemassa suurehkoja eroja ja moni yksittäinen seikka on kontekstisidonnainen. Pienestä otoskoosta huolimatta oli erittäin mielenkiintoista havaita, että kaikissa verrokkitutkimuksissa oli saatu tämän tutkimuksen kanssa samansuuntaisia tuloksia kysymysten ollessa sisällöllisesti lähellä toisiaan. Tämä puoltaa sitä, että tutkimuksesta saadut tulokset ja sitä kautta esille nousseet kehittämistarpeet antavat suuntaviivoja ja sisältöä tutkimuksen kohderyhmään verrattavissa olevien yritysten osaamisen ja toiminnan kehittämistyölle.

Tutkimustyön tuloksia voidaan hyödyntää eri yhteyksissä pk-yritysten kyberturvallisuus tietoisuuden lisäämiseen sekä koulutussisältöjen rakentamiseen vastaaville kohderyhmille. Tuloksia voidaan hyödyntää myös osana kansainvälistä yhteistyötä niissä tilanteissa, joissa on kyse pk-yrityksiin liittyvistä, niiden kyberturvallisuutta edistävistä toimenpiteistä. Kuten kansainvälinen verrokkitutkimus osoittaa, ei Suomi ole yksin tämän asian kanssa, vaan tilanne on muualla Euroopassa ja maailmalla samankaltainen. Ottaen huomioon pk-yritysten rooli osana kansallista ja eurooppalaista kyberturvallisuuden resilienssiä, on meillä kaikilla edessämme haaste, johon tulisi kyetä mahdollisimman pian vastaamaan. Yksi vastauksista on Cyber Scheme Finland -pilottihankkeessa kehitetty FINCSC® –sertifiointikonsepti, jonka pilotointivaiheeseen tämä tutkimus liittyi.

Tutkimustyöni aikana ja erityisesti lähdeaineistoon tutustuessani tuli esille useita tämän tutkimuksen aihepiiriin liittyviä seikkoja, joilla olisi periaatteessa ollut mahdollista laajentaa tätä tutkimusta. Halusin kuitenkin pitää rajauksen alkuperäisen suunnitelman mukaisena, jotta tutkimuksen fokus säilyi.

Yhtenä potentiaalisena jatkotutkimuskohteena olisi selvittää samojen yritysten tilanne nyt, kun on kulunut kaksi vuotta tämän tutkimuksen haastatteluosuuden toteuttamisesta. Suurin osa haastatelluista yrityksistä hankki FINCSC® -perustason sertifikaatin ja näin olisi mahdollista saada vertailevaa tietoa siitä, miten tilanne yrityksissä on kehittynyt tällä aikavälillä ja onko sertifioinnilla mahdollisesti ollut vaikutusta kehitykseen.

Kohdejoukkoa laajentaen olisi myös mielenkiintoista olisi tutkia myös sitä, miten digitalisaatio on edennyt mikro ja pk-yrityskentässä ja millaisena tekijänä yritykset kokevat kyberturvallisuuden osana digitalisoituvaa liiketoimintaa. Tutkimukseen voisi sisällyttää yritysten arvioita potentiaalisista uhkatekijöistä ja niiden mahdollisista vaikutuksesta yrityksen liiketoimintaan. Lisäksi voisi selvittää, millaisia kokemuksia yrityksillä on toteutuneista kyberturvallisuuspoikkeamista, sikäli kun niitä on havaittu. Myös arviot poikkeamien aiheuttamista taloudellisista menetyksistä olisivat kiinnostavia paitsi tutkijalle myös koko yrityskentälle. Loppujen lopuksi tässäkin tapauksessa raha ratkaisee asioiden prioriteetin. Kun jollakin riskitekijällä todetaan olevan riittävät suuri hintalappu, halutaan sen pienentämiseen vasta sitten todella panostaa.

8 LÄHTEET

A brief history of Cyber Essentials. 2017. National Cyber Security Centre (NCSC). www-sivu. Viitattu 11.4.2018.
https://www.cyberessentials.ncsc.gov.uk/2017/11/27/The-NCSC-and-Cyber-Essentials.html

A digital single market in Europe: Bringing down barriers to unlock online opportunities. 2016. European Commission, DG Connect. Viitattu 4.4.2018.
https://publications.europa.eu/en/publication-detail/-/publication/01368318-4e3d-11e6-89bd-01aa75ed71a1/language-en

Aitoa digitaalisuutta vai työsuhdekännyköitä? Tutkimus suomalaisten PK-yritysten digitalisaation asteesta. 2016. Prior Konsultointi Oy. Elisa. Suomen Yrittäjät.
https://materiaalit.elisa.fi/pk-digitalisaatiotutkimus

A New Skills Agenda for Europe. 2016. European Commission. Viitattu 5.4.2018.
http://ec.europa.eu/social/BlobServlet?docId=15621&langId=en

Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–2021 White Paper. 2017. Cisco. Viitattu 7.4.2018.
https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html

Contractual arrangement between the European Union and the European Cyber Security Organisation. 2016. Setting up a Public-Private Partnership in the area of cybersecurity industrial research and innovation. ECSO & European Commission. Viitattu 4.4.2018.

Digital agenda for Europe: Rebooting Europe's economy. 2010. European Commission. Viitattu 4.4.2018.
https://publications.europa.eu/en/publication-detail/-/publication/27a0545e-03bf-425f-8b09-7cef6f0870af/language-en

Euroopan Parlamentin ja Neuvoston Asetus (EU) 2016/679. 2016. Euroopan unionin virallinen lehti. Euroopan Unioni. Viitattu 4.4.2018.
https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Gartner's top 10 Strategic Technology Trends for 2017. 2016. Gartner. www-sivu. Viitattu 4.4.2018.
http://www.gartner.com/smarterwithgartner/gartners-top-10-technology-trends-2017/

Digitaalisesti suuntautuneiden pienten yritysten menestystekijät. 2016. Yrittäjät. Helsinki. Viitattu 9.4.2018.
https://www.yrittajat.fi/sites/default/files/digiselvityksen_raportti2016.pdf

Digitalization. IT Glossary. 2016. Gartner. www-sivu. Viitattu 4.4.2018.

https://www.gartner.com/it-glossary/digitalization/

Hallituksen esitys eduskunnalle liikesalaisuuslaiksi ja eräiksi siihen liittyviksi laeiksi. HE 49/2018. 2018. Valtioneuvosto. Helsinki. Viitattu 19.5.2018. https://www.finlex.fi/fi/esitykset/he/2018/20180049#idp451833168

Hinchcliffe, D. 2014. Is the Internet of Things strategic to the enterprise? Zdnet.2014. Viitattu 7.4.2018. https://www.zdnet.com/article/is-the-internet-of-things-strategic-to-the-enterprise/

Hirsjärvi, S. & Hurme, H. 2009. Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö. Yliopistopaino

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2000. Tutki ja kirjoita. 6. uudistettu painos. Tammi.

Human Capital: Digital inclusion and skills. Europe's Digital Progress Report 2016. 2016. European Commission. Viitattu 5.4.2018 http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=9931

Ilmarinen, V., & Koskela, K.2015. Digitalisaatio, yritysjohdon käsikirja. Talentum. Viitattu 8.4.2018.

Internet of Things Market Statistics – 2015 IoT stats. 2015. Ironpaper. www-sivu. Viitattu 8.4.2018. http://www.ironpaper.com/webintel/articles/internet-things-market-statistics-2015/

ISO/IEC 27032:2012(en). 2012. ISO/IEC. www-sivu. Viitattu 11.4.2018. https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en

JAMK 2016-2010: Jyväskylän ammattikorkeakoulun strategia. 2016. Jyväskylän Ammattikorkeakoulu Oy. Viitattu 23.3.2018.

Katakri 2015 Tietoturvallisuuden auditointityökalu viranomaisille. 2015. Puolustusministeriö. Viitattu 4.4.2018. https://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointity-okalu_viranomaisille.pdf

Keski-Suomen maakunnallinen ICT –strategia. 2013. Keski-Suomen liitto. Viitattu 23.3.2018. https://www.keskisuomi.fi/filebank/24193-ict-strategia2013.pdf

Keski-Suomen maakuntaohjelman toimeenpanosuunnitelma 2015-2016. 2014. Keski-Suomen maakunnan yhteistyöryhmä. Viitattu 23.3.2018.

Klahr, R. Amili, S., Shan, J.N. 2016. Cyber Security Breaches Survey 2016. Main report. HM Government., Ipsos MORI., University of Portsmouth. Viitattu 22.5.2018. https://www.gov.uk/government/publications/cyber-security-breaches-survey-2016

Kyberturvallisuus ja kybertoimintaympäristö. 2014. Ulkoministeriö. www-sivu. Viitattu 11.4.2018.
http://formin.finland.fi/public/Print.aspx?contentid=324279&nodeid=49571&culture=fi-FI&contentlan=1

Lahnalahti, J. 2013. Uusi SFS-ISO/IEC 27001:2013. Esitysmateriaali. Inspecta. Viitattu 4.4.2018.
https://www.sfs.fi/files/4224/27001-julkaisu_2013-12-05_Lahnalahti.pdf

Lakaniemi, I. 2014. Digitalisaatio keskisuurissa yrityksissä.2014. Liikenne- ja viestintäministeriön julkaisuja 14/2014. Liikenne- ja viestintäministeriö. Viitattu 22.2.2018
https://www.lvm.fi/documents/20181/797516/Julkaisuja+14-2014/d9fbe70f-89c4-4504-83bb-c642cacaf40d?version=1.0

Limnéll, J., Majewski, K., Salminen, M. 2014. Kyberturvallisuus. Docendo Oy

Manninen, Brandt, Kallionpää ja Lepola. 2015. Uuskasvun polut – Digitalisaation lupaus. TeliaSonera Finland Oyj.

Meeker, M. 2017. Internet Trends 2017 – Code Conference. Kleiner Perkins. Viitattu 7.4.2018
http://www.kpcb.com/internet-trends

Nevala, J., Aho, J. 2016. Keskisuomalaisten yritysten kyberturvallisuus. Jyväskylä. Oct 2016. Keski-Suomen liitto ja Jyväskylän koulutuskuntayhtymä. Viitattu 22.5.2018.
http://edu360.fi/wp-content/uploads/2016/08/Yrityspuolen_kybertutkimus-FINAL-20160829.pdf

Pk-yritysten toimintaympäristö. Kasvu ja uudistuminen. 2015. Elinkeinoelämän keskusliitto EK. Viitattu 7.4.2018.
https://ek.fi/wp-content/uploads/PKyritysten_toimintaymparisto_kesakuu2015.pdf

Project Cycle Management Guidelines 2004. 2004. European Commission. Viitattu 23.3.2018.
https://ec.europa.eu/europeaid/sites/devco/files/methodology-aid-delivery-methods-project-cycle-management-200403_en_2.pdf

Ratkaisujen Suomi: Puolivälin tarkistus. Hallituksen toimintasuunnitelmavuosille 2017–2019. 2017. Hallituksen julkaisusarja 5/2017. Valtioneuvoston kanslia. Viitattu 1.5.2018
http://vnk.fi/documents/10616/4610410/Toimintasuunnitelma+H_5_2017+280417.pdf

Ratkaisujen Suomi, Pääministeri Juha Sipilän hallituksen strateginen ohjelma. 2015. Hallituksen julkaisusarja 10/2015. Valtioneuvoston kanslia. Edita Prima. Viitattu 1.5.2018
http://valtioneuvosto.fi/documents/10184/1427398/Ratkaisujen+Suomi_FI_YHDISTETTY_netti.pdf

Reform of cyber security in Europe. 2018. European Council. www-sivu. Viitattu 23.3.2018
http://www.consilium.europa.eu/en/policies/cyber-security/

Suomen kyberturvallisuusstrategia. 2013. Turvallisuuskomitean sihteeristö. Viitattu 23.3.2018.
http://puolustusvoimat.fi/documents/2182700/0/Kyberturvallisuusstrategia/bb56d179-9b3a-4816-806d-84c84b04da30

Taanila, A. 2013. Muistilista kyselylomakkeen laatijalle. www-sivu. Viitattu Akin menetelmäblogi. Viitattu 4.4.2018.
https://tilastoapu.wordpress.com/2012/03/22/muistilista-kyselylomakkeen-laatijalle/

Tavoitteena maailman paras verkko. 2018. Elisa. www-sivu. Viitattu 7.4.2018.
https://elisa.fi/verkko/

Tietotekniikan käyttö yrityksissä. 2017. Suomen virallinen tilasto (SVT). Tilastokeskus. Viitattu: 7.4.2018.
http://www.stat.fi/til/icte/index.html

Toimialaluokitus 2008.Tilastokeskus. www-sivu. Viitattu 21.4.2018.
https://www.stat.fi/meta/luokitukset/toimiala/001-2008/index.html

Toiminnan jatkuvuuden hallinta. 2016. Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä - VAHTI 2/2016. Valtiovarainministeriö. Viitattu 25.5.2018.
https://www.vahtiohje.fi/c/document_library/get_file?uuid=11459f91-91c8-4ebe-a34f-9d8d9bfc964c&groupId=10229

Tollefson, J. 2016, Yhteistyöartikkeli: Langattomat IoT-yhteydet tulevat kuluttajalaitteisiin. Blogikirjoitus. Uusi Teknologia –lehti. Viitattu 8.4.2018.
https://www.uusiteknologia.fi/2016/09/06/langattomat-iot-yhteydet-tulevat-kuluttajalaitteisiin/

Yritykset 2016. 2017. Tilastokeskus. www-sivu. Viitattu 23.5.2018
https://www.tilastokeskus.fi/tup/suoluk/suoluk_yritykset.html

Valmiina digikiriin: Digitalisaatio ja virastojen tuottavuuspotentiaali. 2015. Loppuraportti. Valtiokonttori. Viitattu 4.4.2018.
http://www.valtiokonttori.fi/fi-FI/Virastoille_ja_laitoksille/Digitalisaatio/Loppuraportti_Valmiina_digikiriin

Valmiina digikiriin: Virastojen ehdotuksilla uutta tehoa tuottavuuteen – digitalisaation siivittämänä. 2015. Esitysmateriaali. Valtiokonttori. Viitattu 4.4.2018.
http://www.valtiokonttori.fi/download/noname/%7BF1A866F5-A656-426E-BA82-6B2206A1F2A7%7D/92828

Väestön tieto- ja viestintätekniikan käyttö 2017. 2. Internetin käyttö mobiililaitteilla. 2017. Suomen virallinen tilasto (SVT). Tilastokeskus. Viitattu 6.4.2018.

https://www.stat.fi/til/sutivi/2017/13/sutivi_2017_13_2017-11-22_kat_002_fi.html

Yhteiskunnan turvallisuusstrategia. 2010. Valtioneuvoston periaatepäätös. Valtioneuvosto. Viitattu 23.3.2018.
https://www.defmin.fi/files/1696/Yhteiskunnan_turvallisuusstrategia_2010.pdf

von Solms, R., van Niekerk, J. 2013. From information security to cyber security. Computers & Security 38/2013, 97-102. Viitattu 11.4.2018.
https://www.sciencedirect.com/journal/computers-and-security

Yrityksiin kohdistuvat kyberuhat 2016. 2016. Helsingin seudun kauppakamari. Viitattu 24.5.2018.
https://helsinki.chamber.fi/media/filer_public/ae/a7/aea76c12-c030-4769-ae3e-19c479d222b0/yrityksiin_kohdistuvat_kyberuhat_2016_naytto.pdf

Yritys- ja yhteisötietojärjestelmä (YTJ). 2016. Patentti- ja rekisterihallitus. Verohallinto. Viitattu 4.4.2018.
https://www.ytj.fi/index.html

9 LIITTEET

Tutkimushaastattelussa käytetty alkuperäinen kyselylomake vastausasteikkoineen.

HAASTATTELUTUTKIMUS

Aimo Pellinen 8.3.2016

Yrityksen nimi:	
Vastaaja:	
Työtehtävä:	

1. KÄSITTEET JA STRATEGIANÄKÖKULMA	**EI OLE RELEVANTTI (0)**	**EI LAINKAAN (1)**	**HEIKOSTI (2)**	**KOHTALAISESTI (3)**	**HYVIN (4)**	**ERITTÄIN HYVIN (5)**	**LISÄTIETOJA**
Yrityksen johdolle on termin "tietoturvallisuus" merkitys selkeä.							
Yrityksen johdolle on termin "kyberturvallisuus" merkitys selkeä.							
Yrityksen strategiassa on otettu tieto- ja/tai kyberturvallisuus huomioon.							
Yrityksessä on tiedossa, millainen on valmius reagoida mahdolliseen kyberturvallisuuspoikkeamaan.							
Tietoon ja sen käsittelyyn liittyvät riskit ovat merkittäviä yrityksen liiketoiminnan kannalta.							
Yrityksessä on tunnistettu, että liiketoiminnan tavoitteiden saavuttamiseksi tarvitaan strategista informaatioteknologiaan liittyvää suunnittelua.							
Yritykselle on laadittu erillinen IT-strategia.							
Yrityksessä on tunnistettu ja arvioitu tietoon ja sen käsittelyyn liittyvien epävarmuuksien tai epäonnistumisten (uhkien) vaikutuksia liiketoimintaan.							
Yrityksessä on esiintynyt tilanteita, joissa on käytännössä jouduttu arvioimaan kyberturvallisuuteen liittyviä riskejä sekä niiden vaikutuksia							
Kyberturvallisuus ja sen hallinta koetaan yrityksessä uhkatekijänä, josta aiheutuu riskejä ja joka vaikeuttaa ydinliiketoimintaa.							
Kyberturvallisuus koetaan yrityksessä kilpailutekijänä, joka hyvin hallittuna edistää nykyistä ydinliiketoimintaa ja tukee uusia							

KOMMENTTEJA:

2. TIETO JA SEN MERKITYS LIIKETOIMINNALLE (ASSETS)	**EI OLE RELEVANTTI (0)**	**EI LAINKAAN (1)**	**HEIKOSTI (2)**	**KOHTALAISESTI (3)**	**HYVIN (4)**	**ERITTÄIN HYVIN (5)**	**LISÄTIETOJA**
Tieto on tunnistettu osaksi yrityksen omaisuutta.							
Yrityksen liiketoiminnan kannalta kriittinen tieto-omaisuus on määritelty.							
Yrityksessä on määritetty hallinnassa olevan tieto-omaisuuden arvo (sekä taloudellinen että liiketoiminnallinen arvo, hyöty liiketoiminnalle).							
Yrityksen kriittiseen tieto-omaisuuteen sisältyy liiketoiminnan kannalta elintärkeitä sovelluksia. (softa)							
Yrityksen kriittiseen tieto-omaisuuteen sisältyy liiketoiminnan kannalta elintärkeitä järjestelmiä ja tietoverkkoja. (infra)							
Yrityksen kriittiseen tieto-omaisuuteen sisältyy liiketoiminnan kannalta elintärkeätä luottamuksellista tietoa. (data)							
Digitaalisen jatkuvuuden hallinta on tunnistettu strategiseksi tavoitteeksi yrityksessä.							
Digitaalisen jatkuvuuden hallinnan mahdollinen menetys on tunnistettu yrityksen kriittiseksi riskiksi.							
Yrityksessä on määritelty henkilö, joka vastaa digitaalisen jatkuvuuden hallinnasta.							
Yrityksessä on dokumentoitu kyberturvallisuusuhkien varalta palautumissuunnitelma, jolla pyritään varmistamaan digitaalinen jatkuvuus.							
Yrityksessä on selkeä käsitys siitä, miten tieto-omaisuutta tulee hallita (säilyttää, avata, hyödyntää, ymmärtää ja luottaa) nyt ja tulevaisuudessa.							

KOMMENTTEJA:

3. PROSESSIT	EI OLE RELEVANTTI (0)	EI LAINKAAN (1)	HEIKOSTI (2)	KOHTALAISESTI (3)	HYVIN (4)	ERITTÄIN HYVIN (5)	LISÄTIETOJA
Yrityksessä on määritelty ja dokumentoitu turvallisuuteen liittyvät vastuut ja päätösvalta.							
Tiedon omistajuus ja hallinta on määritelty yrityksessä jollekin henkilölle/henkilöille.							
Yrityksen tietojärjestelmistä on saatavissa raportteja, jotka sisältävät liiketoiminnan kannalta käyttökelpoista, ajantasaista ja luotettavaa tietoa.							
Yrityksessä on määritelty ja dokumentoitu, missä ja miten yrityksen liiketoimintakriittistä tietoa säilytetään.							
Yrityksessä on määritelty ja dokumentoitu, miten nimetään ja kuvataan (metadata) tietojärjestelmissä laadittavat ja säilytettävät dokumentit.							
Yrityksen tietojärjestelmiin pääsy on jaoteltu vähintäänkin ns. etuoikeutetun käyttäjän ja tavanomaisen käyttäjän käyttöoikeuksiin.							
Liiketoimintakriittiseen tieto-omaisuuteen pääsyä seurataan ja pääsyyn oikeuttavat tunnukset tietojärjestelmissä vaihdetaan säännöllisesti.							
Yrityksen kaikki ei-julkinen tieto on suojattu niin, että luvaton pääsy siihen käsiksi on estetty.							
Yrityksen langattomiin verkkoihin sisäänpääsyä valvotaan.							
Yrityksessä on määritelty muutoksenhallintakäytänteitä, joilla voidaan estää luvattomien muutosten teko kriittiseen tietoon tai tietojärjestelmiin.							
Yrityksessä seurataan ja arvioidaan tietojenkäsittelyyn liittyviä prosesseja ja niiden tehokkuutta.							
Yrityksen käyttämään informaatioteknologiaan ja -palveluihin liittyvien riskien hallinnalle on tunnistettu olevan tarvetta.							
Yrityksessä on toteutettu kyberturvallisuuden hallintaan liittyviä toimenpiteitä.							
Yrityksessä on politiikka, prosesseja, suunnitelmia tai menetelmiä, jotka auttavat yritystä vastaamaan kyberturvallisuusuhkiin.							
Yrityksessä on pohdittu kyberturvallisuuteen liittyvien riskien pienentämistä vakuutusten avulla.							

KOMMENTTEJA:

4. HENKILÖSTÖN OSAAMINEN	EI OLE RELEVANTTI (0)	EI LAINKAAN (1)	HEIKOSTI (2)	KOHTALAISESTI (3)	HYVIN (4)	ERITTÄIN HYVIN (5)	LISÄTIETOJA
Yrityksen tietojärjestelmistä vastuullisella henkilöllä on riittävät valmiudet ymmärtää vastuullaan olevat riskit ja määritellä hyväksyttävä riskitaso.							
Yrityksessä on määritelty vaatimukset sille, millainen kyvykkyys reagoida kyberturvallisuuspoikkeamaan tulee henkilöstöllä olla.							
Yrityksen henkilöstöä on koulutettu tunnistamaan ja käsittelemään kyberturvallisuuspoikkemia.							
Kaikki yrityksen työntekijät on saatettu tietoisiksi mahdollisista kyberturvallisuusriskeistä, jotka voivat vaikuttaa yrityksen liiketoimintaan.							
Kaikki yrityksen työntekijät on opastettu raportoimaan mahdollisista ja epäilyttävistä kyberturvallisuuspoikkeamista.							
Yrityksessä on käytössä tapoja/menetelmiä/materiaalia, joilla työntekijät saatetaan tietoisiksi kyberturvallisuuteen liittyvistä riskitekijöistä.							
Yrityksen työntekijät ovat saaneet riittävän koulutuksen, jotta he kykenevät kantamaan turvallisuuteen liittyvät vastuunsa.							
Kansantajuista tietoa yleisistä kyberturvallisuuteen liittyvistä ohjeista ja hyvistä käytänteistä on saatavilla yrityksen ulkopuolelta.							

KOMMENTTEJA:

5. FYYSINEN TURVALLISUUS	EI OLE RELEVANTTI (0)	EI LAINKAAN (1)	HEIKOSTI (2)	KOHTALAISESTI (3)	HYVIN (4)	ERITTÄIN HYVIN (5)	LISÄTIETOJA
Fyysinen turvallisuus on jonkun tietyn henkilön vastuulla kaikissa niissä tiloissa, joissa käytetään tai jonne on sijoitettu tietojärjestelmiä.							
Avain tai jokin muu sisäänpääsyyn oikeuttava "väline" tarvitaan kaikkiin niihin tiloihin, joissa tietokoneita, -järjestelmiä tai tallennusvälineitä säilytetään.							
Yrityksen tietojärjestelmät ovat varustettu katkeamattomalla virransyötöllä tai varavoimalaitteella sähkökatkojen varalta.							
Yrityksen kannettavia tietokoneita, tabletteja ja muita kannettavia ATK-laitteita säilytetään turvallisessa paikassa.							
Liiketoimintakriittistä tietoa sisältävät tallennusvälineet säilytetään tarkoitukseen soveltuvissa paloturvallisissa kaapeissa tai tiloissa.							
Ne tilat, joissa tietokoneita, -järjestelmiä tai tallennusvälineitä säilytetään ovat varustettu ajanmukaisin murto- ja palohälytyslaittein.							
Ilman asianmukaisia käyttöoikeuksia olevien henkilöiden pääsy työasemien näyttöpäätteille on estetty.							

KOMMENTTEJA:

YLEISET VAPAAT KOMMENTIT