Jussi Häkkänen

TAPAUSTUTKIMUS TIETOTURVAINVESTOINNEISTA PIENESSÄ KASVUYRITYKSESSÄ

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2020

TIIVISTELMÄ

Häkkänen, Jussi
Tapaustutkimus tietoturvainvestoinneista pienessä kasvuyrityksessä
Jyväskylä: Jyväskylän yliopisto, 2020, 100 s.
Tietojärjestelmätiede, pro gradu -tutkielma
Ohjaaja(t): Niemimaa, Marko

Tutkielmassa selvitetään, miten tietoturvainvestoinnit näkyvät pienessä kasvuyrityksessä ja mikä on yrityksen odotetun kasvun vaikutus yrityksen tietoturvainvestointitarpeisiin. Pieniksi kasvuyrityksiksi luokitellaan startup-yritykset ja kasvuhakuiset pk-yritykset. Tutkielmassa yhdistetään teoria organisaation kasvusta yrityksen tietoturvainvestointitarpeisiin: miten yrityksen johdon näkemys tietoturvainvestointien tarpeesta muuttuu yrityksen kasvaessa? Tutkielman empiirinen osio toteutetaan kvalitatiivisena tapaustutkimuksena. Tuloksissa kuvataan, miten pienessä, voimakkaasti kasvuhakuisessa, suomalaisessa startup-yrityksessä suhtaudutaan tietoturvainvestointeihin. Tuloksista käy ilmi, että yrityksen tietoturvainvestointien ja odotetun kasvun välillä on yhteys. Investointityyppien välillä on eroa; osa tietoturvainvestoinneista koetaan vain isojen organisaatioiden asiaksi ja tarpeelliseksi vasta kun yritys on jo kasvanut huomattavasti suurempaan kokoluokkaan. Tietoturvaan investoidaan sen verran kuin on välttämätöntä, mutta ei ylimääräistä. Tietoturvainvestointien ei koeta tuovan suoraa kilpailuetua. Ensisijaisesti investoidaan kasvua tuoviin asioihin. Tietoturvan pitää olla riittävällä tasolla, mutta jos ei ole mitään pakottavaa syytä investoida resursseja tietoturvaan, muut asiat menevät edelle. Tarve tietoturvainvestoinneille tulee tyypillisesti yrityksen ulkopuolelta: lainsäädännön vaatimukset ja asiakkaan vaatimukset ovat keskeisimpiä syitä tietoturvainvestoinnille. Investointipäätökset tehdään keskustelun kautta ilman erillisiä työkaluja tai viitekehyksiä. Investoinnit pyritään toteuttamaan mahdollisuuksien mukaan ilman rahallisia investointeja, hyödyntämällä esimerkiksi erilaisia vapaasti saatavilla olevia avoimen lähdekoodin ohjelmistoja. Tapausyrityksessä korostui ”tee-se-itse”-lähestymistapa tietoturva-asioihin.

Asiasanat: tietoturvainvestointi, kasvuyritys, startup, kasvuhakuinen pk-yritys

ABSTRACT

Häkkänen, Jussi
Case Study: Information Security Investments in a Small Growth Company
Jyväskylä: University of Jyväskylä, 2020, 100 pp.
Information Systems, Master's Thesis)
Supervisor(s): Niemimaa, Marko

This study aims to clarify how information security investments are considered in a small growth company and how growth affects company's information security investment needs. Small growth companies comprise startup companies and growth focused SMEs. In this work organizational growth theories are coupled with organization's information security investment needs: how does growth affect management's perception of organization's information security investment needs? The empirical part of the study is conducted as a qualitative case study. The case study explores how information security needs are perceived in a small, Finnish, strongly growth-focused startup company. The findings suggest that there is a link between company's information security investments and expected growth. There are differences between investment types; some are considered necessary only in large organizations and others only after meaningful growth. Only essential investments to information security are done, no more. Information security investments are not perceived as a source of direct competitive advantage. Primarily, investments are allocated to sources of growth; company's information security measures need to attain necessary level of protection, however, if there is no mandatory reason to invest in information security, other investments are prioritized. The need for an information security investment generally originates outside the organization: legal requirements and customer demands are the primary reasons to invest in information security. Investment decisions are done based on discussions. Frameworks or tools are not used. Investments without monetary commitment are preferred e.g. by taking advantage of openly available open source software solutions. Homegrown approach to information security topics was emphasized in the case company.

Keywords: information security investment, growth company, startup, growth focused SME

KUVIOT

KUVIO 1 Pienen yrityksen kasvuvaiheet, mukaillen Lewis & Churchill (1983) 19
KUVIO 2 Neljä vaihetta startup-yrityksen elinkaaressa, mukaillen Picken (2017) 22
KUVIO 3 Dynaaminen malli kansainvälisisille markkinoille tähtäävien B2B-yritysten kehitysvaiheista, mukaillen Gabrielsson & Gabrielsson (2013) 25

TAULUKOT

TAULUKKO 1 Pienet kasvuyritykset..... 15
TAULUKKO 2 Tietoturvainvestoinnit akateemisessa tutkimuksessa..... 31
TAULUKKO 3 Turvallisuusriskien hallinnointiprosessi..... 48
TAULUKKO 4 Haastateltavien roolikuvaukset..... 61
TAULUKKO 5 Haastatteluissa esiin nousseita riskejä..... 63
TAULUKKO 6 Tietoturvainvestoinnit suhteessa muihin investointeihin..... 65
TAULUKKO 7 Tapausyrityksen suhtautuminen eri tietoturvainvestointityyppeihin 71

SISÄLLYS

1 JOHDANTO 7

2 PIENET KASVUYRITYKSET 11
2.1 Pienelle kasvuyritykselle tyypillisiä ominaispiirteitä 11
2.1.1 Startup-yritys 12
2.1.2 Kasvuhakuinen pk-yritys 14
2.1.3 Yhteenveto 15
2.2 Kasvuhakuisuus ja kasvuun vaikuttavia tekijöitä 15
2.2.1 Kasvuteoriat 17
2.2.2 Organisaation kasvuvaihemallien kehitys 18
2.2.3 Yhteenveto 25
2.3 Riskienhallinta kasvuyrityksissä 26

3 TIETOTURVAINVESTOINNIT OSANA ORGANISAATION RISKIENHALLINTAA 29
3.1 Keskeisten käsitteiden määritelmät 29
3.2 Tietoturvainvestoinnit 30
3.2.1 Klassiset taloudelliset mallit 33
3.2.2 Käyttäytymistaloustieteeseen perustuvat mallit 36
3.2.3 Vaihtoehtoiset lähestymistavat 37
3.3 Muita tietoturvainvestointeihin vaikuttavia tekijöitä 39
3.4 Tietoturvainvestoinnin haasteet 43
3.5 Erilaisia investointityyppejä 45
3.6 Tietoturvainvestointiprosessi 47
3.7 Yhteenveto 49

4 EMPIIRISEN AINEISTON KERUU JA ANALYYSI 50
4.1 Tutkimusmenetelmä 50
4.2 Datan keräys 54
4.3 Datan analysointi ja luotettavuuden arviointi 57
4.4 Tutkittava tapaus: Yritys Y 59

5 TULOKSET 62
5.1 Riskienhallinta ja tietoturvakulttuuri tapausyrityksessä 62
5.2 Tietoturvainvestoinnit tapausyrityksessä 65
5.3 Yrityksen tietoturvainvestointitarpeiden kehitys yrityksen kasvaessa 71
5.4 Yhteenveto tuloksista 73

6 POHDINTA 75
6.1 Tulosten merkitys 77
6.2 Tutkielman rajoitteet ja jatkotutkimusaiheita 79

7 YHTEENVETO 80

LÄHTEET 81

LIITE 1 HAASTATTELURUNKO 91

LIITE 2 HAASTATTELURUNKO 93

LIITE 3 HAASTATTELURUNKO 95

LIITE 4 TAPAUSYRITYKSEN TOIMINTATAVAT JA YRITYSKULTTUURI 97

1 JOHDANTO

Jopa 16 % pk-yrityksistä (875 000 yritystä) Iso-Britanniassa raportoi joutuneensa kyberhyökkäyksen kohteeksi vuonna 2017[1]. Korkeahkosta luvusta huolimatta lähes puolet yrityksistä (49 %) aikoi investoida alle 1000 puntaa tietoturvaan seuraavan 12 kuukauden aikana. Samanaikaisesti yritysten asiakkaat ovat kuitenkin yhä tietoisempia tietoturvan suhteen, ja ovat kiinnostuneita yhä pienempien yritysten turvallisuuskäytännöistä. Myös Suomessa on edelleen vallalla mielikuva, että yrityksen pieni koko vähentäisi alttiutta kyberrikollisuudelle[2]. Kaikki tietoturvainvestoinnit eivät edellytä suoria rahallisia panostuksia, mutta on todettava, että yritysten turvallisuusympäristö on muuttunut yhä haastavammaksi digitalisaation edetessä. Olisi toivottavaa, että tämä kehitys näkyisi myös pienempien yritysten tietoturvainvestointibudjeteissa. Keskimääräinen kyberhäiriötilanteen hinta pk-yritykselle Iso-Britanniassa oli noin 75 000–311 000 puntaa (Low, 2017). Viime vuosina tietoturvariskit on opittu huomiomaan jo paremmin ainakin monissa suurissa organisaatioissa. Vuonna 2019 Marshin ja Microsoftin[3] toteuttaman kyselyn mukaan kyberriskit olivat nousseet top-5 riskeihin jo lähes 80 % organisaatioista. Tietoturvan sitomisesta yrityksen strategiaan ja päivittäiseen tekemiseen on tullut yhä tärkeämpää, mikä edellyttää, että organisaatiot panostavat siihen resursseja.

Tietoturvainvestointeihin liittyvissä tutkimuksissa on usein kontrolloitu esimerkiksi yrityskokoa ja toimialaa, mutta ei yrityksen kasvuvauhtia. On mm. havaittu, että pienissä yrityksissä usein luotetaan liikaa pienuuden tuomaan virheelliseen turvallisuuden tunteeseen, minkä perusteella erilaiset turvamekanismit saattavat pienissä yrityksissä olla hyvinkin puutteellisia

---

[1] Adams, H & Giff, J (2017, 1.elokuuta). As many as 875,000 UK SMEs suffer cyber security breach in the last 12 months. Haettu 15.10.2020 osoitteesta: https://www.zurich.co.uk/en/about-us/media-centre/general-insurance-news/2017/as-many-as-875000-uk-smes-suffer-cyber-security-breach-in-the-last-12-months

[2] Keränen, M (2018, 6.lokakuuta). Tietoturva-asiantuntija suomalaisyrityksistä: Vallalla on väärä mielikuva, että yrityksen pieni koko vähentäisi alttiutta kyberrikollisuudelle. Haettu 15.10.2020 osoitteesta: https://www.tekniikkatalous.fi/uutiset/tietoturva-asiantuntija-suomalaisyrityksista-vallalla-on-vaara-mielikuva-etta-yrityksen-pieni-koko-vahentaisi-alttiutta-kyberrikollisuudelle/b2d74dd9-8c2b-3850-b56d-4ad5f66415e9

[3] Marsh & Microsoft (2019, syyskuu). 2019 Global Cyber Risk Perception Survey. Haettu 15.10.2020 osoitteesta: https://www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf

(Kotulic & Clark, 2004; Ng & Feng, 2006). Vaikka yrityksen johto tiedostaisi riskit kohtuullisen hyvin, tietoturvaperiaatteita on silti saatettu implementoida hyvin vähän käytäntöön (Bradbard, Norris & Kahai, 1990). Aikaisemmissa tutkimuksissa korostuvat erilaiset kvantitatiiviset mallit tietoturvainvestointien taloudelliseen optimointiin (mm. Gordon & Loeb, 2002). Kvantitatiiviset menetelmät ovat edelleen suosittuja, mutta näissä malleissa on kuitenkin usein puutteita reaalimaailman soveltamisen kannalta (Heidt ym., 2019). Useiden mallien ongelmana on, että ne jättävät suurelta osin huomiotta erilaiset kontekstisidonnaiset tekijät (Heidt ym., 2019). Viime vuosina tietoturvainvestointien tutkimuksen näkökulma on laajentunut. Yhä enemmän on alettu tutkia erilaisia investointipäätökseen vaikuttavia taustatekijöitä: Organisatorinen tutkimus (mm. Dor & Elovici, 2016), käyttäytymistaloustiede (mm. Beebe, 2014) ja myös neurotiede (mm. heuristiikat ja harhat; Cavusoglu, 2010) on tuotu mukaan tutkimukseen.

Yritysten kasvun dynamiikka (mm. Penrose, 1959) puolestaan on kiinnittänyt tutkijoiden huomion jo kauan ennen ensimmäistäkään tutkimusta tietoturvainvestointeihin liittyen. Pienten kasvavien yritysten merkitys koko kansantalouden kannalta on ollut jo pitkään tiedossa, sillä nopeasti kasvavat yritykset luovat paljon työpaikkoja ja ovat tärkeitä kansantalouden tuottavuuden kannalta (Anyadike-Danes ym., 2009; Littunen & Tohmo, 2003). Nopeasti kasvavat yritykset nähdään harvinaisina ja arvokkaana ilmiönä, ja siksi tutkimuksen arvoisina (Levie & Lichtenstein, 2010). Tässä tutkielmassa yhdistetään nämä kaksi tutkimusaluetta: yrityksen kasvu ja yrityksen tietoturvainvestoinnit. Tutkimuskysymykset ovat muotoiltu seuraavasti:

Miten pienen kasvuyrityksen tietoturvainvestointitarve muuttuu yrityksen kasvaessa?
Miten tietoturvainvestointitarpeita arvioidaan suhteessa kasvuun pienissä kasvuyrityksissä?

Tutkielmassa selvitetään yrityksen tietoturvainvestointien ja organisaation kasvun välistä dynamiikkaa: miten yrityksen johdon näkemys tietoturvainvestointien tarpeesta muuttuu yrityksen kasvaessa ja olosuhteiden muuttuessa? Proaktiivinen lähestymistapa on useissa tutkimuksissa todettu parhaaksi tavaksi lähestyä tietoturvaa, mutta toteutuuko se käytännössä? Nähdäänkö tietoturvainvestoinnit pienissä kasvuyrityksissä ylimääräisenä hidasteena vai enemminkin kasvun mahdollistajana?

Pienissä kasvuhakuisissa yrityksissä korostuu resurssien rajallisuus (Huovinen, 2018). Rajallisista resursseista (työvoima, raha, osaaminen jne.) kilpailee monta asiaa. Tietoturvainvestoinnit eivät tyypillisesti tuo suoraa kasvua, saati tuottoa, joten on kiinnostavaa selvittää, miten ilmiö näkyy yrityksen suhtautumisessa tietoturvainvestointeihin. Käytetäänkö pienissä kasvuyrityksissä resursseja tietoturvan kehittämiseen vain pakon edessä? Yritys, joka on menestynyt hyvin, mutta ei ole investoinut riittävällä tasolla tietoturvaan, ottaa suuren riskin (Kort ym., 1999). Pieni kasvuyritys ei voi mitenkään välttyä moniltakaan riskeiltä, mutta voimakas kasvuhakuisuus ja nopea kasvu lisäävät riskejä myös tietoturvan osalta, jos perusta ei ole kunnossa:

uudet toimipisteet, kasvava määrä työntekijöitä, näkyvyyden lisääntyminen (houkuttelee myös rikollisia tuoton perässä) jne. vain muutamia riskejä mainitakseni. Moni tunnettu kasvuyritys Uberista[4] lähtien on ollut otsikoissa erinäisten tietoturvaongelmien ja tietovuotojen vuoksi. Seuraukset voivat olla pahimmillaan katastrofaalisia (vrt. Vastaamo[5]), jos asiaan ei kiinnitetä riittävästi huomiota. Lisäksi mahdollinen epäorgaaninen kasvu (yritysostot ja fuusiot ym.) tuovat omat haasteensa tietoturva-asioiden kannalta.

Yrityksen kasvaessa sen haasteena on säilyttää siedettävän riskitason tasapaino. Riskitaso voi ajan myötä kasvaa yli siedettävän tason, jos yritys ei investoi tietoturva-asioihin. Turvallisuusinvestoinnin tuotto muodostuu laskeneesta riskitasosta (Arora ym., 2004). Useat investointimallit (mm. Sonnenreich ym., 2006; Fenz ym., 2011; Arora ym., 2004) hyödyntävät tätä lähestymistapaa optimaalisen investointitason määrittämiseen. Yritysjohto investoi todennäköisemmin tietoturvaan, mikäli sillä on hyvä ymmärrys yrityksen tietoturvainvestointitarpeista ja olemassa olevat toimivat riskienhallintaproseduurit (Cavusoglu ym., 2015). Investoinnit tietoturvaan voidaan nähdä myös mahdollisena kilpailuetuna nuorempien yritysten keskuudessa (investointi tietoturvaan voi esimerkiksi vaikuttaa positiivisesti asiakasuskollisuuteen ja asiakashankintaan) (Heidt ym., 2019). Tätä näkökulmaa ei juuri käsitellä tietoturvainvestointeja koskevassa tutkimuskirjallisuudessa.

Tutkielman empiirinen osio toteutettiin kvalitatiivisena tapaustutkimuksena. Tapaustutkimuksen tarkoituksena oli tuoda käytännön näkemystä siihen, miten pienessä, voimakkaasti kasvuhakuisessa, suomalaisessa startup-yrityksessä suhtauduttiin tietoturvainvestointeihin.

Tapaustutkimuksen tulokset osoittavat, että yrityksen tietoturvainvestointitarpeiden ja kasvuodotusten välillä on yhteys. Pakottavat ja välttämättömät tietoturvainvestoinnit hoidettiin viipymättä, mutta vapaaehtoiset investoinnit jäivät investointien priorisoinnissa muiden investointien taakse. Ensisijaisesti investoitiin kasvua tuoviin asioihin.

Tutkielma etenee seuraavasti: Alussa määritellään, mitä pienillä kasvuyrityksillä tarkoitetaan tämän tutkielman yhteydessä ja käsitellään pienten kasvuyritysten ominaispiirteitä, kasvuhakuisuutta ja riskienhallintaa. Luku esittelee myös aikaisempaa tutkimusta ja teorioita yritysten kasvusta. Kolmas luku käsittelee tietoturvainvestointeja osana organisaatioiden riskienhallintaa. Luvussa esitellään tietoturvainvestointeihin liittyviä aikaisempia tutkimuksia, investointimalleja, haasteita, päätöksentekoon vaikuttavia tekijöitä, erilaisia tietoturvainvestointityyppejä ja investointiprosessia. Neljännessä luvussa kerrotaan, miten tutkielman empiirinen osio on toteutettu. Luku sisältää myös lyhyen esittelyn tutkimuksen kohteeksi valitusta tapausyrityksestä. Viides luku esittelee tapaustutkimuksen tulokset. Kuudennessa luvussa pohditaan, mitä

---

[4] Hern, A. (2018, 27.marraskuuta). Uber fined £385,000 for data breach affecting millions of passengers. Haettu 15.10.2020 osoitteesta: https://www.theguardian.com/technology/2018/nov/27/uber-fined-385000-for-data-breach-affecting-millions-of-passengers-hacked

[5] Niskakangas, T. (2020, 25.marraskuuta). HS selvitti Vastaamon taloustiedot: Psykoterapiakeskus kasvoi vauhdilla ja yritti pitää tietoturva-asiat mukana kehityksessä. Haettu 25.10.2020 osoitteesta: https://www.hs.fi/talous/art-2000006699158.html

tuloksista voidaan oppia ja mitä tutkielmassa jäi käsittelemättä. Seitsemäs luku sisältää lyhyen yhteenvedon.

2 PIENET KASVUYRITYKSET

Luvussa käsitellään pienten kasvuyritysten riskienhallintaa ja kasvuyrityksille tyypillisiä ominaispiirteitä. Luvussa määritellään termit startup ja kasvuhakuinen pk-yritys, jotka luokitellaan tämän tutkielman yhteydessä pieniksi kasvuyrityksiksi. Kasvuhakuiset yritykset ovat usein melko nuoria, matalasti hierarkkisia, vahvasti kansainvälisiä markkinoita hakevia, tyypillisesti osaamisintensiivisten palvelujen tai teollisuuden yrityksiä, joilla on usein melko kunnianhimoiset liikevaihdon kasvutavoitteet.

2.1 Pienelle kasvuyritykselle tyypillisiä ominaispiirteitä

Kasvuyritys ei ole tieteellisessä kirjallisuudessa kovinkaan vakiintunut termi, vaan määritelmiä on useita. Merriam-Webster sanakirja määrittelee kasvuyrityksen yrityksenä, joka kasvaa nopeammin kuin ympäröivä talous, ja joka sijoittaa suuren osan tuloistaan takaisin omaan liiketoimintaansa. Tyypillisiä muuttujia, joilla kasvuyrityksiä luokitellaan ovat esimerkiksi liikevaihdon kasvuprosentti ja työntekijöiden määrän kasvu. Yritys voi kasvaa orgaanisesti (yrityksen liiketoiminta kasvaa pohjautuen sen omiin resursseihin ja sisäisiin prosesseihin) tai epäorgaanisesti (yrityksen kasvu on ulkoista kasvua, esimerkiksi fuusion tai yritysoston muodossa). Kasvuyritykset ovat merkittäviä työllistäjiä kansantaloudessa (Anyadike-Danes, Bonner, Hart, & Mason, 2009; Barringer, Jones, & Neubaum, 2005; Parker, Storey, & Van Witteloostuijn, 2010; Littunen & Tohmo, 2003) ja niillä on siten suuri merkitys kansantalouden kannalta monissa maissa. Työpaikkojen luonti on nopeaa kovan kasvun yrityksissä (Smallbone ym., 1995). Nopeasti kasvavat yritykset kasvattavat työntekijämäärän ohella myös työn tuottavuutta (Littunen & Tohmo, 2003; Smallbone, Leig & North, 1995). Staattisesti tarkasteltuna, eli tiettynä ajankohtana, suuret ja vanhat yritykset ovat keskeisessä roolissa työllisyyden ja arvonlisäyksen kannalta. Dynaamisesti eli yli ajan tarkasteltaessa havaitaan, että nettona työpaikkoja syntyy voittopuolisesti kasvaviin nuorempiin yrityksiin, joiden lähtökoko on usein vaatimaton. (Kotiranta, Pajarinen & Rouvinen, 2016.)

Kasvuyritykset keräävät usein paljon mediahuomiota, etenkin jos ala on uusi ja trendikäs. Monet tunnetuista kasvuyrityksistä henkilöityvät usein ainakin alussa karismaattisen toimitusjohtajan ympärille. Kasvuyrityksistä erityisesti startupeille on tyypillistä yrittäjähenkisyys ja innovatiivisuus. Suurinta mediahuomiota nauttivien kasvuyritysten joukko on kuitenkin suhteellisen pieni, ja se saattaa luoda hieman vääristyneen kuvan koko joukosta. (Kotiranta ym., 2016.) Vaihtelevan kokoiset ja vaihtelevan ikäiset yritykset eri sektoreilla voivat saavuttaa kovan kasvun. Kovan kasvun yritykset erottaa muista yrityksistä enemmän yritysten strategia ja johdon toimet kuin yritysten profiili. (Smallbone ym., 1995.)

Pienemmän kokoluokan kasvuyritykset ovat joko startup-yrityksiä tai kasvuhakuisia pk-yrityksiä. Tämän tutkielman yhteydessä pienistä kasvuyrityksistä puhuttaessa viitataan sekä startup-yrityksiin että kasvuhakuisiin pk-yrityksiin.

2.1.1 Startup-yritys

Luger & Koo (2005) käyttävät startup-yrityksen määritelmään kolmea eri kriteeriä: uusi, aktiivinen ja itsenäinen. *Uudella* tarkoitetaan sitä, että yritys on vasta äskettäin perustettu, ja se on aloittamassa liiketoimintaansa ensimmäistä kertaa. Esimerkiksi nimeään vaihtavaa, kymmenen vuotta sitten perustettua, pizzeriaa ei siis luokitella uudeksi startup-yritykseksi, jos liiketoimintamalli, yrittäjä ja henkilöstö pysyy pitkälti samana. *Aktiivisuudella* viitataan siihen, että yrityksellä on oltava aktiivista liiketoimintaa, jotta sitä voidaan pitää startup-yhtiönä. Esimerkiksi verosuunnittelua tai vastaavaa tarkoitusta varten rekisteröityjä passiivisia pöytälaatikkoyhtiöitä ei siis lasketa startup-yritysten joukkoon, vaikka ne olisivat uusia. Kolmas kriteeri, *itsenäisyys*, edellyttää, että yritys on uusi itsenäinen toimija. Se ei siis voi olla esimerkiksi jonkin jo toimivan organisaation tytäryhtiö tai haarakonttori. Kotiranta, Pajarinen ja Rouvinen (2016) määrittelevät Etlan tutkimusraportissa suomalaisen startupin peruskriteerit seuraavasti: ”Muodostamamme julkisiin rekisteritietoihin pohjautuvan startup-vuosikerran määritelmän peruskriteerit ovat, että yrityksen on oltava nuori, pienehkö, itsenäinen ja kasvun perusedellytykset omaava”.

- *Ikä* (yrityksen vanhimman toimipaikan ikä on korkeintaan viisi vuotta)
- *Koko* (yritys on pieni; vähintään 1 työntekijä, korkeintaan 49 työntekijää)
- *Kasvun perusedellytykset olemassa* (yritys on ilmoittanut itsensä työnantajarekisteriin ja yhtiömuoto on osakeyhtiö)
- *Omistussuhde* (yritys on itsenäinen, yksityinen ja suomalaisessa omistuksessa)

Mikä erottaa startupin tavallisesta pk-yrityksestä? Startupit tähtäävät määritelmän mukaisesti lähtökohtaisesti (vahvaan) kasvuun, toisin kuin kaikki pk-yritykset (Kollmann ym., 2016). Moni esimerkiksi toiminimen kautta perustetun pk-yrityksen omistaja on tyytyväinen yrityksensä nykytilaan, eikä pyri kasvattamaan yrityksensä kokoa (Levie & Lichtenstein, 2010). Kasvumotivaatio on määritelmän kannalta olennainen asia, sillä yrittäjien kasvumotivaatiolla on vahvistettu olevan suuri merkitys myös yrityksen reaalisen kasvun suhteen (Delmar & Wiklund, 2008).

Yrityksen liiketoiminnalla on myös merkitystä sen suhteen, lasketaanko yritys startupiksi vai ei. Startup-yrityksen määritelmään liitetään usein nopean kasvun ohella myös innovatiivisuus (Kollmann ym., 2016). Innovatiivisuus liittyy usein korkean teknologian yrityksiin tai jotenkin poikkeukselliseen liiketoimintamalliin. Suomessa kaikista startupeista noin kolmannes toimii tietointensiivisissä palveluissa ja kasvavien startupien joukossa on suhteessa

kaikkiin startupeihin selvästi enemmän tietointensiivisten palveluiden sekä rakennusalan yrityksiä (Kotiranta ym., 2016). Suomalaiset startup-yritykset olivat vuonna 2016 Euroopan komission rahoittaman raportin mukaan Euroopan vanhimpia, keskimäärin noin 3,4 vuoden ikäisiä (Kollmann ym., 2016).

Startup-yhtiöihin moni liittää olennaisesti myös pääomasijoittajat. Tämä on osin virheellinen käsitys. Moni startup-yritys on perustettu innovatiivisen idean ympärille, joten on tavallista, että yritys vasta kehittää ensimmäistä tuotettaan eikä tuota vielä voittoa. Kaikista yleisin rahoituksen muoto on usein omistajien säästöt, jonka jälkeen tulevat perhe ja ystävät (Kollmann ym., 2016). Vain pienellä osalla startup-yrityksistä on ulkopuolinen pääomasijoittaja. Kotiranta ym., (2016) toteavat, että pääomasijoitukset ja julkinen innovaatiorahoitus kohdistuvat vain hyvin marginaaliseen joukkoon startupeista Suomessa: Pääomasijoituksia saa vuosikerrasta riippuen 0,4–1,1 % ja Tekesin (Nyk. Business Finland) innovaatiorahoitusta 3–4 % kaikista startupeista. Business Finlandin määritelmässä startup-yritykset ovat alle 5-vuotiaita yrityksiä. Mielikuva pääomasijoittajien rahoituksella pyörivistä startupeista on monelle syntynyt median kautta. Kansainvälisesti tunnettuja esimerkkejä startup-yhtiöinä aloittaneista kasvuyrityksistä ovat esimerkiksi kyydinvälityspalveluna aloittanut Uber ja majoitusliiketoimintaan erikoistunut Airbnb. Uber lähti (perustamisvuosi 2009) kilpailemaan kyydinvälitykseen. Airbnb (perustamisvuosi 2008) lähti kilpailemaan majoitusbisnekseen. Molemmat ovat kasvaneet todella suuriksi organisaatioiksi. Liiketoiminnassa ei ole sinänsä mitään uutta, vaan molemmat tarjoavat perinteisiä palveluja. Uutta oli teknologia ja liiketoimintamalli. Tämä on monen startup-yrityksen lähtökohta. On tosin syytä huomioida, että vain äärimmäisen harva yritys koskaan kasvaa vastaavaan kokoluokkaan, ja siksi näihin yrityksiin viitataankin termillä yksisarvinen. Yksisarvinen tarkoittaa yritystä, joka on saavuttanut (tai voi saavuttaa) yli miljardin dollarin markkina-arvon alle kymmenessä vuodessa. (Kotiranta ym., 2016.) Osa startupeista ostetaan pois jo aiemmin suuremman organisaation toimesta, tai niin kuin suurelle osalle yrityksistä käy, liiketoiminta ei lähde odotetusti käyntiin ja yritys ajautuu konkurssiin tai lopetetaan. Yksisarvisia (kuten Airbnb ja Uber) realistisimmissa startup-keskusteluissa viitataan pääomasijoittajien kohdeyrityksiin tai sellaiseksi mieliviin, mutta kuten todettua, tällöinkin puhutaan varsin pienestä joukosta yrityksiä (Kotiranta ym., 2016).

Startup-yritykset toimivat monelta osin omassa maailmassaan verrattuna jo vakiintuneisiin organisaatioihin. Niiden toimintatavat ovat usein vasta kehittymässä ja ne ovat hyvin yrittäjäkeskeisiä (Kotiranta ym., 2016). Startup-yritykset toimivat riskien ja epävarmuuden täyttämässä ympäristössä, mutta yrittäjillä on usein vaikeuksia tunnistaa kaikkia suorituskykyyn vaikuttavia tekijöitä (Sommer, Loch & Dong, 2019). Liiketoiminta vie monesti alussa enemmän rahaa kuin tuo sisään, etenkin aggressiivisen kasvustrategian valinneissa yrityksissä. Gage (2012) toteaa, että jopa 75 % startupeista Yhdysvalloissa epäonnistuu. Kun valitaan tarkasteluun kymmenen satunnaisesti valittua startup-yritystä, niin joukosta kolmesta neljään yritystä epäonnistuu

täysin, toiset kolmesta neljään yritystä palauttavat alkuperäisen investoinnin, ja vain yksi tai kaksi yrityksistä tuottaa merkittäviä tuottoja. Noin 60 % startup-yrityksistä Yhdysvalloissa selviää vähintään kolme vuotta, mutta vain noin 35 % startupeista jatkaa toimintaansa vielä 10 vuoden jälkeen (Gage, 2012). Suomessa luvut ovat samankaltaisia kuin Gagen artikkelissa. VTT:n tutkimusraportin mukaan yli puolet uusista yrityksistä Suomessa lopettaa toimintansa ensimmäisen viiden vuoden aikana (Kupi, Keränen & Lanne, 2009). Tosin Kotirannan ym., (2016) määritelmän täyttävistä startup-yrityksistä jopa noin 70 % säilyy elossa vähintään viiden vuoden ajan ja tänä aikana niiden työntekijämäärä on keskimäärin kaksinkertaistunut. Kasvukriteerin täyttävissä startupeissa (6–7 % startupeista) työntekijöiden määrä on viiden vuoden kuluttua keskimäärin viisi kertaa suurempi kuin lähtötilanteessa. (Kotiranta ym., 2016.) Kasvukriteerin täyttäviksi startupeiksi määriteltiin tutkimuksessa startupit, jotka työllistivät kolmen vuoden päästä alkuhetkestä vähintään 10 henkilöä, ja joiden työllisyyden kasvu vuositasolla oli vähintään 20 %.

2.1.2 Kasvuhakuinen pk-yritys

Toinen kasvuyritysten alaluokka on kasvuhakuiset pk-yritykset. Tilastokeskus määrittelee pienet ja keskisuuret yritykset (pk-yritykset) yrityksiksi, joiden palveluksessa on vähemmän kuin 250 työntekijää, joiden vuosiliikevaihto on enintään 50 miljoonaa euroa tai taseen loppusumma enintään 43 miljoonaa euroa, ja jotka täyttävät perusteen riippumattomuudesta. Riippumattomia yrityksiä ovat ne yritykset, joiden pääomasta tai äänivaltaisista osakkeista 25 prosenttia tai enemmän ei ole yhden sellaisen yrityksen omistuksessa tai sellaisten yritysten yhteisomistuksessa, joihin ei voida soveltaa tilanteen mukaan joko pk-yrityksen tai pienen yrityksen määritelmää. (Kupi, Keränen & Lanne, 2009.)

Pizzeriaa tai kampaamoa ei perinteisesti lasketa startup-yritysten joukkoon, vaikka niillä olisi suuri kasvumotivaatio. Parempi termi kuvaamaan näitä perinteisten toimialojen kasvuun tähtääviä yrityksiä on kasvuhakuinen pk-yritys. Kasvuhakuinen pk-yritys voi olla perustettu jo kauan aikaa sitten (yrityksen ei tarvitse olla uusi). Kasvuhakuisuus on voinut syntyä yrityksessä myöhemmin esimerkiksi uuden johdon, innovaation tai uuden toimialan valloituksen myötä. Yritykset, jotka ovat perustettu turvaamaan yrittäjän toimeentulo ilman merkittävää kasvuhakuisuutta, ovat tavallisia pk-yrityksiä. (Kollmann ym., 2016.)

Rikama (2016) tutki työ- ja elinkeinoministeriön raportissa voimakkaasti kasvuhakuisia pk-yrityksiä Suomessa. Kasvuhakuiset pk-yritykset olivat kaikilla mittareilla keskiverto pk-yritystä vahvemmin uusiutuvia. Ne ovat innokkaampia laajentumaan uusille markkinoille, lanseeraamaan uusia tuotteita ja ottavat ketterämmin käyttöön uutta teknologiaa ja liiketoimintamalleja. Kasvuhakuisilla yrityksillä on tyypillisesti tähtäimessä jo lähtökohtaisesti laajemmat valtakunnalliset ja kansainväliset markkinat, ja ne operoivat etenkin kansainvälisillä markkinoilla huomattavasti muita pk-yrityksiä yleisemmin.

(Rikama, 2016.) Kasvuhakuisiksi yrityksiksi määriteltiin yhtiöt, joiden edustajat identifioivat yrityksen itse kasvuhakuiseksi yritykseksi (vaihtoehtoina oli valita joko kasvuhakuinen tai voimakkaasti kasvuhakuinen yritys tai jokin ei kasvuun suuntautuneista vaihtoehdoista.) Seuraavat erityispiirteet nousivat Rikaman (2016) raportissa esiin: voimakkaasti kasvuhakuisten yritysten määrä on rajallinen, sillä ne kattavat vain noin 8 % pk-yrityksistä Suomessa. Yleisimmin kasvuyrityksiä on osaamisintensiivisissä palveluissa. Kasvuhakuiset pk-yritykset ovat tyypillisesti nuoria ja moni niistä panostaa digitaalisuuteen.

2.1.3 Yhteenveto

Yhteenvetona, pienellä kasvuyrityksellä voidaan tarkoittaa sekä startup-yrityksiä että kasvuhakuisia pk-yrityksiä. Pienet kasvuyritykset ovat yrittäjäkeskeisiä, nuoria ja (voimakkaasti) kasvuhakuisia. Ne ovat innokkaita laajentumaan uusille markkinoille ja lanseeraamaan uusia tuotteita. Pienet kasvuyritykset tähtäävät jo lähtökohtaisesti suurempaan kokoluokkaan ja ne ottavat ketterästi käyttöön uutta teknologiaa ja uusia liiketoimintamalleja. Pienet kasvuyritykset ovat usein pidemmällä digitalisaatiossa kuin vähemmän kasvuhakuiset pk-yritykset. Taulukko 1 havainnollistaa startup-yrityksen ja kasvuhakuisen pk-yrityksen määritelmiä. Seuraava luku käsittelee yritysten kasvuhakuisuutta ja menestyksekkään kasvun kannalta merkittäviä tekijöitä.

TAULUKKO 1 Pienet kasvuyritykset

	Startup	**Kasvuhakuinen pk-yritys**
Yrityksen ikä	1–10 vuotta	Vaihtelee, ei ylärajaa
Henkilöstömäärä	~ 12 (Kollmann ym., 2016)	Yli 20 (Rikama, 2016)
Innovatiivisuus (teknologia, liiketoimintamalli)	Tyypillisesti erittäin innovaatiokeskeisiä	Keskimääräistä pk-yritystä innovaatiokeskeisempiä
Kasvuhakuisuus	Keskeisessä roolissa, investoi kasvuun	Keskeisessä roolissa, investoi kasvuun

2.2 Kasvuhakuisuus ja kasvuun vaikuttavia tekijöitä

Tämä luku käsittelee yrityksen kasvuhakuisuutta ja kasvuun vaikuttavia tekijöitä. Luvussa esitellään lyhyesti, miten teoriat organisaation kasvusta ovat kehittyneet klassisista kasvuteorioista nykypäivän moderneihin kasvuteorioihin. Kuvailussa keskitytään erityisesti erilaisiin kasvuvaihemalleihin, muihin kasvuteorioihin viitataan vain lyhyesti.

Yrityksen kasvu on tyypillisesti katkonainen prosessi (Smallbone, Leig & North, 1995). Kasvusta on kuitenkin mahdollista tunnistaa erilaisia vaiheita ja kasvuun vaikuttavia tekijöitä. Storey (2016) tunnistaa kolme keskeistä pienen yrityksen kasvuun liittyvää tekijää: 1. yrittäjän alkuresurssit, 2. yrityksen

ominaispiirteet, 3. valittu kasvustrategia. Littunen ja Tohmo (2003) erottelevat seuraavat tekijät, joilla on vaikutusta yrityksen kasvuun: Yritystä perustettaessa tärkeitä sisäisiä tekijöitä ovat etenkin yrittäjän osaaminen, tietotaito, kompetenssi ja sisäinen motivaatio. Myös ulkoisilla tekijöillä, kuten erilaisilla veto-työntö-tekijöillä (kannustimet ja vaatimukset ym.), tilannesidonnaisilla tekijöillä, ympäristöllä ja yrityksen tuottaman tuotannon / palvelun rakenteella on vaikutusta.

Vetotekijöillä viitataan erilaisiin positiivisiin tekijöihin, jotka saavat yrittäjän aloittamaan liiketoiminnan – yritystoiminta voi olla esimerkiksi yrittäjän intohimo, yrittäjä on motivoitunut työllistämään itse itsensä tai yrittäjä tunnistaa houkuttelevan markkinatilaisuuden jne. Työntötekijöillä taas viitataan tilanteeseen, jossa yrittäjällä on jokseenkin kielteinen suhtautuminen yritystoimintaan – yrittäjä on voinut aloittaa yritystoiminnan esimerkiksi muiden vaihtoehtojen puuttuessa tai työttömyyden pelon ajamana. Nopeasti kasvavien yritysten joukossa korostuvat positiiviset vetotekijät, jotka ovat saaneet yrittäjän aloittamaan liiketoiminnan. (Littunen & Tohmo, 2003.)

Tilannesidonnaisilla tekijöillä Littunen ja Tohmo (2003) tarkoittavat erilaisia asioita, jotka ovat hyvin yrityskohtaisia, kuten yrittäjän osaaminen ja luonteenpiirteet, yrityksen johtamistapa, liiketoimintamallin (idean) toimivuus, tehokas yhteistyökumppaniverkosto, yrityksen strategiset valinnat, rahoitusjärjestelyt jne. Useat teoriat organisaation kasvusta ja kestävän kilpailuedun saavuttamisesta korostavat näitä tilannesidonnaisia tekijöitä, mm. yrityksen johtamistavan joustavuuden ja mukautumisen tärkeyttä. Resurssiperustainen näkökulma (RBV, mm. Barney, 2001) korostaa yrityksen sisäisten resurssien merkitystä kilpailuedun kannalta, Penrose (1959) puhuu yrityksen kyvyistä yhdistellä sen resursseja kilpailuedun saavuttamiseksi. Dynaamisten kyvykkyyksien teoria (Eisenhardt & Martin, 2000) ammentaa aikaisemmista teorioista ja näkee dynaamiset kyvykkyydet prosesseina, jotka liittyvät yritysten kykyyn uudistaa resurssejaan ja kyvykkyyksiään, niin että ne pystyvät paremmin vastaamaan liiketoimintaympäristönsä muutoksiin. Teorioista löytyy myös empiiristä tutkimusta. Smallbone ym., (1995) tutkimuksessa yli 10 vuotta onnistuneesti kasvaneilta yrityksiltä vaadittiin sisäisen organisaatiorakenteen mukauttamista. Esimerkiksi delegointi oli keskeisessä roolissa; johtajien piti osata delegoida operatiivisia tehtäviä voidakseen keskittyä enemmän strategiapuoleen.

Yrityksen paikallisympäristön ominaispiirteillä on myös merkitystä: Aloittavan yrityksen menestymisen kannalta on edullista, jos ympärillä on paljon pieniä yrityksiä, saatavilla on korkeasti koulutettua työvoimaa ja alueella on aktiivista liiketoimintaa. (Littunen & Tohmo, 2003.)

Yrityksen ominaispiirteillä Storey (2016) tarkoittaa asioita, kuten yrittäjän osaaminen ja osaamisen kehitys, yrityksen sijainti, yrityksen tuotteiden / palveluiden luonne ja yrityksen strategiset valinnat. Yrityksen strategiset valinnat voidaan määritellä keinovalikoimana, jolla yritys pyrkii saavuttamaan asettamansa tavoitteet. Strategisiin valintoihin kuuluvat mm. liiketoimintasuunnitelma, yrityksen positio markkinalla, tulevaisuuden visio,

yrityksen reagointikyky, verkostoituminen, liikesuhteiden luonti jne. Nopeasti kasvavat yritykset investoivat keskimääräistä enemmän ja ne ovat ketteriä mukauttamaan strategiaansa markkinaympäristöön sopivaksi (Smallbone ym., 1995). Myös yrityksen digitalisaatiolla on yhteys yrityksen kasvuun. Moderneja digitaalisia työkaluja käyttävillä yrityksillä on keskimäärin positiivisemmat odotukset tulevaisuuden suhteen (Larja & Räisänen, 2019).

2.2.1 Kasvuteoriat

Yritysten kestävä kasvu on arvonluonnin ja työpaikkojen luonnin kannalta elintärkeää. Yritysten perustajat kohtaavat haasteen kasvuun liittyvien muutosten edessä: Organisaatioiden siirtyessä kasvuvaiheesta toiseen niiden ongelmat muuttavat muotoaan. Näin ollen yrityksissä tarvitaan erilaisia johtamistaitoja, priorisointia ja rakenteellisia muutoksia. (Hanks ym., 1994.) Erilaiset organisaatioiden kasvuteoriat pyrkivät havainnollistamaan näitä ongelmia, joita kasvavat yritykset kohtaavat. Erilaiset kasvuvaihemallit olivat säännöllisesti hyödynnetyin teoreettinen lähestymistapa yrittäjämäisen liiketoiminnan kasvun ymmärtämiseen vuodesta 1962 vuoteen 2006. (Levie & Lichtenstein, 2010.)

O'Farrell ja Hitchens (1988) sekä McMahon (1998) jakavat kasvuteoriat neljään pääluokkaan:

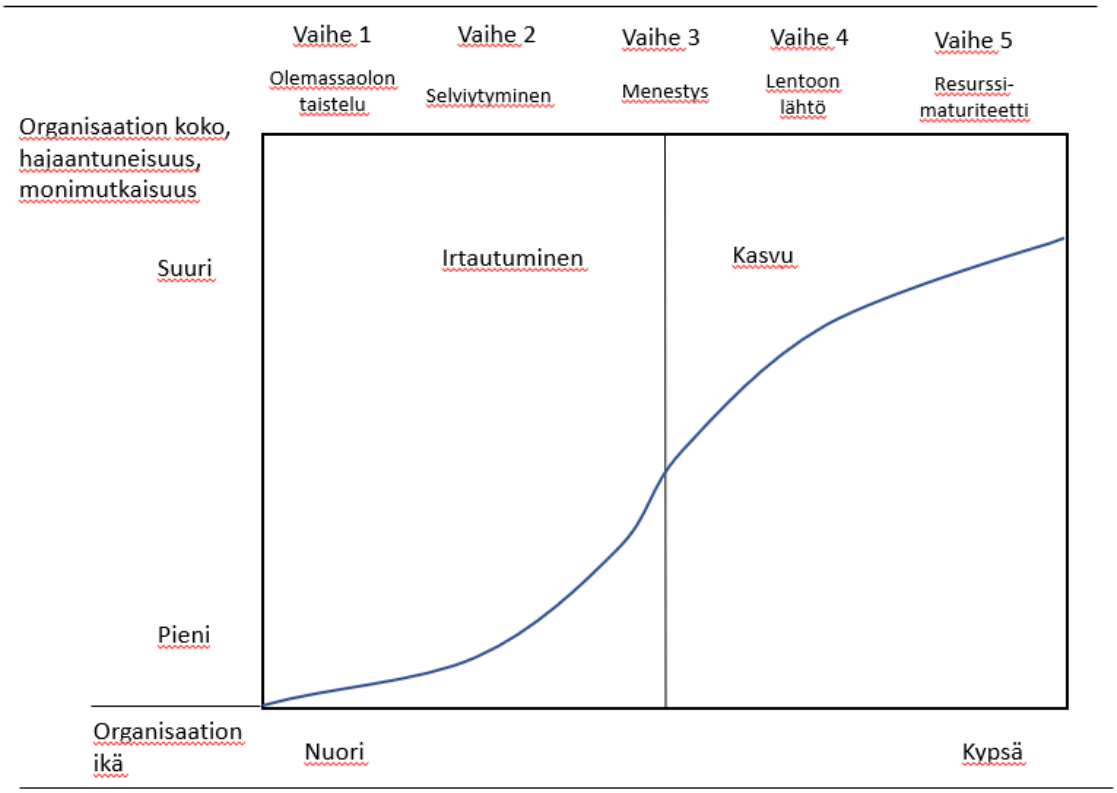
1. *Enimmäkseen staattiset tasapainoteoriat* (mostly static equilibrium theories): Penrosen (1959) näkemykset johdon ajan ja asiantuntevuuden saatavuudesta, ja sen vaikutuksesta yrityksen saavutettavissa olevaan kasvuun ovat tärkeimmässä roolissa.
2. *Stokastiset yrityksen kasvumallit* (stochastic models of firm growth): Tiivistettynä, stokastiset mallit olettavat, että monet tekijät vaikuttavat organisaation kasvuun, ja siksi ei ole olemassa yhtä hallitsevaa teoriaa.
3. *Yrityksen omistajien ja johdon näkemys yrityksen kasvusta* (strategic management perspectives on SME growth): Mallit keskittyvät yrittäjän menettelytapojen, motiivien ja strategian tunnistamiseen. Keskeisessä roolissa on yrittäjän näkemys siitä, mihin yrittäjä haluaa firmaansa viedä. Nämä erilaiset motiivit ja menettelytavat näkyvät yrityksen kasvussa.
4. *Erilaiset organisaation kasvuvaihemallit:* Mallit pohjautuvat taloudellisiin teorioihin. Niissä pienten organisaatioiden kasvu nähdään prosessina, josta voidaan tunnistaa erilaisia kehitysvaiheita, joiden läpi organisaatio kulkee kasvaessaan. Esim. Greiner (1989), Lewis ja Churchill (1983), Picken (2017).

2.2.2 Organisaation kasvuvaihemallien kehitys

Teorioita pienen yrityksen kasvusta löytyy paljon enemmän, kuin mitä tämän tutkielman yhteydessä esitellään (mm. Hanks ym., 1994; Penrose, 1959; Scott & Bruce, 1987; Wiklund, Patzelt, & Shepherd, 2009; Farouk & Saleh, 2011; Lester, Parnell & Carraher, 2003). Tässä luvussa esitellään ensin kaksi staattista kasvuvaihemallia: Lewisin & Churchillin (1983) ja Pickenin (2017) teoriat organisaation kasvusta, jonka jälkeen on vielä esimerkki Gabrielssonin ja Gabrielssonin (2013) dynaamisesta kasvuteoriasta.

Klassinen teoria organisaation kasvuvaiheista: Lewis ja Churchill (1983) on esimerkki klassisesta staattisesta kasvuvaihemallista. He jakavat suositussa teoriassaan pienten yritysten kasvuvaiheet viiteen kehitysvaiheeseen, joissa siirtymä vaiheesta toiseen tapahtuu eri ”kriisien” välityksellä. Malli pohjautuu Greinerin (1989) alun perin vuonna 1972 esittämään teoriaan yrityksen kasvusta evoluution ja ”revoluution” kautta. Kuvio 1 havainnollistaa asiaa. Kasvuvaiheet etenevät seuraavasti:

1. Ensimmäisessä vaiheessa, ”taistelussa olemassaolostaan”, yritys keskittyy asiakkaiden haalintaan ja toimittamaan kehittämäänsä palvelua tai tuotetta.
2. Toisessa vaiheessa, ”selviytyminen”, yritys on todistanut, että sen liiketoiminnalla on kysyntää, mutta kysymys on, onko yrityksen mahdollista pitää liiketoimintaa yllä ja kääntää se voitolliseksi.
3. Kolmas vaihe on ”menestys”: Yrityksen omistajien on tehtävä valinta - jatkaako yritys kasvun polulla vai keskittyykö se pitämään nykyisen liiketoimintansa vakaana ja voitollisena. Kolmannen vaiheen saavuttaneen yrityksen omistajilla on jo usein mahdollisuus halutessaan tehdä siirtoja omistajuuden suhteen, kuten irtautua yrityksestä kokonaan tai siirtyä johdossa taka-alalle.
4. Neljäs vaihe teoriassa on ”lentoon lähtö”: Yrityksen omistajat / johto on päättänyt tavoittelevansa yrityksen kasvua. Johdon pohdittava on, miten mahdollistaa nopea kasvu ja miten kasvu rahoitetaan.
5. Viidennessä vaiheessa yritys saavuttaa ”resurssimaturiteetin”. Yritys on jo kasvanut siihen kokoluokkaan, että sillä on mahdollisuudet nousta merkittäväksi tekijäksi markkinallaan. Yrityksellä on etuna kokonsa, taloudelliset resurssinsa ja johdon taidot, jos se säilyttää yrittäjämäisen asenteensa.



KUVIO 1 Pienen yrityksen kasvuvaiheet, mukaillen Lewis & Churchill (1983)

Lewisin ja Churchillin mallissa jokaista kehitysvaihetta kuvaa eri asteinen toiminnan laajuus, jota arvioidaan kolmella tekijällä: yrityksen koko, hajaantuneisuus ja monipuolisuus. Yrityksen alkuvaiheilla sen toiminta on pientä, keskittynyttä ja melko yksinkertaista. Toiminnan kasvaessa myös organisaatio luonnollisesti kasvaa ja asiat monimutkaistuvat. Lewis ja Churchill identifioivat mallissaan viisi johtamisen dynaamista muuttujaa, jotka vaikuttavat organisaation kasvuun kaikissa organisaation kasvuvaiheissa. Yrityksen kohtaamat haasteet ja vaatimukset muuttuvat yrityksen siirtyessä kasvuvaiheesta toiseen.

1. *Johtamisen tyyli*: Alussa yrityksen liiketoiminta perustuu johdon (yrittäjän) kykyihin toteuttaa omaa liiketoimintaansa: myydä, tuottaa, keksiä ym. Yrittäjän kyvyillä delegoida ei vielä tässä vaiheessa ole juuri merkitystä, kun työntekijöitä on vähän. Muut taidot ratkaisevat. Yrityksen kasvaessa yrittäjän tekemisen painopiste siirtyy kuitenkin yhä enemmän itse tekemisestä toiminnan johtamiseen. Yrittäjän pitää osata delegoida ja johtaa muiden tekemistä.
2. *Organisaatiorakenne ja muodollisten prosessien ja järjestelmien aste*: Alussa organisaatiorakenne on yksinkertainen ja muodollisten prosessien ja järjestelmien määrä on minimaalinen. Toiminta perustuu enemmän suoraan valvontaan ja luottamukseen kuin määriteltyihin rooleihin ja prosesseihin.

3. *Strategiset tavoitteet*: Yrityksen strategiset tavoitteet elävät organisaation kasvaessa. Alussa määräävässä asemassa on usein keskittyminen yrityksen selviytymiseen, mutta toiminnan kasvaessa strategiset tavoitteet monipuolistuvat ja vaihtelevat sen mukaan, mihin yrityksen johto haluaa yrityksen etenevän: Tähtääkö se esimerkiksi voimakkaaseen kasvuun vai voitollisen nykytilan säilyttämiseen jne.
4. *Omistajien osallistuminen liiketoimintaan*: Alussa yrityksen omistaja(t), eli yrittäjä(t), on käytännössä koko yritys. Organisaation kasvun myötä heidän roolinsa kuitenkin muuttuu. Osa haluaa siirtyä sivuun organisaation henkilöstön pärjätessä omillaan, osa haluaa yhä pysyä mukana, mutta joutuu keskittämään ajankäyttöään yhä tarkemmin.

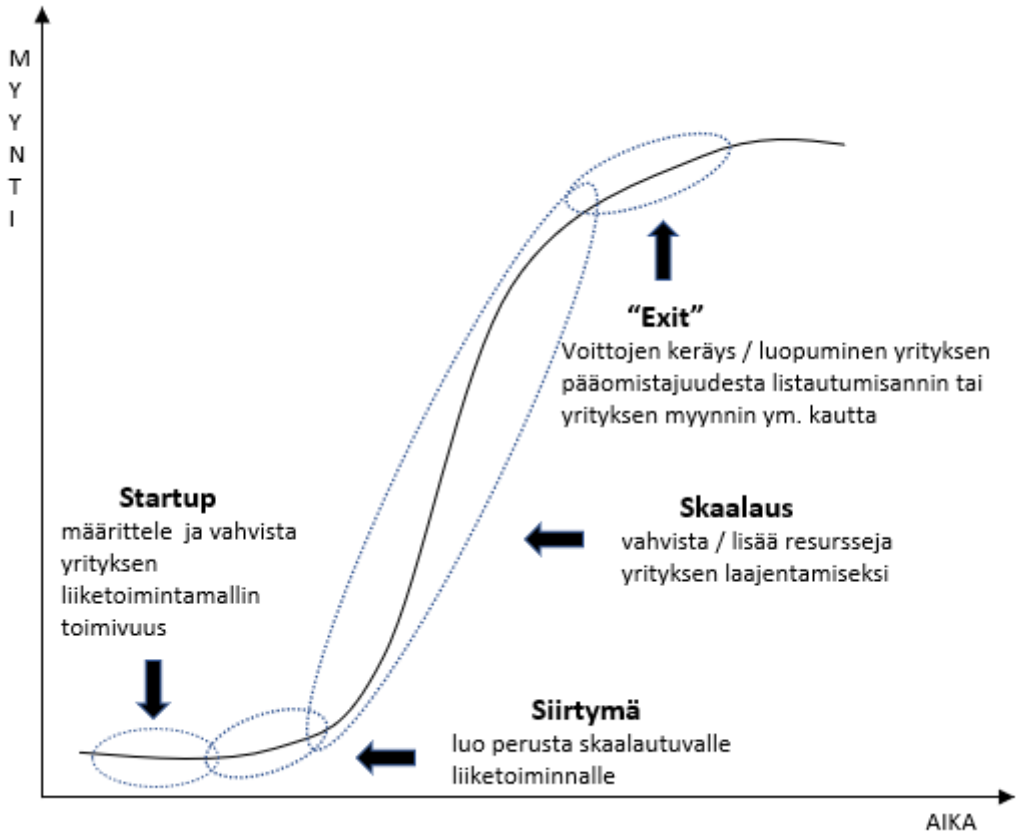
Lewis & Churchill yhdistävät malliinsa lisäksi vielä neljä tekijää, jotka liittyvät yritykseen ja neljä omistajaan (yrittäjään) liittyvää tekijää; näiden tekijöiden merkitys vaihtelee ja muuttuu yrityksen kasvaessa. Ne korostavat tarvetta yrittäjän joustavuudelle. Yritykseen liittyvät seuraavat tekijät: taloudelliset resurssit (ml. käteisvarat ja lainanotto), henkilöstö (erityisesti henkilöstön laatu ja osaaminen), toiminnanohjausresurssit (tietojärjestelmät, suunnittelu- ja valvontajärjestelmät) ja yrityksen liiketoiminnalliset resurssit (asiakas- ja toimittajasuhteet, markkinaosuus, prosessiteknologia, jakeluprosessit ja maine). Omistajaan liittyvät tekijät: omistajan tavoitteet (omat tavoitteet ja yritykselle asetetut tavoitteet, omistajan operatiiviset kyvyt (esim. tuotanto, johtaminen ja markkinointi), omistajan halu delegoida vastuuta ja johtaa muiden tekemistä ja omistajan strategiset kyvykkyydet (tulevaisuuden suunnittelu). Lewisin & Churchillin (1983) teoria on klassinen esimerkki kasvumallista, joka esittää, kuinka yrityksen kasvu tuo mukanaan erinäisiä ongelmia ja muutoksia, joihin yrityksen omistajan (yrittäjän) pitää osata reagoida, jotta kasvu voi jatkua.

Kasvuvaihemalleja julkaistaan yhä edelleen tutkimuksessa. Mm. Picken (2017) esittää oman teoriansa startup-yrityksen kasvusta (kuvio 2). Mallissa kasvuvaiheet eivät ole tarkkaan eriteltyjä ja vaiheet voivat mennä osin päällekkäin, mutta suunta on selkeä. Mallissa on paljon samoja asioita, kuin Lewisin & Churchillin (1983) mallissa, mutta toisaalta se korostaa ajan hengen mukaisesti enemmän esimerkiksi asiakaslähtöisyyttä ja toiminnan ripeää skaalausta, mikä ei vielä Lewisin ja Churchillin mallin aikaan ollut yhtä keskeisessä roolissa. Seuraavana kuvataan Pickenin (2017) kasvumalli startup-yrityksen kasvusta.

Moderni teoria startup-yrityksen kasvuvaiheista: Pickenin (2017) mallissa startup-yritys käy onnistuessaan läpi neljä kasvuvaihetta: Startup, siirtymä, skaalaus ja exit. Startup-vaiheessa tärkeintä on määritellä yrityksen liiketoimintamalli ja todistaa sen toimivuus käytännössä. Startup-vaiheessa organisaatiorakenne ja yrityksen toimintatavat ovat vielä usein hyvin epämuodollisia ja joustavia. Startup-vaiheen jälkeen edessä on tärkeä siirtymävaihe, joka luo perustan skaalautuvalle liiketoiminnalle. Siirtymävaihe alkaa, kun yritys saa ensimmäisen kerran jalansijaa markkinalla. Siirtymävaiheessa yrityksen pitää omaksua järjestelmällisempiä tapoja toimia, jotta se on valmiina ripeään toiminnan skaalaukseen. Yrittäjän pitää selvitä kahdeksasta siirtymävaiheen esteestä:

1. *Suunnan määrittäminen ja määritetyistä tavoitteista kiinni pitäminen*: Yrittäjällä pitää olla selkeä ja realistinen visio organisaation tavoitteista (asiakasryhmä, tarjoama, arvolupaus, liiketoimintamalli jne.), jotta yritys keskittyy oikeisiin asioihin.
2. *Tuotteiden / palveluiden paikan löytäminen laajentuneilla markkinoilla*: Asiakassuhteiden ja jakelukanavien luonti, tuote- ja/tai palveluvalikoiman laajentaminen ja sovittaminen uusille markkinoille.
3. *Asiakas- ja markkinalähtöisyyden ja reagointikyvyn säilyttäminen*: Organisaation pitää pystyä säilyttää alkuaikojen ketteryys, vaikka organisaatio kasvaa ja tehtävät eriytyvät. Yrityksen pitää luoda / kehittää uusia tehokkaita prosesseja, jotta asiakaslähtöisyys voidaan säilyttää.
4. *Organisaation rakentaminen ja johdon sitouttaminen*: Johtoryhmän valinta on kriittistä yrityksen menestymisen kannalta. Tarvittavat taidot ja organisaation tarpeet muuttuvat yrityksen kasvaessa.
5. *Infrastruktuurin ja prosessien kehittäminen*: Tehokas päätöksentekoprosessi, johtaminen ja infrastruktuuri ovat elintärkeitä kasvun tukemiseksi. Kun yritys saa jalansijaa markkinoilta, tarvitaan uusia järjestelmiä ja prosesseja.
6. *Taloudelliset kyvykkyydet*: Pelkkä rahankeräys ei riitä. Sijoittajia kiinnostaa myös resurssien tehokas hyödyntäminen, toimivat kontrollit, pääoman tehokas allokointi, uskottavat taloudelliset ennusteet ja selkeä kommunikointi sidosryhmille.
7. *Organisaatiokulttuuri*: Yrityksen perustajilla on mahdollisuus luoda kulttuuri, joka on yhteydessä sen arvoihin ja normeihin. Oikeanlaisen yrityskulttuurin luomisessa epäonnistuminen johtaa yrityksen epäonnistumiseen.
8. *Riskien ja haavoittuvuuksien hallinta*: Nopeasti kasvavat uudet yritykset ovat alttiita riskeille. Nopea kasvu, kapeat tuottokanavat, kokemattomat työntekijät, avaintyöntekijöiden petturuus, riittämätön infrastruktuuri, tietojärjestelmät ja erilaiset harhat ovat esimerkkejä erilaisista riskien lähteistä.

Skaalausvaiheessa yrityksen omistajien pitää vahvistaa merkittävästi yrityksen resursseja ja hyödyntää yhteistyöverkostoaan vipuvartena; tavoitteenaan liiketoiminnan voimakas kasvu. Yritys pyrkii saavuttamaan jalansijan kohdemarkkinallaan, saavuttaakseen sen (markkina-aseman) tuomat kilpailuedut. Liiketoiminnan ripeä skaalaus edellyttää yritykseltä muodollisuutta, määriteltyjä prosesseja ja kurinalaisuutta. Epämuodolliset toimintatavat eivät ole enää tehokkaita, joten yrityksen pitää omaksua muodollisempia toimintatapoja: yrityksen sisällä tapahtuu yhä enemmän erikoistumista ja prosessit muuttuvat muodollisempaan suuntaan. Mallin viimeinen vaihe on exit, omistajanvaihto, jossa yrityksen omistajat ja sijoittajat myyvät omistuksiaan (esim. listautumisanti, yhdistyminen, yrityksen myynti), jotta he pääsevät ”nauttimaan työnsä hedelmistä”.



KUVIO 2 Neljä vaihetta startup-yrityksen elinkaaressa, mukaillen Picken (2017)

Staattiset kasvuvaihemallit ovat saaneet myös kritiikkiä. Useat tutkijat ovat todenneet, että ei ole olemassa yhtä kaiken kattavaa teoriaa, joka selittäisi yrityksen kasvun riittävän hyvin (Gibb & Davies, 1990; Levie & Lichtenstein, 2010; O'Farrell &Hitchens, 1988; McMahon, 1998). Kasvuvaihemallit perustuvat usein oletukselle, että organisaatiot kehittyvät yhdenmukaisella ja ennustettavalla tavalla (Levie & Lichtenstein, 2010). Yrityksen kasvu on tyypillisesti kuitenkin katkonainen prosessi (Smallbone, Leig & North, 1995). Staattisten kasvuvaihemallien ongelmana on, että esimerkiksi korkean teknologian startup-yrityksissä ei ole tavatonta, että yritykset "jättävät välistä" kasvuvaiheita kasvaessaan nopeasti suureen kokoluokkaan muutamassa vuodessa (Hanks ym., 1994). Hanks ym., (1994) mukaan korkean teknologian startup-yritykset kohtaavat kasvuun liittyvät kriisit aiemmin ja nopeammin kuin vähemmän vaihtelevissa ympäristöissä. Levie & Lichtenstein (2010) toteavat, että eri malleissa on eri määrä kasvuvaiheita (kolmesta jopa kymmeneen (O'Farrell & Hitchens, 1988), mutta siihen ei ole pystytty esittämään vakuuttavia perusteluja miksi asia on niin. Lisäksi tutkijat eivät ole päässeet yhteisymmärrykseen siitä, miksi organisaatiot ylipäätään siirtyvät kasvaessaan vaiheesta toiseen (Levie & Lichtenstein, 2010). Kasvuvaihemalleilla on usein korkea näennäisvaliditeetti (yrittäjät tunnistavat yrityksensä olevan tietyssä kasvuvaiheessa), mutta se ei riitä vakuuttamaan kaikkia tutkijoita. Levie ja Lichtenstein (2010) esittävät, että

staattiset kasvuvaihemallit tulisi hylätä, sillä ne eivät ole soveltuvia työkaluja liiketoiminnan kasvun ymmärtämiseen. Vaihtoehtoinen teoria staattisten mallien tilalle on mm. Levie & Lichtensteinin (2010) itsensä esittämä dynaaminen kasvumalli. Seuraavaksi esitellään Gabrielssonin ja Gabrielssonin (2013) esittämä teoria yrityksen kasvusta.

Dynaamiset teoriat yrityksen kasvusta: Gabrielsson & Gabrielsson (2013) esittävät vaihtoehdon staattisille malleille. Heidän mallinsa pohjautuu Levie & Lichtensteinin (2010) esittämään ajatukseen yrityksen dynaamisista tiloista ja tilojen muutoksista. Mallissa on neljä vaihetta, jotka kansainvälisille markkinoille tähtäävät b2b-yritykset käyvät läpi. Vaiheiden määrä voi vaihdella kontekstista riippuen, sillä yrityksen kehitys ei ole aina lineaarista. Lisäksi jokaisessa kasvuvaiheessa yrityksellä on mahdollisuus joko selvitä tai epäonnistua.

Dynaaminen kasvumalli pohjautuu ajatukseen, että organisaatiot ovat, kuten elävät organismit, riippuvaisia ympäristöstään (Levie & Lichtenstein, 2010). Dynaamiset tilat ovat avoimia, monimutkaisia, sopeutuvia järjestelmiä, jotka operoivat epätasapainoisessa / epätäydellisessä todellisuudessa. Yritys on ”energiankonversiojärjestelmä”, joka organisoi resursseja (materiaaleja, kyvykkyyksiä jne.) tuotteiksi ja palveluiksi, jotka tuovat arvoa yrityksen asiakkaille. (Levie & Lichtenstein, 2010.) Yrityksen liiketoimintamalli määrittää sen arvonluontistrategian. Yrityksen liiketoimintamalli koostuu aktiviteeteista, resursseista, yhteistyöjärjestelyistä ja strategisesta asemasta, joita yritys tarvitsee muuttaakseen havaitsemansa liiketoimintamahdollisuuden aidoksi liiketoiminnaksi. Strategiset päätökset, toiminnan organisointiin liittyvät aktiviteetit ja organisatoriset prosessit heijastavat yrityksen sisäistä hallitsevaa liiketoimintalogiikkaa. (Levie & Lichtenstein, 2010.)

Yrittäjän arvio kohdemarkkinan kokonaiskasvusta ja yrityksen kasvumahdollisuuksista tällä markkinalla ovat tärkeä osa ”mahdollisuusjännitettä” (opportunity tension). Mahdollisuusjännite tarkoittaa jokaisen dynaamisen tilan ”sisäänrakennettua” yhdistelmää, eli ”yrittäjän näkemystä resurssipotentiaalista” (yrittäjän tunnistama liiketoimintamahdollisuus, markkinapotentiaali) *ja* yrittäjän halu / kyky muuttaa tämä potentiaali todellisuudeksi. Yrittäjän näkemys koostuu valistuneesta arvauksesta esimerkiksi markkinan mahdollisesta koosta, saatavilla olevista resursseista ja sitoutumisesta perustamaan organisaatio, joka tarvitaan tämän mahdollisuuden toimeenpanemiseksi. Arvio perustuu pääosin yrittäjän henkilökohtaiseen uskoon tulevista mahdollisuuksista ja uskosta omiin kyvykkyyksiin, etenkin jos markkinaa itsessään ei vielä ole olemassa – mikä ei ole mitenkään poikkeuksellinen ilmiö useimpien nopean kasvun startup-yritysten kohdalla. (Levie & Lichtenstein, 2010.) Mikä Levien & Lictensteinin (2010) dynaamisten tilojen mallissa muuttaa ”mahdollisuusjännitteen” aidoksi arvon luonniksi, on yrityksen liiketoimintamalli. Yrityksen liiketoimintamalli muodostuu vuorovaikutuksessa yrityksen verkoston kanssa. Yrityksen pääasiallinen tarkoitus on luoda asiakas (Drucker, 2020). Yrityksellä on edellytykset olemassaoloon vain, jos sen asiakkaat saavat aidosti arvoa yrityksen

tuottamista tuotteista / palveluista. Näin yritys voi säilyttää itsensä myös epätasapainon tilassa. (Levie & Lichtenstein, 2010.)

Gabrielssonin ja Gabrielssonin (2013) mallissa tutkittavat yritykset kävivät onnistuessaan läpi neljä vaihetta:

1. Yrityksen perustaminen (International New Venture creation)
2. Yrityksen tuotteen / palvelun kaupallistaminen ja siirtymä kansainvälisille markkinoille (Commercialization and foreign entries)
3. Nopea kasvu ja laajentuminen ulkomailla (Rapid growth and foreign expansion)
4. Toiminnan kypsyys ja järkeistäminen (Rationalization and foreign maturity)

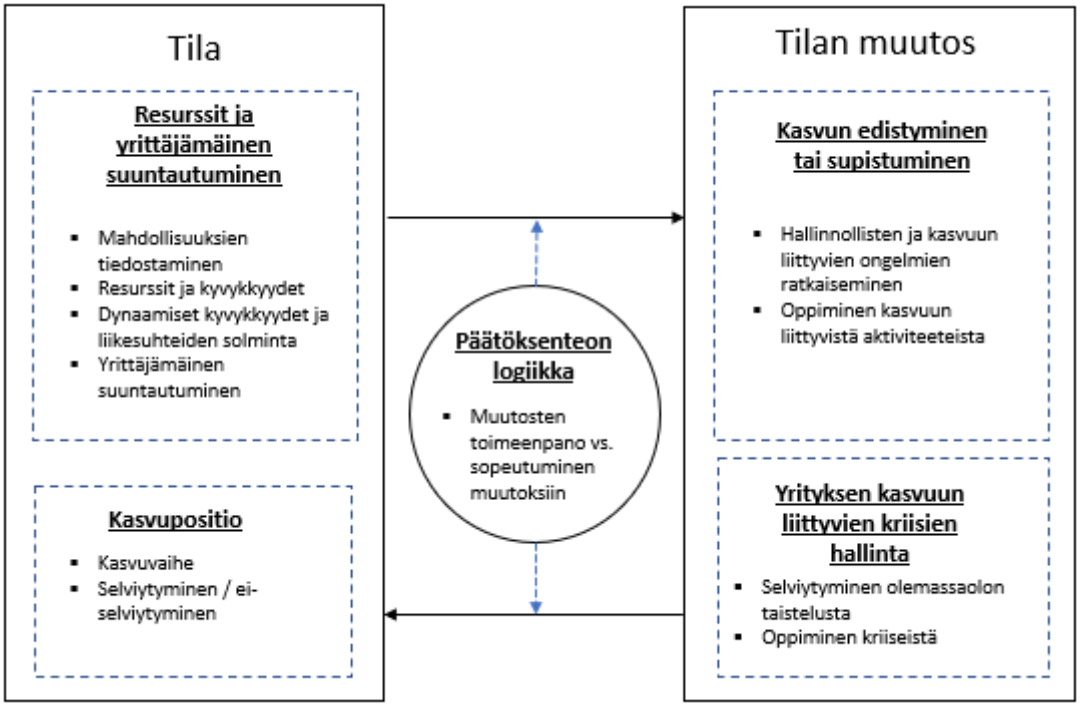
Kasvuvaiheiden määrä voi tutkijoiden mukaan vaihdella kontekstista riippuen, sillä yrityksen kehitys ei ole aina lineaarista. Lisäksi jokaisessa kasvuvaiheessa yrityksellä on mahdollisuus joko selvitä tai epäonnistua. Yrityksen kasvu saattoi myös hetkittäin taantua ja toiminta supistua. Gabrielssonin ja Gabrielssonin tutkimuksen kohteena olivat avoimella ja pienellä talousalueella toimivat korkean teknologian b2b-yritykset (yritykseltä-yritykselle myynti).

Yritykset kohtaavat kasvaessaan monenlaisia kasvuun liittyviä ongelmia. Ensinnäkin, yrityksen ensimmäisenä haasteena on ylipäätään selviytyä. Toiseksi, yritys kohtaa erilaisia johtamisen ongelmia toiminnan muuttaessa muotoaan ja muita kansainvälistymiseen liittyviä haasteita. Kaikki nämä haasteet vaativat ratkaisua ennen yrityksen siirtymää seuraavaan kasvuvaiheeseen. (Gabrielsson & Gabrielsson, 2013.) Yrityksen johtamisessa korostuvat johdon dynaamiset kyvykkyydet (Eisenhardt & Martin, 2000) ja yrittäjämäinen suuntautuminen. Yrityksen selviytymisen ja menestymisen kannalta on elintärkeää, että yritys osaa sekä löytää että luoda uusia mahdollisuuksia kasvaa ja tehdä liiketoimintaa. Oppiminen on tärkeässä roolissa yrityksen kasvun kannalta. Myös yrityksen kyvyllä luoda omat verkostonsa on suuri vaikutus yrityksen kasvuun, sekä investointitarpeiden että riskien minimoimisen kannalta. Etenkin yritysten väliset b2b-suhteet ovat tärkeitä. Yritysten pitää osata hyödyntää oman verkostonsa resursseja tehokkaasti. Kun yrityksen ei tarvitse hoitaa kaikkea itse, se pienentää tarvittavia investointikustannuksia ja laskee riskitasoa. Johdon kyvykkyys on merkittävässä roolissa siirtymissä kasvutilojen välillä, mutta myös kasvuun liittyvien ongelmien ratkaisemisessa. (Gabrielsson & Gabrielsson, 2013.)

Aikaisessa vaiheessa yrityksen selviytymisen kannalta tärkeintä on mahdollisuuksien luonti ja tutkiva oppiminen (explorative learning, esimerkiksi tuoteinnovointi ja uusien asioiden kokeilu). Myöhemmissä kasvuvaiheissa korostuu yrityksen kyky löytää uusia mahdollisuuksia ja ”hyödyntävän oppimisen” (exploitative learning, esimerkiksi asioiden toisintaminen uusissa ympäristöissä ja parantelu) merkitys kasvaa. Yrittäjämäinen suuntautuminen on tärkein kyvykkyys yrityksen alkutaipaleella, mutta myöhemmissä vaiheissa sen ylikorostuminen voi jopa kääntyä negatiiviseksi yrityksen selviytymisen kannalta. Yritysten pitää siirtyä ketteryydestä kohti hallittavampia

toimintatapoja siirtyessään kasvuvaiheesta toiseen (toiminnan laajentuessa riittävän paljon).

Yrityksen tapa tehdä päätöksiä, eli päätöksentekologiikka, on merkittävä sisäinen valmiustekijä ja keskeisessä roolissa yrityksen kasvun kannalta. Päätöksenteon logiikka vaikuttaa sekä yrityksen kasvupositioon että kasvutilan (growth state) muutokseen. Yritys voi lähestyä muutoksia kahdelta kantilta: yritys voi pyrkiä aktiivisesti mukauttamaan omaa toimintaympäristöänsä itselleen sopivaksi tai vastaavasti yrittää sopeutua liiketoimintaympäristön muutoksiin. Kuvio 3 kuvaa Gabrielssonin ja Gabrielssonin (2013) mallia.



KUVIO 3 Dynaaminen malli kansainvälisisille markkinoille tähtäävien B2B-yritysten kehitysvaiheista, mukaillen Gabrielsson & Gabrielsson (2013)

2.2.3 Yhteenveto

Yrityksen kasvun kannalta edellytyksenä on, että se selviää ensimmäisistä ”olemassaolon taisteluistaan” yrityksen perustamisen jälkeen ja löytää asiakkaita (Churchill & Lewis, 1983; Hanks ym., 1994; Gabrielsson & Gabrielsson, 2013; Picken, 2017). Kaikki tässä esitellyt mallit korostavat toimivan liiketoimintamallin tärkeyttä yrityksen selviytymisen ja kasvun kannalta (Levie & Lichtenstein, 2010). Oppimisen merkitys on suuri (Littunen & Tohmo, 2003; Gabrielsson & Gabrielsson, 2013). Yrityksen alkutaipaleella korostuvat yrittäjämäinen suuntautuminen ja yrittäjän kyvyt (Churchill & Lewis, 1983). Myöhemmin tärkeiksi nousevat erilaiset organisointikyvykkyydet, sillä yrityksen pitää omaksua järjestäytyneempiä toimintatapoja (Churchill & Lewis, 1983; Hanks ym., 1994) ja liiallisesta yrittäjämäisestä suuntautuneisuudesta voi olla jopa haittaa (Gabrielsson & Gabrielsson, 2013). Nopean kasvun kannalta on

tärkeää, että yritys osaa luoda verkostoja ja hyödyntää verkostonsa resursseja (Picken, 2017; Gabrielsson & Gabrielsson, 2013). Yrityksen kasvaessa, yrityksen johto kohtaa erilaisia kasvuun liittyviä ongelmia ja kriisejä, jotka sen pitää osata ratkaista, jotta yritys voi jatkaa kasvuaan (Churchill & Lewis, 1983; Gabrielsson & Gabrielsson, 2013). Muita kasvun kannalta merkityksellisiä tekijöitä ovat esimerkiksi yrityksen sijainti (Littunen & Tohmo, 2003), digitalisaation aste (Larja & Räisänen, 2019), yrityksen tuote- ja palveluvalikoima (Picken, 2017) ja omistajien liiketoimintaan osallistumisen aste (Churchill & Lewis, 1983; Gabrielsson & Gabrielsson, 2013; Picken, 2017). Seuraavassa luvussa käsitellään lyhyesti riskienhallinnan erityispiirteitä pk-yrityksissä ja startup-yrityksissä.

2.3 Riskienhallinta kasvuyrityksissä

Luku käsittelee riskienhallinnan tavoitteita ja keinoja kasvuyrityksille tyypillisessä toimintaympäristössä. Riskienhallinta kuuluu, tai ainakin pitäisi kuulua, jokaisen organisaation toimintaan. Hyvin hoidettu riskienhallinta on usein melko huomaamatonta toimintaa, mutta heikon riskienhallinnan seuraukset kärsitään usein kantapään kautta (Kupi, Keränen & Lanne, 2009). Myös tietoturvaan panostaminen kuuluu olennaisena osana riskienhallintaan yrityksissä (Bojanc & Jerman-Blažič, 2008).

Riskienhallinta voidaan määritellä pyrkimyksenä haitallisten tapahtumien välttämiseen tai niiden seurausten minimoimiseen (Kupi ym., 2009; Raggad, 2010). Riskienhallintastandardi (AS/NZS 4360:2004) määrittelee riskin jonkin tapahtuman muutoksena, joka voi vaikuttaa asetettujen tavoitteiden saavuttamiseen. Riski voi olla sekä positiivinen että negatiivinen. Riskienhallinta on myös potentiaalisten mahdollisuuksien tunnistamista, analysoimista ja hyödyntämistä organisaation tavoitteiden saavuttamiseksi. (Kupi, Keränen & Lanne, 2009.) Riskienhallinta tähtää ennen kaikkea liiketoiminnan jatkuvuuden turvaamiseen, mutta on yhtä lailla tärkeää myös uutta liiketoimintaa rakennettaessa. Riskienhallintaan sisältyvät toimintakulttuuri, prosessit ja rakenteet, jotka edesauttavat potentiaalisten mahdollisuuksien toteutumista ja joiden avulla hallitaan haitallisia tapahtumia. Tavoitteena on mahdollistaa organisaation liiketaloudellinen menestys. Kyse on varautumisesta uhkiin ja toisaalta mahdollisuuksien hyödyntämisestä. (Kupi ym., 2009.)

Kupi ym., (2009) selvittivät riskienhallinnan roolia osana pk-yritysten strategista johtamista. Organisaation strateginen johto määrittelee, mitä riskejä yrityksessä otetaan ja mitä vältetään. Riskienhallinta on luontaisesti subjektiivista olemukseltaan (Adams, 2007). Riskienhallinnassa ei ole selkeitä sääntöjä seurattavaksi – se sisältää aina tulkintoja ja arvauksia. Historia ei ennusta tulevaisuutta ja tulevaisuus on aina epävarma (Adams, 2007). Riskienhallinta on helppo laiminlyödä, koska sen puute usein huomataan kunnolla vasta kun riskit realisoituvat. Hyvin hoidettu riskienhallinta on proaktiivista toimintaa, joka voi tuoda kilpailuetua yritykselle (Hambrick & Crozier, 1985). Yrityksen johto voi keskittyä strategian kehittämiseen ja

tulevaisuuden suunnitteluun, kun liiketoiminta on jokseenkin ennustettavissa, ja yrityksen aika ei kulu vain akuuttien ongelmien hoitamiseen (Kupi ym., 2009). Huonosti hoidettu riskienhallinta tekee johtamisesta reaktiivista, jolloin yritysjohdon huomio kohdistuu liikaa nykytilanteeseen ja tulevaisuuden suunnittelu kärsii (Kupi ym., 2009). Hyvin menestyvät yritykset varautuvat kasvuloikkaan jo ennalta luomalla perustan proaktiiviselle johtamiselle (Hambrick & Crozier, 1985).

Pk-yritysten riskienhallinta on harvoin yhtä pitkälle jalostunutta ja muodollista kuin suuremmissa organisaatioissa. Kupi ym. (2009) toteavat, että mikro-organisaatioissa korostuu tarve ymmärtää riskienhallinta yritystoiminnan kulmakivenä, mutta pk-yrityksillä ei ole useinkaan mahdollisuutta palkata erillistä työntekijää hoitamaan riskienhallintaa. Pk-yrityksissä ja startupeissa muutamat avainhenkilöt vastaavat usein hyvin laajoista kokonaisuuksista yritystoiminnan kentällä. (Kupi ym., 2009.) Lisäksi pk-yritysten riskienkantokyky on usein heikko johtuen rajallista resursseista (Kupi ym., 2009). Usein tiedostetuillekaan riskeille ei voida tehdä suuria budjettivarauksia siltä varalta, että riski sattuisi realisoitumaan. Kasvuyrityskontekstissa toisaalta korostuvat tuntemattomat riskit, joihin on usein mahdotonta varautua ennalta (Sommer, Loch & Dong, 2009). Sommer ym., (2009) argumentoivat, että perinteiset riskienhallinnan menetelmät sopivat hyvin tilanteisiin, joissa riskien luonne on hyvin ymmärretty, mutta huonommin tilanteisiin, joissa tulevaisuus on hämärän peitossa. Uudet yritykset harvoin onnistuvat näkemään heti alussa parhaita markkinatilaisuuksia tai parhaita tapoja tarttua niihin. Sommer ym., (2009) tunnistavat kaksi keskeistä lähestymistapaa kyseisen ongelman ratkaisuun: Valikointi (selectionism) ja yrityksen ja erehdyksen kautta (trial- and error) oppiminen. Ne ovat kaksi startup-yrityksille tyypillistä tapaa lähestyä epävarmaa tulevaisuutta. Valikoinnilla tarkoitetaan lähestymistapaa, jossa yritys kokeilee useita vaihtoehtoisia ratkaisuja ja valitsee jälkikäteen ratkaisuista sopivimman. Toisin sanoen, yritys kokeilee niin montaa eri vaihtoehtoista menetelmää, että oletettavasti joku ratkaisuista johtaa toivottuun lopputulokseen. Yrityksen ja erehdyksen kautta oppiminen tarkoittaa lähestymistapaa, jossa yritys aktiivisesti etsii uutta informaatiota ja muovaa toimintatapojaan vastaamaan tätä uutta informaatiota. Tämä joustava sopeutuminen ennalta-arvaamattomiin muutoksiin on ollut olennaisessa osassa monessa läpimurtoteknologiassa. (Sommer, Loch & Dong, 2009.)

Yrityksen toimintaympäristö ratkaisee, mikä on toimivin lähestymistapa riskienhallintaan. Jos toimintaympäristö ei ole erityisen monimutkainen tai ennalta-arvaamaton, perinteisen riskienhallinnan menetelmät kuten yksityiskohtainen suunnittelu ym. ovat tehokkaita menetelmiä. Toisaalta, jos toimintaympäristö on hyvin vaikea ja ennalta-arvaamaton, tarkka suunnittelu on vähemmän kriittistä onnistumisen kannalta ja oppiminen matkan varrella korostuu. Mikäli toimintaympäristö taas on hyvin epävarma, mutta ei erityisen monimutkainen, yrityksen kannattaa hyödyntää yrityksen ja erehdyksen kautta oppimista etukäteissuunnittelun lisänä. (Sommer ym., 2009.) Karydan ym., (2006) mukaan käyttäjien osallistaminen riskienhallintaan (tietoturvan saralla),

johtaa organisaation parempaan suorituskykyyn esimerkiksi seuraavien asioiden kohdalla: organisaation tietoisuus riskeistä paranee, tietoturva on sidottu paremmin yrityksen liiketoimintaan, käytettyjen kontrollien laatu paranee ja kontrollit kehittyvät. Käyttäjät voivat olla siten arvokas resurssi kontrollien ja turvallisuuskäytänteiden määrittämisessä.

Yhteenvetona voidaan todeta, että riskienhallinta on tärkeä tekijä tuloksellisen liiketoiminnan kannalta, jota ei tulisi laiminlyödä. Yrityksen toimintaympäristö ratkaisee, mitkä menetelmät ovat toimivimpia, mutta hyvin hoidettu riskienhallinta on proaktiivista toimintaa, joka voi tuoda aitoa kilpailuetua yritykselle (ja mahdollistaa kestävän kasvun). Seuraava luku käsittelee tietoturvainvestointeja osana organisaation riskienhallintaa.

3 TIETOTURVAINVESTOINNIT OSANA ORGANISAATION RISKIENHALLINTAA

Luvussa määritellään tutkielman kannalta olennaiset termit. Lisäksi käydään läpi tietoturvainvestointien tueksi kehitettyjä päätöksentekomalleja ja akateemista kirjallisuutta, erilaisia taustatekijöitä, joilla on todettu olevan vaikutusta investointipäätöksiin, tietoturvainvestointeihin liittyviä haasteita, erilaisia investointityyppejä ja tietoturvainvestointiprosessia. Lukijan pitäisi saada tämän luvun jälkeen käsitys siitä, mitä tietoturvainvestointi tarkoittaa käytännössä, millaista tutkimusta tietoturvainvestoinneista on toistaiseksi tehty ja mitä haasteita investointiprosessiin liittyy.

3.1 Keskeisten käsitteiden määritelmät

Tietoturva: (ISO/IEC, 2005) standardi määrittelee tietoturvan tiedon luottamuksellisuuden, koskemattomuuden, ja saatavuuden varmistamisena. Suojattava informaatio voi esiintyä monessa muodossa.

- Luottamuksellisuus: Vain luvan saaneet henkilöt voivat käsitellä suojattua informaatiota
- Koskemattomuus: Informaatio on tarkkaa, puutteetonta ja yhdenmukaista, ja vain sallitut henkilöt voivat muokata sitä
- Saatavuus: Informaatio on saatavilla sallituille henkilöille kohtuullisen aikarajan puitteissa.

Whitman and Mattord (2011) lisäävät tietoturvan määritelmään lisäksi tarkkuuden, aitouden, hyödyllisyyden ja hallussapidon käsitteet suojattavina tiedon ominaisuuksina. Tietoturvan perimmäisenä tavoitteena voidaan pitää organisaation liiketoiminnan jatkuvuuden varmistamista (Von Solms, 1998).

IT-investointi: Investoinnilla konseptina on yksi tarkoitus: tuotto (Tsiakis & Stephanides, 2005). Investointi informaatioteknologiaan voidaan nähdä investointina organisaation tulevaan kasvuun. It-investointi toimii mahdollistajana, joka luo pohjan yrityksen liiketoimintastrategian toteuttamiselle ja / tai tuo kustannussäästöjä (Mahmood & Mann, 1993). Strateginen IT-investointi mahdollistaa organisaation nopean reagoinnin ympäristön muutoksiin.

Tietoturvainvestointi: Tietoturvainvestointi kuuluu IT-investointien joukkoon. Tietoturvainvestoinnin perimmäinen pyrkimys on varmistaa organisaation liiketoiminnan jatkuvuus ja toimia liiketoiminnan mahdollistajana (Tsiakis & Stephanides, 2005). Gordon ja Loeb (2002) määrittävät tietoturvainvestoinnin

harkittuna päätöksenä lisätä resursseja suojaamaan jotain tiettyä informaatiota. Suojattava informaatio voi olla mitä tahansa; esimerkiksi henkilötiedoista koostuva lista, tietojärjestelmä, yrityksen strateginen suunnitelma tai yrityksen verkkosivu. Tietoturvainvestointi voi pyrkiä varmistamaan esimerkiksi suojattavan informaation luottamuksellisuuden, koskemattomuuden, oikeellisuuden, saatavuuden tai kiistämättömyyden. (Gordon & Loeb, 2002.) Tietoturvainvestointi voi kohdistua myös liiketoimintaprosessin tai muun resurssin suojaukseen. Tietoturvainvestoinnin tuotto määritellään todennäköisyytenä sille, että organisaatio kokee kyberhäiriötilanteen – ja mikä on tämän häiriötilanteen hinta – verrattuna tilanteeseen, jossa yritys on investoinut kontrolleihin, joilla häiriötilanne pystytään välttämään tai häiriön seuraukset ovat vähemmän vakavat. Yrityksen tulee siis verrata tietoturvainvestointipäätöstä tehdessään, implementoitavien kontrollien hintaa suhteessa suojattavan informaation hintaan ja mahdollisen häiriötilanteen aiheuttamiin kustannuksiin. (Tsiakis & Stephanides, 2005.)

Riskienhallinta (tietoturva): Riskienhallinta on prosessi, jossa identifioidaan haavoittuvuudet ja uhat organisaation liiketoimintaprosesseissaan hyödyntämille informaatioresursseille, ja päätetään mahdollisista vastatoimista, joilla riski voidaan laskea hyväksyttävälle tasolle, perustuen informaatioresurssien arvoon organisaatiolle (Raggad, 2010).

3.2 Tietoturvainvestoinnit

Tietoturvainvestointeihin liittyvä tutkimus painottui 2000-luvun ensimmäisellä vuosikymmenellä enemmän erilaisiin kvantitatiivisiin menetelmiin, joilla tietoturvainvestointi voidaan optimoida mm. (Gordon & Loeb, 2002; Kort ym., 1999; Bodin ym., 2005). Kvantitatiiviset menetelmät ovat edelleen suosittuja, mutta näissä malleissa on kuitenkin useita puutteita reaalimaailman soveltamisen kannalta (Cavusoglu, 2010; Dor & Elovici, 2016; Heidt ym., 2019; Shao, Siponen & Pahnila, 2019). Moni malleista olettaa, että investointipäätöksen tekijä toimii rationaalisesti (normatiiviset mallit kuten Gordon & Loeb, 2002) ja useat vaikeasti arvioitavat parametrit ovat ennalta tiedossa (mm. peliteoriaan pohjautuvat mallit kuten (Cavusoglu, Raghunathan & Yue, 2008). Kvantitatiivisia menetelmiä hyödyntävät mallit painottavat investoinnin taloudellista näkökulmaa: vaikka investointi turvallisuuteen on yleensä hyvä asia, lisäinvestointi turvallisuuteen ei ole aina hintansa arvoista (Gordon & Loeb, 2002). Ensimmäiset matemaattiset mallit ovat tehty yleisellä tasolla päätöksenteon tueksi ja stimuloimaan tutkimusta aihepiiriin liittyen. Esimerkiksi Gordonin & Loebin (2002) malli on onnistunut siinä hyvin. Mallia on jatkettu useaan otteeseen mm. peliteorialla (Cavusoglu, Raghunathan & Yue, 2008), dynaamisilla malleilla (Behara, Huang & Hu, 2007) ja tietoturvainvestoinnin optimaalisen ajoituksen suhteen (Tatsumi & Goto, 2010).

Viime vuosikymmenellä tietoturvainvestointeihin painottuvan tutkimuksen näkökulma alkoi laajentua. Mukaan tuli yhä enemmän myös erilaisia kvalitatiivisin menetelmin toteutettuja tutkimuksia, jotka laajensivat tutkimusta mm. käyttäytymistieteeseen ja organisatorisiin teorioihin pohjautuen mm. (Heidt ym., 2019; Cavusoglu, 2010; Cavusoglu ym., 2015; Moore, Dynes & Chang, 2015). Investointiprosessiin liittyvän päätöksenteon kontekstisidonnaisuuteen alettiin kiinnittää enemmän huomiota (Heidt ym., 2019; Beebe, 2014; Dor & Elovici, 2016). Yhä enemmän julkaistaan myös erilaisia järjestelmädynamiikan mallinnukseen ja simulointiin pohjautuvia tutkimuksia (mm. Nazareth & Choi, 2015; Carias ym., 2019), joiden pyrkimyksenä on auttaa organisaatioita määrittämään optimaalinen tietoturvainvestointien taso. Optimaalisen investointitason löytäminen on malleille yleinen, yhteinen ongelma, jonka ne pyrkivät ratkaisemaan vaihtoehtoisin menetelmin. Esimerkiksi Nazarethin & Choin (2015) mallissa perustasolla turvallisuuskustannukset laskevat organisaation investoidessa tietoturvaan. Mutta ei rajattomasti, vaan tietyn rajan jälkeen kustannukset ylittävät hyödyt, jolloin lisäinvestoinnit ovat ylimääräisiä kustannuksia ilman todellista hyötyä. Taulukko 2 esittelee aikaisempaa tietoturvainvestointeihin liittyvää tutkimusta.

TAULUKKO 2 Tietoturvainvestoinnit akateemisessa tutkimuksessa

Tutkimuksen tyyppi / näkökulma	**Tutkimus**	**Metodologia**
Taloudellinen näkökulma tietoturvainvestointien optimointiin kvantitatiivisin menetelmin kustannustehokkuuden, hyödyn, tulevien kassavirtojen ja investointibudjetin allokoinnin ym. asioiden suhteen	Kort ym., (1999), Gordon & Loeb (2002), Matsuura (2003), Arora ym., (2004), Purser (2004), Westerlind (2004), Bodin ym., (2005), Tsiakis & Stephanides (2005), Hausken (2006), Huang ym., (2006), Sonnenreich ym., (2006), Ryan & Ryan (2006), Willemson (2006), Herath & Herath (2008), Huang ym. (2008), Bojanc & Jerman-Blažič (2008), Mizzi (2010), Fenz (2011), Huang & Behara (2013)	Matemaattinen malli, matemaattinen malli + tapaustutkimus
Tietoturvainvestoinnin optimointi (peliteoria): Vastapuolen (kyberrikollisten hyökkäysstrategioiden) vaikutus organisaation investointipäätöksiin	Cavusoglu ym., (2004), Bistarelli, Dall'Aglio & Peretti (2006), Cavusoglu, Raghunathan & Yue (2008)	Matemaattinen malli
Systemaattinen kirjallisuuskatsaus tietoturvainvestointien arviointiin käytetyistä taloudellisista menetelmistä	Schatz & Bashroush (2017)	Kirjallisuuskatsaus

Tietoturvainvestoinnin optimaalinen ajoitus suhteessa ajankohtaisiin ja tulevaisuuden uhkiin	Tatsumi & Goto (2010), Ioannidis (2012)	Matemaattinen malli
Tietoturvainvestoinnit ja kumppaniverkosto: Tiedon jakaminen yhteistyöverkostossa, vapaamatkustajaongelma	Gal-Or & Ghose (2005), Tanaka ym., (2005), Liu ym., (2011)	Matemaattinen malli
Mallinnus tietoturvainvestoinneista datan luottamuksellisuuden ja saatavuuden turvaamisen näkökulmasta	Ioannidis ym., (2009)	Matemaattinen malli
Päätöksentekoon vaikuttavat kognitiiviset ja psykologiset harhat, kontekstuaalisten tekijöiden vaikutus	Cavusoglu (2010), Heidt, Gerlach & Buxmann (2019)	Kirjallisuuskatsaus, puolistrukturoitu haastattelu
Puolueellisen muotoilun (engl. framing bias) vaikutus päätöksentekoon	Beebe (2014)	Kyselytutkimus
Institutionaalisten tekijöiden vaikutus organisaation tietoturvainvestointeihin	Cavusoglu ym., (2015)	Kyselytutkimus
Miten ja miksi organisaatiot tekevät tietoturvainvestointeja, käsitteellinen malli päätöksentekoprosessista	Moore ym. (2015), Dor & Elovici (2016)	Puolistrukturoitu haastattelu, avoin haastattelu
Käyttäytymistaloustieteeseen perustuva tietoturvainvestointien viitekehys, maineeseen perustuva laumateoria (herding theory)	Shao (2015), Shao, Siponen & Pahnila (2019)	Kenttätutkimus, kyselytutkimus
Organisaation tietoturvainvestointeihin liittyvien ilmoitusten / ilmoitettujen tietoturvapoikkeamien vaikutus osakkeen markkina-arvoon	Campbell ym., (2003), Cavusoglu, Mishra & Raghunathan (2004), Chai, Kim & Rao (2011)	Tapausmetodologia
Tietoturvainvestointeihin liittyvä päätöksenteko, arviointi ja oppiminen	Weishäupl, Yasasin & Schryen (2018)	Monitapaustutkimus
Tietoturvainvestoinnin arviointi järjestelmädynamiikan mallinnuksen keinoin	Behara ym., (2007), Nazareth & Choi (2015)	Järjestelmädynamiikan mallinnus ja simulointi

Investointistrategiana kyberresilienssi teollisen esineiden internetin näkökulmasta	Carias ym., (2019)	Järjestelmädynamiikan mallinnus ja simulointi

3.2.1 Klassiset taloudelliset mallit

Suosittu lähestymistapa tutkimuksille on ollut taloudellinen näkökulma. Tutkimuksissa verrataan perinteisesti investoinnin kustannuksia suhteessa investoinnin tuomaan hyötyyn mm. (Gordon & Loeb, 2002; Westerlind, 2004; Willemson, 2006; Kort ym., 1999; Hausken, 2006; Fenz, 2011). Rue, Pfleeger ja Ortiz (2007) jakavat taloudelliset tietoturvainvestointimallit kolmeen luokkaan: Kirjanpitomallit, peliteoriaan pohjautuvat mallit ja syöte/tuloste -mallit. Kirjanpitomallit avustavat organisaatiota määrittämään, kuinka paljon organisaation pitäisi käyttää resursseja tietyn informaation suojaamiseksi. Kirjanpitomalleissa (mm. Gordon & Loeb, 2002) investoinnin tuotto lasketaan korkeampana turvallisuutena. Optimaalinen taso investoinnille on piste, jossa lisäinvestoinnin rajahyöty laskee nollaan. Malleissa keskeisin tekijä investoinnin tuoton laskemisen kannalta on uhkatason lasku. Kirjanpitomalli sopii sovellettavaksi ympäristöissä, joissa organisaatiolla on hallussaan informaatiota, jolla on arvoa, ja tarvittavat resurssit suojata sitä (Rue ym., 2007). Sen lisäksi organisaation pitää pystyä määrittämään suojattavan informaationsa arvo, informaation haavoittuvuus ja toimiva laskukaava oikean investointitason laskemiseksi. Kirjanpitomallien ongelmana usein on, että vaikka ne olisivat teoriassa toimivia, niitä on usein hankala soveltaa käytännössä, sillä harvalla organisaatiolla on hallussaan tarvittavaa dataa, saati osaamista mallien hyödyntämisen kannalta. (Rue ym., 2007.) Kaikkiin tilanteisiin kirjanpitomallit eivät muutenkaan sovellu, kuten mm. Willemson (2006) osoittaa.

Soo Hoo (2000) esittelee oman prosessinsa päätöksentekoon ja suosittelee myös asiantuntijoiden analyysin hyödyntämistä sen yhteydessä. Mallissa ehdotetaan vaihtoehtoisten tulevaisuuksien määrittelyä: ensimmäisessä skenaariossa arvioidaan, miten jokin kyberhäiriötilanne (esim. tietovuoto) vaikuttaa organisaation tulevaisuuteen ja toisessa skenaariossa arvioidaan, miten organisaatio olisi pärjännyt ilman kyseistä poikkeamaa. Lähestymistapa eroaa kirjanpitomallien tavasta siten, että tässä lähestymistavassa ei määritetä organisaation datavarannoille arvoa.

Syöte/tuloste -mallilla Rue ym., (2007) viittaavat esimerkiksi tutkijoiden Andrijcic ja Horowitz (2006) esittämään malliin, jossa tutkitaan kyberhyökkäysten aiheuttamia makrotaloudellisia vaikutuksia. Peliteoriaan pohjautuvia malleja esitellään luvussa 3.2.2 Seuraavana esitellään erilaisia investointien tuoton arviointiin ja investointipäätöksen tueksi kehitettyjä menetelmiä.

Perinteiset investoinnin kannattavuuden arviointiin käytetyt menetelmät:
Yksi paljon käytetty tapa arvioida investoinnin hyötyä, on verrata investointia suhteessa mahdollisen tietomurron aiheuttamiin kustannuksiin mm. (Bojanc & Jerman-Blažič, 2008; Gordon & Loeb, 2002b; Hausken, 2006). Tähän voidaan käyttää apuna erilaisia tilastollisia malleja, joiden avulla oletettuja hyötyjä voidaan kvantifioida, kuten sijoitetun pääoman tuottoprosentti (ROI), sisäinen korkokanta (IRR) ja nettonykyarvo (NPV). Kirjanpidon konseptia sijoitetun pääoman tuottoprosentti (ROI) tai sen variaatioita käytetään paljon (Schatz & Bashroush, 2017).

Sijoitetun pääoman tuottoprosentti (ROI) ja sen variaatiot: ROI on toiminnan kannattavuuden mittari. Se on kaava investoinnin tehokkuuden arviointiin vertaamalla investoinnin kustannuksia suhteessa odotettuun hyötyyn. Kaava yksinkertaisesti mittaa, kuinka paljon organisaatio saa investointiin käytetylle rahalle vastinetta. (Bojanc & Jerman-Blažič, 2008.) Mallin hyödyntämisen hankaluutena on oletettujen hyötyjen kvantifiointi.

$$ROI = \frac{\text{investoinnin oletetut hyödyt} - \text{investoinnin kustannukset}}{\text{investoinnin kustannukset}}$$

Odotettu vuosittainen tappio (annual loss expectancy, ALE) ja turvallisuusinvestoinnin tuotto (ROSI): Soo Hoo (2000) käyttää tietotekniikan riskejä arvioidessaan odotetun vuosittaisen tappion määritelmää (annual loss expectancy, ALE). Hän puhuu kvantitatiivisen analyysin puolesta tietoturvainvestointien tarvetta ja määrää arvioitaessa. Variaatio sijoitetun pääoman tuottoprosentista on esimerkiksi turvallisuusinvestoinnin tuotto (ROSI). Turvallisuusinvestoinnin tuottokaavassa investoinnin hyöty lasketaan oletetun vuosittaisen tappion määrästä ilman investointia, erotuksena vuosittaisen tappion määrä investoinnin kanssa (Bojanc & Jerman-Blažič, 2008.):

$$ROSI = \frac{ALE_{ilman\ investointia} - ALE_{investoinnin\ kanssa} - \text{investoinnin kustannukset}}{\text{investoinnin kustannukset}}$$

Muita variaatioita sijoitetun pääoman tuottoprosentista: esimerkiksi Return on Attack (ROA), joka ottaa huomioon hyökkääjän tuotot ja kustannukset (tappiot) (Schatz & Bashroush, 2017).

Nettonykyarvo (NPV): Nettonykyarvo on toiminnan kannattavuuden mittari. Se on kaava investoinnin tulevien kassavirtojen nykyarvon määrittämiseen. Nettonykyarvo soveltuu investoinnin kustannusten ja hyötyjen arvioon pidemmällä aikavälillä, sillä sen avulla voidaan diskontata tulevia kassavirtoja nykyhetkeen. (Bojanc & Jerman-Blažič, 2008.) n = pitoaika, B_t = nettohyötyjen nykyarvo ajanjaksolla t, C_t = kaikki kustannukset, i = sisäinen korkokanta.

$$NPV = \sum_{t=0}^{n} \frac{B_t - C_t}{(1-i)^t}$$

Sisäinen korkokanta (IRR): Sisäistä korkokantaa hyödynnetään usein kuten nettonykyarvoa, pidemmän aikavälin investointien arviointiin. Investoinnin sisäinen korkokanta on se laskentakorko, jolla investoinnin nettonykyarvo on nolla. (Bojanc & Jerman-Blažič, 2008.)

$$\sum_{t=0}^{n} \frac{B_t - C_t}{(1 + IRR)^t} = 0$$

Eri arvonmääritysmenetelmiä voidaan yhdistellä, sillä yksittäin käytettynä mallit eivät sovellu kovin hyvin tietoturvainvestointipäätösten arviointiin (Gordon & Loeb, 2002b; Bojanc & Jerman-Blažič, 2008). Esimerkiksi Bojanc & Jerman-Blažič (2008) yhdistävät mallissaan tässä esitellyt sijoitetun pääoman tuottoasteen (ROI), nettonykyarvon (NPV) ja sisäisen korkokannan (IRR). Gordon & Loeb (2002b) keskustelevat artikkelissaan kyseisten arvonmääritysmenetelmien eroista ja puutteista.

Tukijärjestelmä päätöksentekoon (Decision Support Systems, DSS): Järjestelmällinen tapa ymmärtää ja parantaa päätöksentekoprosessia, pyrkimyksenä tehostaa päätöksentekoa organisaatiossa (Schatz & Bashroush, 2017). Fenz, Ekelhart & Neubauer (2011) kehittivät ohjelmistoratkaisun päätöksenteon tueksi, jonka avulla organisaatio voi arvioida eri tietoturvainvestointien vaikutusta organisaation riskitasoon. Malli auttaa johtoa arvioimaan, mitä he saavat investointinsa vastineeksi ja onko investointi tehokas. Fenz ym., mallin käytettävyyden kannalta etuna on, että ohjelmiston käyttö ei vaadi syvää ymmärrystä tietoturvasta. Fenz ym., (2011) malli huomioi myös investointipäätöksen vaihtoehtokustannukset. Vaihtoehtokustannuksilla tarkoitetaan kustannuksia, jotka syntyvät, kun organisaation pitää valita useiden tavoitteiden välillä: Rajallisten resurssien tapauksessa investointi yhteen tavoitteeseen on pois toisesta tavoitteesta. Tavoitteet voivat myös olla ristiriitaisia. (Fenz ym., 2011.)

Hyödyn maksimointi: Subjekti yrittää maksimoida investoinnista saatavan arvon (Schatz & Bashroush, 2017). Hyödyn maksimointiin perustuvissa malleissa päämääränä on löytää optimaalinen tietoturvainvestoinnin taso suhteessa organisaation uhkaympäristöön ja haavoittuvuuksiin. Jos organisaatio investoi alle tämän optimitason, se johtaa riskitasoon, jota ei voida hyväksyä. Toisaalta optimaalisen investointitason ylittävät investoinnit eivät tuo hyväksyttävää tuottoa investoinnille. (Gordon & Loeb, 2002; Soo Hoo, 2000.) Riskejä välttävän päätöksentekijän tapauksessa tietoturvainvestoinnin maksimikoko kasvaa suhteessa tietovuodon aiheuttamaan potentiaaliseen tappioon, mutta ei koskaan ylitä sitä. Lisäksi edellytetään, että on olemassa potentiaalinen minimitappio, jonka alla optimaalinen investointi on olla investoimatta. (Huang, Hu & Behara, 2008.)

Analyyttinen hierarkisointiprosessi (The Analytic Hierarchy Process, AHP): Analyyttinen hierarkisointiprosessi on järjestelmällinen tapa purkaa monimutkaisia ongelmia pienempiin osiin. Pyrkimyksenä on koostaa ositelluista ongelman ratkaisusta yhtenäinen ratkaisu alkuperäiseen ongelmaan. Bodin, Gordon & Loeb (2005) hyödyntävät AHP-menetelmää: he yhdistävät mallissaan

sekä kvantitatiivisia että kvalitatiivisia tekijöitä. AHP-menetelmää voi hyödyntää itsenäisesti tai yhdessä muiden menetelmien kanssa, mutta se ei korvaa päätöksentekijän roolia. Menetelmän avulla voidaan tehdä järjestelmällistä vertailua eri vaihtoehtojen ja kriteeristöjen välillä (Bodin ym., 2005).

Teoria aidoista vaihtoehdoista (Real Options Theory, ROT): ROT menetelmänä ottaa huomioon investointipäätöksen luontaisen joustavuuden ja esittää keinot sen kvantifioimiseen (Schatz & Bashroush, 2017). Esimerkiksi Tatsumi ja Goto (2010) hyödyntävät tätä menetelmää pohtiessaan tietoturvainvestoinnin optimaalista ajoitusta.

3.2.2 Käyttäytymistaloustieteeseen perustuvat mallit

2000-luvun alun tutkimuksissa on esitetty peliteorian ja erilaisten dynaamisten tekijöiden vaikutukset huomioivia simulointien ym. hyödyntämistä jatkotutkimuksissa (mm. Gordon & Loeb, 2002; SooHoo, 2000). Näin on käynytkin. Mm. Carias ym., (2019), Nazareth & Choi (2015), Behara ym., (2007) hyödyntävät järjestelmädynamiikan mallinnuksen ja simuloinnin tekniikoita. Menetelmän avulla voidaan luoda malli, joka kuvaa reaalimaailman rakennetta, ja simuloida erilaisia skenaarioita; miten investointi kohteeseen A vaikuttaa kohteen houkuttelevuuteen hyökkäyskohteena ja niin edelleen. Anderson ja Moore (2006) kuvaavat yleisellä tasolla tietoturvainvestointien ulkoisvaikutuksia taloudellisesta näkökulmasta.

Peliteoria tutkii strategista päätöksentekoa kilpailu- tai konfliktitilanteissa matemaattisia malleja hyödyntämällä (Schatz & Bashroush, 2017). Myös peliteoriaan pohjautuvissa malleissa tavoitteena on tietoturvainvestointien optimointi (esim. Bistarelli, Dall'Aglio & Peretti, 2006). Malleissa tutkitaan esimerkiksi organisaation valitseman puolustusstrategian vaikutusta muiden osapuolien tekemiseen ja muiden osapuolien strategioiden vaikutusta organisaation omaan tekemiseen. Myös odotukset muiden osapuolien strategioista ovat teoriassa keskeisessä roolissa. Organisaation puolustusstrategiassa huomioidaan muiden osapuolien vaikutus puolustusstrategian toimivuuteen (Schatz & Bashroush, 2017). Malleissa pyritään huomioimaan esimerkiksi riippuvuudet ja korvaavuudet hyökkääjän ja puolustajan ja muiden puolustajien välillä (Schatz & Bashroush, 2017). Tavoitteena on valita puolustusstrategia siten, että se mahdollistaa optimaalisen aseman saavuttamisen suhteessa organisaation asettamiin tavoitteisiin. Esimerkkitilanne: Hyökkääjä haluaa rikkoa järjestelmän (mahdollisimman pienellä vaivalla) ja vastapuolella puolustaja haluaa suojata järjestelmää (minimikustannuksin). Puolustavan organisaation tavoitteena on investoida vastatoimiin juuri sen verran kuin on tarpeellista. Schatz & Bashroush (2017) nostavat peliteoriasta esimerkiksi informaation jakamisen: yritysten on järkevää hyödyntää muiden osapuolien jakamaa tietoturvainformaatiota, mutta ei välttämättä jakaa omaa tietoansa parantaakseen omaa puolustusasemaansa. Tämä voi johtaa vapaamatkustusongelmaan, mikä voi toisaalta muuttaa myös

hyökkääjien hyökkäysstrategioita. Yrityksillä ei ole aina kannustimia toimia oikein, joten myös valtiot yrittävät yhä useammin puuttua tilanteeseen ja ohjata yrityksiä haluamaansa suuntaan. Valtioiden tavoitteena on saada organisaatiot jakamaan yhä enemmän tietoa (työkaluja, tekniikoita, prosesseja) uhkatekijöistä ja vastatoimista organisaatioiden kesken parantaakseen organisaatioiden puolustusasemaa kokonaisvaltaisesti. (Schatz & Bashroush, 2017.) Näin syntyy usean osapuolen välinen dynamiikka, jossa muutos (tai odotus muutoksesta) yhden tekijän strategiassa vaikuttaa kaikkien muiden strategioihin.

Peliteoriaan pohjautuvat mallit sopivat myös esimerkiksi tilanteisiin, joissa järjestelmää ylläpitää ja käyttää joukko yksilöitä, joiden intressit eivät välttämättä kohtaa (Rue ym., 2007). Peliteoriaan pohjautuvien mallien käytännön hyödyntämisessä on myös hankaluutensa, sillä mallit olettavat usein täydellistä informaatiota, mikä ei ole kovin realistista. Ei ole myöskään selvää, voidaanko kaikkia tilanteita edes kuvata yhden systeemin kautta, kuten malli edellyttää. (Rue ym., 2007).

3.2.3 Vaihtoehtoiset lähestymistavat

Taloudellisessa näkökulmassa on rajoitteensa, kuten edellä on esitetty. Tietoturvainvestoinnin arviointi tuotto-odotuksen avulla on usein hankalaa, sillä investointi tietoturvaan harvoin tuottaa mitään suoraan kassavirtoja lisäävässä muodossa (Schatz & Bashroush, 2017). Tietoturvainvestoinnin tuotto ei muodostu kasvaneista tuotoista tai laskeneista kustannuksista, vaan tietoturvariskien vähentymisestä (Huang ym., 2008). Toisaalta välilliset hyödyt voivat olla myös suoraan kustannuksia laskevia (esim. tietoturvasertifiointi, joka voi vaikuttaa vakuutusten hintaan alentavasti (Low, 2017). Tietoturvainvestointeja on tutkittu myös muista näkökulmista.

Dor ja Elovici (2016) tutkivat tietoturvainvestointeihin liittyvää päätöksentekoprosessia. Organisaatiorakenteella ja prosesseilla on merkitystä tietoturvainvestointien kannalta. Ne vaikuttavat esimerkiksi organisaation kyvykkyyksiin riskienhallinnan saralla, tietoturvajohtajan (CISO) käyttäytymiseen, ja organisaation kykyyn käsitellä uhkia. Dor ja Elovici kehittivät konseptuaalisen mallin tietoturvainvestointeihin liittyvästä päätöksentekoprosessista. Malli koostuu 14 vaiheesta (mm. uhkaympäristön analysointi, tietoturvan nykytila, vaihtoehtojen analysointi jne.) päätöksentekoprosessissa ja 16 konseptista (mm. strategia, rajoitteet, riskienhallinta, kilpailuetu jne.). Kaikki 16 konseptia sekä vaikuttavat että reagoivat näihin 14 vaiheeseen. Organisaatioilla on erilaisia käytäntöjä ja tapoja tietoturvainvestointipäätösten suhteen, ja ne käyttäytyvät eri tavoin investointiprosesseissaan. Useissa tapauksissa päätöksentekoprosessille ei voida asettaa selkeitä rajoja, ja vaikka prosessi yleisellä tasolla näyttäisi sisältävän eri vaiheita, vaiheet eivät ole välttämättä jatkuvia. Myös eri sidosryhmien agendat ja rajoitteet yhtä lailla vaikuttavat päätöksentekoon. (Dor & Elovici, 2016.) Tietoturva-alan ammattilaisella on usein hyvin eri näkemys riskeistä kuin tietoturva-asioihin ei niin perehtyneellä, alan ulkopuolisella henkilöllä.

Moore ym., (2015) tutkivat organisaatioiden tapaa hallita ja priorisoida kyberriskejä sekä motiiveja investointipäätösten taustalla. He havaitsivat, että johdon tuki on yksityisellä sektorilla jo melko korkealla, ja yrityksissä ollaan valmiita investoimaan tietoturvaan resursseja. Pullonkaulaksi nousi rahan sijasta pikemminkin henkilöresurssien riittämättömyys ja vaikeus rekrytoida asiantuntijoita. Laskeva riskitaso oli korkein motivaatiotekijä tietoturvainvestoinnin takana. (Moore ym., 2015.)

Investointeja priorisoitaessa organisaatioissa hyödynnetään yleisesti viitekehyksiä päätöksenteon tukena (Moore ym., 2015). Viitekehyksiä oli laidasta laitaan (tunnettuja viitekehyksiä kuten ISO ja NIST sekä sisäisesti kehitettyjä omia viitekehyksiä tai useiden viitekehysten yhdistelmiä). Päätöksentekoprosessit ovat kuitenkin Weishäupl ym., (2018) mukaan harvoin standardisoituja. Heidän mukaansa päätöksenteossa ei juuri hyödynnetä akateemisen kirjallisuuden esittämiä investointimalleja ja standardisoituja päätöksentekoprosesseja. Maakohtaisessa sääntelyssä on eroja, joten on mahdollista, että yhdysvaltalaiset yritykset (Moore ym., 2015 tutkimuksen kohderyhmä) ovat tietoturvaan liittyvässä päätöksenteon standardisoinnissa eurooppalaisia vastinparejaan (Weishäupl ym., 2018 tutkimuksen kohderyhmä) edellä tai ero on puhdasta sattumaa.

Moore ym., (2015) toteavat, että organisaatioiden käyttämät mittarit painottavat usein prosessia lopputuloksen sijasta. Eli budjetointipäätöksiä ei tehdä kvantitatiivisin menetelmin laskemalla esimerkiksi tuottoa investoinnille (ROI). Pääpaino on aukkojen täyttämisessä organisaation nykytilan ja tavoitellun aseman välillä (tietoturvan kannalta). Organisaatioissa keskitytään huomattavasti vähemmän yksittäisen investointipäätösten kustannusten ja hyödyn mittaamiseen. Asioita katsotaan kokonaisuutena prosessien kannalta. Eri sektoreiden välillä ei ollut muutamaa poikkeusta lukuun ottamatta merkittäviä eroja lähestymistavassa kyberriskeihin. Tietoturvatiedon jakaminen organisaatioiden kesken oli yleistä. Organisaatiot jakoivat tietoa keskenään sekä hankkivat tietoa uhista kolmansilta osapuolilta.

Heidt ym., (2019) loivat konseptuaalisen mallin tietoturvaan liittyvästä päätöksenteosta, jossa kontekstisidonnaiset tekijät ovat merkittävässä roolissa. Pk-yritysten kontekstissa seuraavat asiat nousivat esiin: Päätöksentekijät ovat vahvasti sidoksissa ympäristöönsä, ja saavat sieltä vaikutteita. Ympäristöllä, yksilöllisillä luonteenpiirteillä ja organisaation ominaispiirteillä - etenkin resurssien rajallisuudella (budjetti, työvoima, aika, osaaminen) – on merkittävä vaikutus. Nämä tekijät vaikuttavat siihen, että taloudellisia työkaluja ja metodeja, kuten ROI-laskelmia, on usein vaikea hyödyntää yrityksissä käytännössä, vaikka pk-yrityksen johto olisikin niistä tietoinen; ajan, rahan ja datan puutteen vuoksi.

Suurimmassa osassa pk-yrityksistä ei ole käytössä IT-budjetointia (ml. tietoturva) lainkaan. Tietoturvainvestoinnit nähdään ylimääräisinä kuluina, joista ei ole juuri näkyvää hyötyä. Päätöksentekoprosesseissa on mukana kustannukset, mutta ei hyötyä; kustannus-hyöty laskelmat ovat siis usein lähinnä kustannuslaskelmia, joiden perusteella päätöksiä tehdään. Lopulliset investointipäätökset perustuvat harvoin perinpohjaiseen analyysiin

tai ”numeroiden murskaamiseen” vaan useimmiten melko pintapuoliseen arvioon. (Heidt ym., 2019.) Investointien arviointia varten ei ole olemassa prosesseja tai mittareita juuri missään yrityksessä, ja oppiminen tapahtuu usein lähinnä ad hoc -pohjalta (Weishäupl ym., 2018).

Cavusoglu ym., (2015) tunnistivat tutkimuksessaan seuraavat tekijät, joilla oli merkittävä vaikutus yritysten tietoturvainvestointipäätöksiin: Normatiivinen paine (esim. paine liikekumppaneilta) ja pakottava tarve (lainsäädännön asettamat vaatimukset) Tutkimuksessa havaittiin myös, että yritysjohto investoi todennäköisemmin tietoturvaan, mikäli sillä on hyvä ymmärrys yrityksen tietoturvatarpeista ja olemassa olevat toimivat riskienhallintaproseduurit.

3.3 Muita tietoturvainvestointeihin vaikuttavia tekijöitä

Heidt ym. (2019) nostavat esiin eri rooli-identiteettien merkityksen päätöksenteossa (esim. toimitusjohtaja on samalla omistaja ja vastaa IT-päätöksistä). Rooli-identiteettien on osoitettu vaikuttavan päätöksentekoon (mm. Mathias & Williams, 2017).

Ympäristölliset tekijät, kuten asiakasvaatimukset ja säännölliset laaduntarkastukset nousivat esiin. Ne pakottivat yrityksiä omaksumaan tiettyjä datan suojauskäytäntöjä ja palautumisprosesseja tai vaihtoehtoisesti kehittämään omat tietoturvaprosessinsa- ja käytäntönsä (Heidt ym., 2019). Valtion asettama sääntely vaikuttaa, sillä se toimii usein lähtökohtana alkuperäiselle investontitarpeelle ja määritti yritysten investointikohteen ja investoinnin rajat (Weishäupl ym., 2018). Weishäupl ym., (2018) havaitsivat, että yrityksen ulkoinen ympäristö ja teollisuudenalasta riippuvaiset tekijät (lainsäädäntö, teollisuudenalan sääntely, yhteistyökumppanien vaatimukset) ovat usein pääajuri tietoturvainvestointipäätösten takana. Esimerkiksi vuonna 2018 voimaantulleella EU:n yleisellä tietosuoja-asetuksella (GDPR) on ollut työntävä vaikutus organisaatioiden tietoturvainvestointipäätöksiin. Sanktioiden pelossa yritykset ovat kokeneet tietoturvaan panostamisen pakolliseksi (Heidt ym., 2019).

Puolueellinen muotoilu: Beebe (2014) tutki puolueellisen muotoilun vaikutusta investointipäätöksiin prospektiteorian pohjalta. Hän havaitsi, että päätöksentekijät eivät aina toimi rationaalisesti, vaan valintatilanteen asettelulla on vaikutusta lopputulemaan. Prospektiteoriassa (Kahneman & Tversky, 1979) on havaittu, että riskin sisältäviä päätöksiä tehdessään yksilöt päätyvät usein välttämään riskejä, jos valinta on tehtävä voitollisten vaihtoehtojen väliltä. Tappiollisista vaihtoehdoista valitessaan yksilöt toimivat päinvastoin. He päätyvät useammin valitsemaan riskipitoisemman vaihtoehdon, jos vaihtoehdot on muotoiltu tappioina. Beebe (2014) vahvisti teorian toimivuuden myös tietoturvainvestointien kontekstissa.

Laumakäyttäytyminen: Päätöksenteon motiiveja eri tietoturvainvestointien takana on toistaiseksi tutkittu vähemmän kuin investointien taloudellista optimointia, mutta mm. (Shao, Siponen, & Pahnila, 2019) ovat kiinnostuneita

näistä laadultaan hankalasti mitattavista olevista motiiveista. Vertaisten käyttäytymisellä on vaikutusta organisatoriseen päätöksentekoon (Heidt ym., 2019). Shao (2015) ja Shao ym. (2019) havaitsivat tutkimuksessaan, että tietoturvajohtajat päätyvät hyvin usein seuraamaan asiantuntijoiden suosituksia, parhaita käytänteitä ja muiden organisaatioiden käytäntöjä investointipäätöstensä tukena. Laumakäyttäytyminen on tietoturva-asioissa tyypillistä, sillä johtajat ottavat hyvin usein mallia aikaisista omaksujista investoidessaan esimerkiksi uuteen teknologiaan. Maineeseen perustuvan laumateorian (reputational herding theory) mukaan, jos investointipäätöksestä vastuussa oleva johtaja on epävarma omasta kyvystään tehdä päätös, muiden seuraaminen on hyvä valinta. Teorian kannalta seuraavat kaksi komponenttia ovat olennaisia: 1) investoinnin arvossa on arvaamattomia tekijöitä 2) älykkäät johtajat tekevät samanlaisia päätöksiä. Mikäli investointipäätös osoittautuu epäonnistuneeksi, investointipäätöksen tehnyt johtaja ei ole yksin tulilinjalla. (Shao ym., 2019).

Johdon asenteet ja ennakkoluulot: Puutteellinen ymmärrys sekä johto- että työntekijätasolla on organisaatioiden suurimpia esteitä hyvällä tasolla olevan tietoturvan saavuttamisen kannalta. Ylimmän johdon tuki on tärkeä organisaation turvallisuuskulttuurin kehittämisen ja valvonnan kannalta. Tuen puutteen vaikutus on kaksiosainen; yhtäältä organisaatio on vähemmän suvaitseva hyviä turvallisuuskäytänteitä kohtaan ja toisaalta olemassa olevien menetelmätapojen toteutumista seurataan vähemmän (Knapp ym., 2006). Yritysten johdon täytyy ymmärtää organisaatioidensa haavoittuvuus, jotta ne ylipäätään lähtevät ajamaan järjestelmiensä suojausta ja kehittämään tarvittavia tietoturvakäytänteitä. (Rhee, Ryu & Kim, 2012.) Johdon tietämättömyys riskeistä korostui menneinä vuosina (mm. Straub & Welke, 1998), mutta viime vuosina kehitystä on tapahtunut parempaan suuntaan. Straub ja Welke (1998) keskeinen havainto oli, että johtajilla ei ollut keskimäärin riittävästi tietoa siitä, miten tietojärjestelmiä tulisi suojata ja mitä he voivat tehdä riskejä pienentääkseen. Nykyisin tilanne on erilainen. Eri konsulttiyhtiöiden toteuttamista raporteista voidaan havaita selkeä trendi siihen suuntaan, että yhä useammassa organisaatiossa tietoturva on noussut ylimmän johdon asiaksi (mm. KPMG, 2017; Microsoft & Marsh, 2019). Rhee, Ryu & Kim (2012) toteavat, että organisaation johdon täytyy ymmärtää tarve kontrolleille ja turvakeinoille, jotta he toteuttavat niitä käytännössä. Tähän liittyy, että heidän täytyy siis ymmärtää oma haavoittuvuutensa. Toimitusjohtajat tuskin ovat useimmissa tapauksissa itse erityisen hyvin perillä tietojärjestelmien suojauksesta, mutta he kantavat vastuun riskeistä, joten organisaatioihin on palkattu tietoturva-asiantuntijoita ja kyberriskeihin suhtaudutaan vakavasti. Raporteista voidaan havaita, että tietoisuus riskeistä on kasvanut, mutta varautuminen riskeihin on yhä monilta osin puutteellista.

Psykologiset harhat ja heuristiikat: Toisin kuin rationaalisen valinnan teoriassa oletetaan, päätöksentekijät eivät usein tiedosta kaikkia turvallisuusriskejä ja vaihtoehtoisia varautumiskeinoja riskeihin. Päätöksentekoprosessi ei ole immuuni ei-taloudellisille tekijöille, jotka

vaikuttavat päätöksentekoon. Johdolla ei ole tietoturvainvestointien tapauksissa koskaan hallussaan täyttä informaatiota. Päätös perustuu aina epätäydelliseen informaatioon, joka rajoittaa investointipäätöksen mahdollisuuksia onnistua (Cavusoglu, 2010.) Nk. rajoitettu rationaalisuus (bounded rationality) on Simonin (1955) esittämä konsepti, joka kuvaa päätöksentekijän sisäsyntyisiä rajoja käsitellä (vastaanottaa, tallentaa, palauttaa ja siirtää) monimutkaisiin ongelmiin liittyvää informaatiota. Kognitiiviset tai psykologiset harhat voivat nousta esiin päätöksenteossa, jos päätöksentekijä sortuu ”kognitiivisiin oikoreitteihin” tai päätöksentekijään vaikuttaa systemaattisesti erilaiset psykologiset vinoumat. Nämä harhat voivat vaikuttaa merkittävästi tehtyihin päätöksiin. (Cavusoglu, 2010.)

Ihmisillä on taipumusta uskoa monissa negatiivissa tilanteissa, että riski on heidän itsensä kohdalla pienempi kuin muilla, nk. *optimistinen harha* (Weinstein & Klein, 1996). Syitä voi olla esimerkiksi, että henkilöillä ei ole kykyjä arvioida riskejä tarpeeksi hyvin tai henkilö on motivoitunut aliarvioimaan riskin esiintymisen todennäköisyyttä ja sen vaikutusta. (Weinstein & Klein, 1996.) Yksilöt eivät usko, että negatiivisia tapahtumia ei välttämättä tapahtuisi ollenkaan, vaan enemminkin he uskovat, että nämä ovat suhteellisen epätodennäköisiä heidän kohdallansa. Tietoturvakäytänteet ym. ovat suunnattu organisaatiossa muille henkilöille kuin yksilölle itselleen. (McKenna, 1993.) Johto voi sivuuttaa tai aliarvioida riskin vakavuuden, jos he eivät kunnolla ymmärrä sitä. Hypoteettiset vaarat usein sivuutetaan ennen kuin riski realisoituu (Cavusoglu, 2010).

Rhee ym., (2012) havaitsivat, että johtajat arvioivat omat tietoturvariskinsä huomattavasti alemmaksi kuin vertailukumppaniensa riskit. Toisin sanoen, oli tyypillistä, että johto koki, että heidän oman organisaationsa kohdalla sama riski on pienempi kuin muilla. Johtajat näyttävät siis ymmärtävän tietoturvariskien todellisuuden, mutta kokevat silti olevansa niiltä suojassa, ikään kuin eri todellisuudessa. Tulosten perusteella näyttäisi siltä, että johtajat kokevat haavoittuvuuksiensa olevan yhteydessä heidän liikekumppaneihinsa, mutta samalla uskovat, että heidän mahdollisuutensa kontrolloida näitä haavoittuvuuksia olisi silti yrityksen omissa käsissä, itsenäisesti hallittavissa. (Rhee ym., 2012.)

Cavusoglu (2010) listaa erilaisia harhoja ja heuristiikkoja, jotka voivat vaikuttaa tietoturvapäätöksiin organisaatiossa. *Epäselvyys-efekti* (ambiguity effect): Päätöksentekijät voivat jättää huomiotta informaation, jota on vaikea omaksua. Päätöksentekijät voivat esimerkiksi tehdä päätöksen olla investoimatta teknologiaan, jossa investoinnin mahdollisuus onnistua esitetään haitarina yksittäisen arvon sijaan.

Simulaatioheuristiikat (simulation heuristic): Epätodennäköiset riskit on helppo sivuuttaa, koska yksilöiden on vaikea kuvitella niiden toteutuvan. Ja yhtä lailla, vaikka epätodennäköinen riski sattuisi realisoitumaan, ihmisten on helppo sivuuttaa se poikkeustapauksena, johon ei ole tarvetta myöhemmin enää reagoida.

Rationaalinen sivuuttaminen (rational ignorance): Päätöksentekijän äärimmäinen välinpitämättömyyden muoto. Tilanteissa, joissa päätöksentekijän saatavilla on runsaasti informaatiota, päätöksentekijä voi tehdä tietoisen valinnan jättää riski kokonaan huomiotta tai tehdä päätöksen perustuen vain osaan saatavilla olevasta informaatiosta. Näin voi käydä esimerkiksi tilanteissa, joissa päätöksentekijä kokee, että hyöty saatavilla olevaan informaatioon paneutumisesta on pienempi kuin siihen uhrattava vaivannäkö.

Ankkurointi (anchoring): Päätöksenteon harha, jossa päätöksentekijä painottaa vahvasti tiettyä informaatiota. Ankkurointiharha voi aiheuttaa vakavia ongelmia tietoturvakontekstissa, vääristäessään päätöksentekijän kokonaiskuvaa.

Hyberbolinen diskonttaus (hyberbolic discounting): Ihmisillä on taipumus painottaa välittömiä hyötyjä enemmän kuin pidemmän ajan hyötyjä, mutta vaikutus heikkenee ajan kuluessa. Tämä harha korostuu yrityksissä, jotka toimivat tiukan budjettiraamin rajoissa. Useat tietoturvariskien laskemiseen tähtäävät toimenpiteet vaativat alkuinvestointia, mutta investoinnin hyödyt ilmenevät vasta pitkällä aikavälillä.

Positiivisen lopputuleman harha (positive outcome bias): Päätöksentekijöillä on taipumusta yliarvioida suotuisten lopputulemien todennäköisyys. Yrityksen johto voi esimerkiksi perustella päätöksen olla investoimatta tietoturvaan toteamalla, että nykyiset (puutteelliset) ratkaisut ovat toimineet tähänkin asti. Positiivisen lopputuleman harha on erityisen vaarallinen tietoturvakontekstissa, jos päätöksentekijät eivät tiedosta kaikkia riskejä ja tekevät päätöksiä perustuen virheellisin oletuksiin.

Liiallinen itseluottamus (overconfidence): Tarkoittaa taipumusta uskoa liiaksi omiin kykyihin suhteessa todellisuuteen. Tietoturvakontekstissa liiallinen itseluottamus saattaa johtaa ali-investointiin, kun päätöksentekijät uskovat ilman todisteita, että heidän organisaatiossaan tietoturva ja varautuminen riskeihin on paremmalla tasolla kuin muissa organisaatioissa.

Vahvistusharha (confirmation bias): Ihmisillä on taipumus etsiä omia oletuksia vahvistavaa informaatiota ja sivuuttaa ristiriitainen informaatio. Vahvistusharha voi yhdessä liiallisen itseluottamuksen kanssa aiheuttaa vakavia tietoturvaongelmia organisaatiossa, jos päätöksentekijöiden kuvitelmat eivät vastaa todellisuutta.

Organisaatiokulttuuri ja riskinottohalukkuus: Organisaatiokulttuuri on merkittävässä roolissa (Hu ym., 2012). Organisaatiokulttuuri vaikuttaa, miten ja mihin tietoturvakontrolleihin yritys investoi. Individualistisessa organisaatiokulttuurissa ollaan valmiita ottamaan enemmän riskiä. Jos kontrollit tai prosessit vahingoittavat yksilön autonomiaa (liikkumavaraa), he ovat vähemmän halukkaita noudattamaan sääntöjä (Mars, 1996). Oikopolkujen keksiminen, materiaalien hyödyntäminen omaan käyttöön, sääntöjen rikkominen ja huijaaminen on tyypillistä yksilökeskeisessä maailmankuvassa. Individualistisessa organisaatiokulttuurissa yksilöt hyödyntävät epäselvyyksiä säännöissä, jättävät noudattamatta prosesseja (oikoreittien keksiminen) prosessin sujuvuuden vuoksi ja valitsevat useammin lyhytaikaisen

henkilökohtaisen hyödyn, mahdollisia organisaatiolle koituvia pitkän ajan seurauksia pohtimatta. Individualistiset taipumukset ovat myös yhteydessä korkeampaan riskinottoon. (Mars, 1996.)

On jo pitkään tiedetty, että kokonaisvaltaisen tietoturvan saavuttamisen kannalta, investointi teknologiaan ei yksinään riitä. Tästä syystä myös loppukäyttäjien turvallisuuskäyttäytymistä seurataan, ja aiheesta julkaistaan tutkimuksia. Loppukäyttäjillä voi olla hyvin eriäviä näkemyksiä siitä, mikä on turvallista käyttäytymistä. Turvallisuuskäytännöt koetaan usein hankalina ja aikaa vievinä, ja käytänteiden koetaan hidastavan muita liiketoimintaprosesseja (Weishäupl ym., 2018). Loppukäyttäjien asenteisiin liittyvissä tutkimuksissa eri kannustin- ja rankaisumenetelmien on havaittu olevan tehokkaampia kuin toisten. Esimerkiksi sillä on suuri merkitys, kuinka todennäköisesti työntekijä uskoo jäävänsä kiinni tietoturvakäytäntöjen noudattamatta jättämisestä (Herath & Rao, 2009). Vertaisten käyttäytyminen ja muut sosiaaliset paineet vaikuttavat loppukäyttäjän käyttäytymiseen (Herath & Rao, 2009). Johdon toimintatavat, valvontakäytänteet- ja menetelmät sekä kollegoiden yhteydenpito ja keskustelu (socialization) ovat positiivisesti yhteydessä työntekijöiden näkemykseen organisaation ”tietoturvailmapiiristä”. Työntekijöiden positiivisella näkemyksellä organisaation ”tietoturvailmapiiristä” sekä usko omiin kykyihinsä, on positiivinen vaikutus tietoturvakäytänteiden seuraamiseen. (Chan, Woon & Kankanhalli, 2005.) Myös loppukäyttäjän näkemyksellä siitä, kuinka vaikuttavia hän uskoo omien toimiensa olevan, on suuri vaikutus siihen, miten käyttäjä seuraa organisaation tietoturvakäytänteitä (Hu ym., 2012). Vaikka organisaatiolla on käytänteet ja proseduurit, monet työntekijät ja ulkopuoliset alihankkijat usein laiminlyövät niitä tietoisesti tai tahattomasti (Herath & Rao, 2009).

Ihmiset suhtautuvat riskeihin eri tavoin. Käyttäjät arvioivat riskejä henkilökohtaisen vastuun kautta (mitä minulle tapahtuu, jos jään kiinni tms.). Tietoturva-asiantuntijoille on luontaista suhtautua riskeihin pahinta mahdollista skenaariota pohtimalla. Päätöksentekijät ovat joko riskinottajia, riskiä vältteleviä tai jotain sieltä väliltä. (Karyda ym., 2006). Yritykset, jotka pärjäävät keskimääräistä paremmin usein kaihtavat riskejä (Huang ym., 2008). Riskiaversio on käyttäytymistaloustieteellinen malli inhimillisestä päätöksenteosta epävarmuuden vallitessa (Kahneman & Tversky, 1979). ”Riskiaversiiviset” päätöksentekijät ovat halukkaampia investoimaan tietoturvaan laskeakseen yrityksen riskitasoa, mutta samaan aikaan he eivät kuitenkaan näe kaikkia riskejä suojautumisen arvoisina (Huang ym., 2008).

3.4 Tietoturvainvestoinnin haasteet

IT-investointien arvon määrittäminen on hankalaa, sillä IT-investoinneille on luonteenomaista pitkät takaisinmaksuajat, epävarmuus ja jatkuvasti muuttuva liiketoimintaympäristö (Bardhan, Sougstad & Sougstad, 2004). Investoinneilla turvallisuuteen on usein taipumus näyttää ylimääräisiltä kustannuksilta,

huolimatta siitä toimivatko ne (investoinnin arvo kyseenalaistetaan, jos mitään ei tapahdu) vai ei (investoinnista huolimatta meidän järjestelmiimme hyökättiin) (Schatz ja Bashroush, 2017).

Tietoturvaympäristön muutostahti on kova: uhkat ja uhkiin liittyvät strategiset vastatoimet vaihtuvat säännöllisesti. Muuttuva ympäristö vaikuttaa myös aikaisempien investointimallien ja viitekehysten oletuksiin (Dor & Elovici, 2016). Mallit ja viitekehykset vanhentuvat ja muuttuvat tarpeettomiksi, kun ne eivät enää tarjoa apua päätöksentekoon. Mallien hyödyntämisessä on myös muita ongelmia. Pettigrew (2014) toteaa, että suuri osa organisaatioista ei hyödynnä malleja, koska kokevat ne liian monimutkaisiksi tai mallit eivät sovellu hyvin käytäntöön.

Sopivien vastatoimien määrittäminen on monimutkainen prosessi, joka perustuu arvioihin ja oletuksiin. Miten perustella tietoturvainvestoinnin kustannustehokkuus ja hyöty, kun parhaassa tapauksessa mitään ei tapahdu? Miten määrittää optimaalinen tietoturvaan investoitava määrä? Tietoturva-asiantuntijan pitää osata kääntää tunnistetut riskit taloudellisiksi kaavoiksi osoittamalla niiden arvo ja tarpeellisuus suhteessa muihin investointeihin, jotta investointipäätös voidaan hyväksyä (koska ne kilpailevat samasta potista rahaa). (Schatz ja Bashroush, 2017.) Tietoturvainvestointien arviointi ja mittaaminen on liiketoiminnan ongelma, joka pitää huomioida myös strategisella tasolla. Informaatioresurssien turvaaminen on sekä teknologian hyödyntämistä että ihmisten johtamista (sovitut tietoturvakäytänteet, sääntöjen noudattaminen, tehtävään soveltuvat laitteistot ja ohjelmistot jne.) (Dor & Elovici, 2016.) Ilman kunnollista suunnitelmaa, odottamaton tietoturvapoikkeama voi aiheuttaa vakavaa vahinkoa organisaation informaatioresursseille ja omaisuudelle. Tietoturvainvestointien arvon määrittäminen on kuitenkin hankalaa, sillä ei ole helppo luoda sopivaa kriteeristöä, joilla arvioida investointeja. Tietoturvapoikkeamien todellisten kustannusten arviointia hankaloittaa sekä datan kvantifioinnin vaikeus että tarvittavan datan puute. (Arora ym., 2004).

Mikään määrä investointeja ei estä kaikkia hyökkäyksiä ja täydellinen haavoittumattomuus on mahdotonta (Nazareth & Choi, 2015; Arora ym., 2004). Korkeilla tietoturvainvestointitasolla lisäinvestoinnit eivät enää laske onnistuneiden hyökkäysten määrää. Ne ovat silloin ylimääräisiä kustannuksia ilman todellista hyötyä.

Moore ym. (2015) osoittavat ristiriidan päätöksentekijöiden korkean itseluottamuksen ja yhä yleisten korkean profiilin tietomurtojen välillä: Tietoturvainvestointipäätöksiin osallistuvilla henkilöillä on usein voimakas luotto viitekehyksiin, ja omiin kykyihinsä tunnistaa ja implementoida parhaat kontrollit tietoturvan parantamiseksi omassa organisaatiossaan. Siitä huolimatta korkean profiilin tietomurtojen määrä ei näytä juuri laantumisen merkkejä. Moore ym. epäilevät, että ristiriita saattaa johtua liiallisesta luottamuksesta prosessiperusteisiin mittareihin sen sijaan että organisaatiossa keskityttäisiin varmistamaan (tieto)turvallinen lopputulema.

Kumppaniverkostot ovat monella organisaatiolla laajoja ja monimutkaisia: resursseja ja dataa jaetaan verkoston kesken, jolloin verkosto on

yhtä vahva kuin sen heikoin lenkki. Keskinäisten osapuolien haavoittuvuus vaikuttaa tarvittavien tietoturvainvestointien määrään (Tanaka, Matsuura & Sudoh, 2004). Tanaka ym., (2004) tutkivat, kuinka paljon tietoa tulisi jakaa kumppaniverkoston sisällä. Verkoston kesken jaetun datan suojaaminen on ongelmallista, sillä tilanne mahdollistaa vapaamatkustuksen. Heidän mukaansa tietoturvainvestointeja tulee vaatia kaikilta osapuolilta, mutta haasteena on, että tehtyjä investointeja on kuitenkin vaikea vahvistaa organisaation ulkopuolelta. Liu ym., (2011) ehdottavat, että verkostossa olisi hyvä olla yhteinen koordinoiva osapuoli, joka varmistaa, että investoinnit ovat tasapainossa. Tiedon jakaminen osapuolien kesken on hyödyllistä, sillä se laskee turhien investointien määrää. Liu ym., (2011) huomauttavat, että tietoturvaratkaisuiden toimittajat (tietoturvayritykset) saattavat tietyissä tilanteissa hyödyntää tiedon jakamattomuutta, sillä ne voivat myydä enemmän tietoturvatuotteita kuin olisi tarpeen verkoston suojaamiseksi.

3.5 Erilaisia investointityyppejä

Kaikkia mahdollisia vahinkoja ei voida estää, joten yrityksen on huomattavasti edullisempaa hyväksyä osa mahdollisista kyberhyökkäyksen aiheuttamista vahingoista kuin yrittää estää kaikki. Tietoturva-aktiviteetteja voidaan verrata muihin organisatorisiin prosesseihin, jotka eivät tuota voittoa, mutta ovat siitä huolimatta organisaation toiminnan kannalta äärimmäisen tärkeitä tukitoimintoja (Arora ym., 2004). Useimpien tietoturvainvestointien ja kontrollien implementoinnin pääajurina toimii uhat ja hyökkäykset (Nazareth & Choi, 2015). Organisaation houkuttelevuus hyökkäyskohteena määräytyy sen oletetun arvon ja oletettujen turvamekanismien suhteen - Organisaatiolla on suurempi riski joutua hyökkäyksen kohteeksi, jos hyökkääjä olettaa sen olevan helppo kohde (Nazareth & Choi, 2015). Organisaation sisäisten ja ulkoisten prosessien välille ei voida asettaa selkeitä rajoja – tietoturva on sidoksissa organisatorisiin ja sosiaalisiin prosesseihin (Behara, Huang & Hu, 2007). Monet tietomurrot tapahtuvat useiden tekijöiden vuorovaikutuksessa. Osaa tekijöistä organisaatio voi hallita, osaa ei.

Organisaatioiden tietoturvasta vastaavalla johdolla on laaja valikoima mahdollisia vastatoimia (mm. havaitsemiskyky, ennaltaehkäisevät- ja ohjaavat kontrollit, palautumiskyky ja estäminen) (Nazareth & Choi, 2015). Vastatoimet voidaan jakaa myös proaktiivisiin ja reaktiivisiin menettelytapoihin (Hamill, Deckro & Kloeber, 2005). Cavusoglu ym., (2015) erittelevät kolme tietoturvakontrollityyppiä (tietoturvateknologiat, pätevä tietoturvahenkilöstö ja henkilöstön tietoturvatietoisuuden taso), joihin organisaatio voi investoida.

Kaikki tietoturvainvestoinnit eivät ole yhtä tehokkaita taloudellisesta perspektiivistä (Nazareth & Choi, 2015). Asiantuntijat tyypillisesti uskovat, että kaikista tärkein tietoturvainvestointi on investointi teknologiaan (Carias ym., 2019). Beharan ym., (2007) mukaan organisaation on tehokkaampaa investoida tasaisesti useaan erilaiseen tietoturvakontrolliin, sen sijaan, että se keskittyisi

ensisijaisesti teknisiin kontrolleihin, kuten havaitsemiskykyyn (intrusion detection) ja haavoittuvuuksien paikkaamiseen. Nazarethin ja Choin (2015) mukaan tehokkaimpia kontrolleja ovat investoinnit havaitsemis- ja estämiskykyä parantaviin työkaluihin (esim. virustentorjuntaohjelmat, tunkeutumisen havaitsemisjärjestelmät ja palomuurit), sillä ne johtavat pienempään määrään onnistuneita hyökkäyksiä (Nazareth & Choi, 2015). Hyökkäyksiä voidaan vähentää myös paikkaamalla haavoittuvuuksia ja vahvistamalla organisaation tietoturvallisia käytäntöjä. Investoinnit palautumiskykyyn taas eivät näy laskevana hyökkäysten määränä, vaikka ovatkin äärimmäisen tarpeellisia. (Nazareth & Choi, 2015.) Investoinnit ohjaaviin ja ennaltaehkäiseviin käytänteisiin (engl. deterrence) ovat vähemmän tehokkaita kuin investoinnit teknologiaan (Nazareth & Choi, 2015). Ennaltaehkäisevillä kontrolleilla on monta muotoa. Ne ovat esimerkiksi tietoturvakäytäntöjen muotoilua ja proseduureja hyökkäysten määrän vähentämiseen ja hyökkääjien tunnistamiseen (Nazareth & Choi, 2015).

Investointi henkilöstön tietoturvakoulutukseen kuuluu ohjaaviin ja ennaltaehkäiseviin aktiviteetteihin. Yrityksen henkilöstö on yrityksen ensimmäinen puolustuslinja, joten tietoturvakoulutukseen panostaminen on järkevää. Ihmiset vaikuttavat kahdella tavalla: he aiheuttavat tietovuotoja ja tekevät riskisiä päätöksiä, jotka vaikuttavat organisaation mahdollisuuksiin vastata uhkiin (Kotulic & Clark, 2004). Rhee, Ryu & Kim (2012) toteavat, että paras keino vastata esimerkiksi optimistisen harhan aiheuttamiin harhakuvitelmiin, on tietoturvatietoisuuden kasvattaminen organisaatiossa. Organisaatioissa tarvitaan systemaattista lähestymistapaa tietoturvauhkiin varautumisessa (Rhee ym., 2012). Useimmat ohjaavat keinot edellyttävät työntekijöiden sitoutumista, mikä on harvoin itsestäänselvyys ja laskee sen vuoksi investointien tehoa. Tietoturvakäytänteiden määrittely on turhaa, jos niitä ei noudateta. Organisaation henkilöstön olisi hyvä ymmärtää Melara ym., (2003) mukaan seuraavia asioita:

- Miten järjestelmä toimii (tai miten sen pitäisi toimia)
- Mitä riskejä tietojärjestelmään liittyy
- Kolme näkökulmaa, joista turvallisuus muodostuu (luottamuksellisuus, koskemattomuus, saatavuus)
- Jokaisen työntekijän oma rooli järjestelmän suojaamisessa
- Lainsäädännölliset seuraukset tarkoitushakuisista järjestelmän tai yrityksen omistaman datan väärinkäytöksistä (yleensä toimiva keino sisäpiirin rikkomuksia vastaan)
- Työkalut ja mittarit, joita henkilöstön oletetaan sitoutuvan käyttämään

Organisaatio voi investoida myös esimerkiksi tietoturvavakuutuksiin tai tietoturvasertifiointiin (esim. ISO 27001). Tekniset ja organisatoriset kontrollit eivät riitä suojaamaan organisaatiota kaikilta riskeiltä. Vakuutukset sopivat hyvin muiden vastatoimien jälkeen jäljellä olevaan riskiin varautumiseen (Shackelford, 2012; Franke, 2017). Franken (2017) mukaan tietoturvavakuutusta

hyödynnetään usein esimerkiksi palveluntarjoajan ja asiakkaan sopimuksen väliin jäävien aukkojen paikkaamisessa eli ns. jäännösriskin (sopimusrajoitteet vrt. asiakkaan todellinen tappio) hallinnassa. Tietoturvasertifioinnilla yritys voi osoittaa hallitsevansa tietoturvalliset toimintatavat yhteistyökumppaneilleen ja asiakkailleen (Suhonen, 2019). Tietoturvavakuutukset ovat taloudellista riskienhallintaa (Franke, 2017). Niillä tarkoitetaan erillisiä vakuutussopimuksia, jotka ovat suunniteltu auttamaan organisaatiota suojautumaan tappioilta ja mahdollisista vahingonkorvausvelvoitteista, jotka johtuvat esimerkiksi: omaisuusvahingoista ja varkauksista, datan vahingoittumisesta ja varkauksista, tietoverkon katkoksista, laitteiston vahingoittumisesta sekä kyberkiristyksestä (Bandyopadhyay ym., 2009; Shackelford, 2012.) Vakuutukset auttavat organisaatioita palautumaan datan menetyksistä tai muista kyberhäiriötilanteista, kuten palvelukatkoksista (Low, 2017).

Tietoturvavakuutusten merkitys muiden varautumiskeinojen joukossa on kasvanut pilvipalvelujen ja IT-palvelujen ulkoistamisen myötä: Kun organisaation IT-hallinta on ulkoistettu yrityksen ulkopuolelle, yrityksen on vaikea hallita siihen liittyviä riskejä teknisten tai organisatoristen kontrollien avulla (Franke, 2017). Informaatioasymmetria palveluntarjoajan (vakuutusyhtiön) ja vakuutuksenottajan välillä on hidastanut vakuutusten käyttöönottoa organisaatioissa (Bandyopadhyay ym., 2009). Vakuutusyhtiöillä on taipumuksena hinnoitella vakuutus samalla tavalla, yrityskohtaisista riskeistä riippumatta (Low, 2017), mikä on johtanut siihen, että yritykset kokevat kyberturvavakuutukset ylihinnoitelluiksi (Bandyopadhyay ym., 2009). Vakuuttaminen kyberhyökkäyksiä vastaan on huomattavasti kalliimpaa kuin yleiset vastuuvakuutukset tai omaisuuden vakuuttaminen (Low, 2017). Pk-yrityksille on tarjolla kybervakuutuksia, mutta ne ovat usein hankalasti ymmärrettävissä, sillä poikkeuksien ja ehtojen listaus on niin pitkä. Low (2017) mukaan luotettava ja kustannustehokas palautumisprosessi voi siis osoittautua organisaatiolle halvemmaksi ratkaisuksi kuin tietoturvavakuutuksen ottaminen.

Seuraavassa luvussa 3.6 kerrotaan, miten tietoturvainvestointiprosessi perinteisesti etenee akateemisessa kirjallisuudessa, ja mitä vaiheita prosessiin liittyy.

3.6 Tietoturvainvestointiprosessi

Tietoturvaan liittyvät uhkakuvat muuttuvat jatkuvasti. Varautuminen uhkiin on haastavaa, joten organisaatioiden pitää Dor ja Elovicin (2016) mukaan omaksua yhä ammattimaisempia tietoturvainvestointiprosesseja. Bojanc ja Jerman-Blažič (2008) ehdottavat standardoitua lähestymistapaa investointiprosessiin. Taulukko 3 kuvaa akateemisessa kirjallisuudessa tyypillisesti esitetyn turvallisuusriskien hallinnointiprosessin etenemistä, jota voidaan hyvin verrata tietoturvainvestointiprosessiin.

TAULUKKO 3 Turvallisuusriskien hallinnointiprosessi

Vaihe	Tehtävä
Liiketoiminnan kannalta merkittävien omaisuuserien tunnistaminen / liiketoimintaprosessin tärkeysasteen määrittely	Organisaation hallussa olevan datan luokittelu (mm. datan tärkeys, haavoittuvuus, olemassa olevat kontrollit, uhkakuvat, hyväksyttävä riskitaso jne.), liiketoimintaprosessien tunnistaminen ja priorisointi
Turvallisuuteen liittyvän ongelman tai tarpeen havaitseminen	Uhkien identifiointi ja mahdollisen onnistuneen hyökkäyksen aiheuttaminen vahinkojen arviointi, haavoittuvuuksien tunnistaminen järjestelmissä ja prosesseissa
Riskianalyysi	Arvio uhan toteutumisen todennäköisyydestä, turvallisuusriskien vaikuttavuuden arviointi
Vaihtoehtojen vertailu ja arviointi	Esim. ohjaavat ja ennaltaehkäisevät aktiviteetit, estäminen, havaitseminen, palautumiskyky, riskin siirtäminen
Päätös vaihtoehtojen välillä	Kontrollin kohdistaminen esim. ihmiset, teknologia, prosessit
Kontrollien implementointi	Soveltuvien kontrollien implementointi pyrkimyksenä minimoida riskit
Kontrollien arviointi	Käyttöönotettujen kontrollien vaikuttavuuden arviointi

Turvallisuusriskien hallinnointiprosessi (tai investointiprosessi) alkaa sillä, että ensin tunnistetaan liiketoiminnan kannalta merkittävät omaisuuserät: miksi ja mitä omaisuuseriä organisaation pitää suojata. Fenz ym., (2011) mallissa prosessi alkaa liiketoimintaprosessien tärkeysasteen määrittelyllä. Gordon & Loeb (2002) argumentoivat, että tietoturvasta vastaavan johdon olisi järkevää erotella yrityksen hallussa oleva data, datan riskipitoisuuden (security breach vulnerability) perusteella eri luokkiin, ja toimia sen mukaan. Heidän mallissaan datan haavoittuvuus jaetaan kolmeen luokkaan: korkea haavoittuvuus, keskitason haavoittuvuus ja matala haavoittuvuus.

Seuraava askel on uhka-analyysi, jossa analysoidaan organisaation kannalta merkittäviä uhkakuvia. Prosessiin kuuluu uhkien identifiointi, haavoittuvuuksien tunnistaminen järjestelmissä ja prosesseissa sekä mahdollisen onnistuneen hyökkäyksen aiheuttaminen vahinkojen arviointi. Haavoittuvuusanalyysi pyrkii osoittamaan, missä ja miten uhat voivat ilmetä. Bojanc ja Jerman-Blažič (2008) toteavat, että näiden kahden lähestymistavan (suojattavan datan /prosessien / järjestelmien tunnistaminen + uhka-analyysi) yhdistäminen mahdollistaa hyvän ymmärryksen saavuttamisen liiketoiminnan kannalta merkittävistä riskeistä.

Seuraavana prosessissa on vuorossa riskianalyysi. Riskianalyysissa arvioidaan turvallisuusriskien toteutumisen todennäköisyyttä ja vaikuttavuutta. Kun riski on määritelty, voidaan käyttää taloudellisia malleja tarvittavien investointien määrittämiseen riskin minimoimiseksi. Prosessiin kuuluu vaihtoehtojen vertailu ja arviointi. Kun päätös on tehty, valitut kontrollit implementoidaan ja niiden vaikuttavuutta seurataan.

Tietoturvainvestointiprosessista ja tietoturvariskien hallintaprosessista löytyy myös huomattavasti yksityiskohtaisempia malleja kuin tässä esitelty (mm. Soo Hoo, 2000; Purser, 2004; Jerman-Blažič, 2008; Nazareth & Choi, 2015; Carias ym., 2019; Straub & Welke, 1998).

3.7 Yhteenveto

Tietoturvainvestoinnit kuuluvat IT-investointien joukkoon. Tietoturvainvestoinnin perimmäinen pyrkimys on varmistaa organisaation liiketoiminnan jatkuvuus ja toimia liiketoiminnan mahdollistajana (Tsiakis & Stephanides, 2005). Tietoturvainvestointi voi pyrkiä varmistamaan esimerkiksi suojattavan informaation tai prosessin luottamuksellisuuden, koskemattomuuden, oikeellisuuden, saatavuuden tai kiistämättömyyden (Gordon & Loeb, 2002; Fenz ym., 2011). Päätöksentekijöiden ei ole helppoa vertailla tietoturvainvestointien hyötyjä ja kustannuksia: Negatiiviset seuraukset, joihin investoinneilla varaudutaan ovat luonteeltaan epäselviä ja sattumanvaraisia, joten myös sopivien vastatoimien määrittäminen on jokseenkin hankalaa. Investoinnin hyödyt ovat usein abstrakteja ja epäsuoria, mutta kustannukset sen sijaan suoria (Cavusoglu, 2010). Tietoturvainvestoinnin tuotto muodostuu tietoturvariskien vähentymisestä (Huang ym., 2008). Tietoturvainvestointi voi kohdistua teknologiaan, ihmisiin tai prosesseihin (Purser, 2004). Investoinnilla voidaan parantaa esimerkiksi organisaation estämiskykyä, palautumiskykyä, ennaltaehkäiseviä ja ohjaavia prosesseja tai havaitsemiskykyä (Straub & Welke, 1998). Ulkoisilla tekijöillä (lainsäädäntö, asiakkaan ja yhteistyökumppanien vaatimukset) on usein merkittävä työntävä vaikutus tietoturvainvestointipäätökseen (Weishäupl ym., 2018; Cavusoglu ym., 2015; Heidt ym., 2019). Tietoturvainvestointien optimoinnista on laajalti akateemista tutkimusta (mm. Gordon & Loeb, 2002). Muut päätöksentekoon vaikuttavat asiat (psykologiset harhat, kontekstisidonnaiset tekijät, organisatoriset tekijät ym.) ovat viime vuosina yleistyneet tutkimuksessa (Heidt ym., 2019). Klassiset investointien arviointiin käytetyt mittarit (sijoitetun pääoman tuottoaste, nettonykyarvo, sisäinen korkokanta) eivät sellaisenaan sovellu kovin hyvin tietoturvainvestointien arviointiin (Bojanc & Jerman-Blažič, 2008; Sonnenreich ym., 2006), mutta malleista on lukuisia tietoturvainvestointeihin sovellettuja variaatioita. Tietoturvainvestointimallien hyödyntämistä käytännössä rajoittaa usein puutteellinen informaatio, hankalasti arvioitavissa olevat parametrit sekä useiden mallien oletus rationaalisesti toimivasta päätöksentekijästä (Cavusoglu, 2010; Shao ym., 2019). Akateemisen kirjallisuuden esittämä tietoturvainvestointiprosessi sisältää yleensä liiketoiminnan kannalta merkittävien omaisuuserien tunnistamisen, turvallisuuteen liittyvän ongelman tai tarpeen havaitsemisen, riskianalyysin, vaihtoehtojen arvioinnin ja lopulta investointipäätöksen.

4 EMPIIRISEN AINEISTON KERUU JA ANALYYSI

Tutkielman osana toteutettiin pienimuotoinen tapaustutkimus, joka tuo käytännön näkemystä siihen, miten pienessä, voimakkaasti kasvuhakuisessa, suomalaisessa startup-yrityksessä suhtaudutaan tietoturvainvestointeihin. Tapaustutkimuksen pyrkimyksenä oli tuoda uutta tietoa tietoturvainvestointien (sekä investointitarpeen kehittymisen) ja yrityksen kasvun välisestä dynamiikasta.

Luku on jaettu seuraaviin osioihin: Ensimmäisessä alaluvussa kerrotaan, miksi päädyin toteuttamaan tutkielman empiirisen osion tapaustutkimuksena. Toinen alaluku käsittelee tiedonkeruumenetelmää ja sen valintaa sekä haastattelujen kulkua. Kolmas alaluku kertoo kerätyn datan analysointiin valituista menetelmistä ja toimintatavoista. Viimeinen alaluku kuvaa tapausyrityksen perustiedot ja tapausyrityksen valintaperusteet.

4.1 Tutkimusmenetelmä

Tutkielman empiirinen osio toteutettiin kvalitatiivisena tapaustutkimuksena. Eisenhardtin (1989) mukaan tapaustutkimus sopii hyvin esimerkiksi tapahtuman tai ilmiön kuvailuun. Tavoitteena on rikas, empiirinen kuvaus tutkimuksen kohteena olevasta ilmiöstä tukeutumalla useisiin erityyppisiin datalähteisiin (Yin, 1994). Tutkielmassa käsitellään hyvin arkaluonteista aihetta (tietoturvainvestoinnit) joten oikean tutkimusmenetelmän valitseminen oli tärkeää. Jos valittu tutkimusmenetelmä ei syystä tai toisesta olisi toiminut, riittävän laadukkaan tutkimusdatan keruu olisi saattanut epäonnistua. Esimerkiksi kyselytutkimuksen massapostittaminen laajalle joukolle ei välttämättä olisi toiminut erityisen hyvin, sillä yritykset ovat vähemmän todennäköisiä luovuttamaan arkaluonteista dataa kyselytutkimuksessa (Kotulic & Clark, 2004). Aikaisemmissa tutkimuksissa kuten esimerkiksi Kotulic ja Clark (2004); Loch, Carr & Warkentin (1992) moni oli jättänyt vastaamatta kysymyksiin, koska he eivät olleet uskaltaneet vastata aiheen arkaluonteisuuden vuoksi ”tietoturvasyistä”. Tietoturvatutkimukset ovat luonteeltaan yksi tunkeilevimmista tutkimustyypeistä (Kotulic & Clark, 2004) ja tutkielman kohderyhmä eli Suomessa toimivat pienet kasvuyritykset ovat melko rajatun kokoinen joukko (Huovinen, 2018). Kyselyn vastausprosentti olisi todennäköisesti jäänyt hyvin maltilliseksi, joten tutkimus olisi saattanut epäonnistua riittävän laadukkaan tutkimusdatan puutteeseen. Näistä syistä päädyin toteuttamaan tutkielman empiirisen osion tapaustutkimuksena. Tyypillisesti tapaustutkimuksessa tutkittava joukko on huomattavasti pienempi kuin kyselytutkimuksessa, mutta toisaalta tapaustutkimus mahdollistaa tapausyksiköiden yksityiskohtaisemman tarkastelun (Rowley, 2002).

Kvalitatiivisen tutkimuksen lähtökohtana on pyrkiä kuvailemaan tutkittavaa ilmiötä mahdollisimman hyvin (Hirsjärvi, Remes & Sajavaara, 2009). Kvalitatiivinen tutkimus pyrkii kokoamaan tietoa spesifistä tilanteesta tai ilmiöstä (yksi tapaus) tai pienestä joukosta yhtäläisiä tapauksia (monta tapausta) (Hirsjärvi ym., 2009). Kvalitatiiviset tutkimusmenetelmät keskittyvät ensisijaisesti siihen, mitä ihmiset kertovat sinulle ja mitä he tekevät. Tutkijan pyrkimyksenä on ymmärtää, mitä on tapahtumassa (ja miksi). Kvalitatiivinen tutkimus on aina sidoksissa aikaan ja paikkaan. Kvalitatiivisen tutkimuksen tarkoituksena on löytää uutta faktoihin perustuvaa informaatiota tutkimuskohteesta. Se on monipuolinen ja kokonaisvaltainen lähestymistapa informaation keräämiseksi luonnollisissa olosuhteissa. Kvalitatiivisessa tutkimuksessa ei ole tarkoitus pyrkiä yleistyksiin, vaan siinä pyritään kuvaamaan, ymmärtämään ja tulkitsemaan jotakin tapahtumaa, toimintaa tai ilmiötä. (Gillham, 2010.) Gillham (2010) tähdentää, että kvalitatiiviset tutkimusmenetelmät mahdollistavat pääsyn tutkimuskohteen ”ihon alle”, sillä kvalitatiivisin tutkimusmenetelmin voidaan kuvailla mitä ryhmässä tai organisaatiossa todella tapahtuu, sisältä päin: kuvailla sitä epämuodollista todellisuutta, joka voidaan kokea vain ryhmän tai organisaation sisältä käsin. Jotta tapausta voidaan tutkia läpikotaisesti, pitää tapaus nähdä heidän näkökulmastansa, jotka osallistuvat siihen. Tapaustutkimuksen soveltuvuus täytyy kuitenkin varmistaa, jotta sitä voidaan luotettavasti käyttää. Erikssonin ja Koistisen (2014) mukaan tapaustutkimus kannattaa valita tutkimuksiin, joissa jotkin tai useat seuraavista ehdoista täyttyvät:

- ’Mitä-’, ’miten-’ ja ’miksi-’kysymykset ovat keskeisellä sijalla
- Tutkijalla on vähän kontrollia tapahtumiin
- Aiheesta on tehty vain vähän empiiristä tutkimusta
- Tutkimuskohteena on jokin tämän ajan elävässä elämässä oleva ilmiö

Yllä olevat kriteerit täyttyivät tässä tutkielmassa hyvin, sillä tietoturvainvestoinneista oli toistaiseksi tehty melko vähän empiiristä tutkimusta suhteessa aiheen ajankohtaisuuteen ja merkittävyyteen.

Rowleyn (2002) mukaan tutkijan pitää pystyä perustelemaan hyvin, miksi tutkimuksessa on päädytty tutkimaan vain yhtä tapausta monitapaustutkimuksen sijaan. Tutkittavan tapauksen pitää olla jotenkin uniikki tai erikoinen, tai sen pitää paljastaa jotain erityistä (Rowley, 2002). Tämä tutkielma päätettiin toteuttaa yksittäisenä tapauksena, koska aiheesta ei ollut aiemmin tehty juuri tutkimusta. Tutkielma toimi alustavana esitutkimuksena, jonka tulosten perusteella voitiin paremmin arvioida, olisiko tutkimusaiheessa potentiaalia jatkotutkimukseen monitapaustutkimuksen tai pitkittäistutkimuksen muodossa. Rowleyn (2002) näkemyksen mukaan yhden tapauksen käyttö on näissä tilanteissa hyvin perusteltavissa. Lisäksi on syytä painottaa tutkimuksen uutta tulokulmaa. Oli melko vaikea etukäteen arvioida, miten tietoturvainvestointeja toteutettiin missäkin kasvuyrityksessä sen hetkisen

tutkimustiedon perusteella. Oli siis vaikea noudattaa esimerkiksi Yin (1994) neuvoa monitapaustutkimuksen tapausten valitsemisessa. Hänen mukaansa tapausyritykset pitäisi optimaalisessa tilanteessa valita siten, että tapaukset oletettavasti tuovat joko samankaltaisia tuloksia, tai siten, että niissä on merkittäviä eroja. Tämän tutkielman yhteydessä se ei olisi ollut mahdollista, sillä yritysten tietoturvainvestoinneista on harvoin tietoa julkisesti saatavilla. Stake (1995) on ylipäätään skeptinen erillisten tapausten vertailtavuuden suhteen. Hänen mukaansa vertailu vaikuttaa negatiivisesti kokonaiskuvaan tutkittavasta tapauksesta, sillä se väistämättä vähentää tapausten holistisuutta rajaamalla tapaukset vain vertailun kohteena oleviin ulottuvuuksiin. Jos tapauksia on enemmän kuin muutama, on selvää, ettei kutakin tapausta voi käsitellä yhtä monipuolisesti (Eriksson & Koistinen, 2014). Aihepiirin kannalta holistinen tutkimus yhdestä tapauksesta tarjoaa syvempää näkemystä kuin tutkimus, jossa tutkittavia tapauksia on enemmän mutta haastatteluita tapausyritystä kohti vähemmän. Haastattelujen laajuutta olisi pitänyt rajata monitapaustutkimuksessa enemmän, jotta työmäärä ei olisi kasvanut kohtuuttomaksi.

Tapaustutkimuksessa on tärkeää valita tutkimusyksikkö hyvin (Rowley, 2002). Jotta valinta onnistuisi, tutkijan pitää osata määritellä tutkimuksen kohde eli tutkimusyksikkö. Erikssonin & Koistisen (2014) mukaan tutkittavia tapauksia voidaan määritellä sekä ennen aineiston keruun aloittamista, sen aikana tai vasta sen jälkeen, kun ensimmäinen aineiston analyysikierros on tehty. Staken (1995) mukaan tapauksen valintaa ei ohjaa vain teoria: tärkeintä on valita tapaus, joka mahdollistaa oppimisen ja ymmärryksen lisäämisen tutkittavasta kohteesta. Hän suosii eri lähestymistapaa kuin Yin ja Eisenhardt. Staken (1995) näkemyksen mukaan holistinen ymmärrys tutkittavasta tapauksesta on tutkimuksen ensisijainen tavoite, tutkimuksen yleistettävyyden ylikorostamisen sijaan. Tutkittavan kohteen rikas kuvaus on jo tavoite sinänsä. Tällainen tapaus kehittää ymmärrystämme, ja sen avulla saatamme pystyä kehittämään tai muokkaamaan teoriaa tai käsitejärjestelmää. Tapaus muuntuu ja tarkentuu sitä mukaa kun tutkija oppii lisää tutkimusprosessinsa aikana. (Eriksson & Koistinen, 2014.) Tapauksen valintaan vaikuttavat lisäksi käytännön asiat (Rowley, 2002):

- Saatavuus (pystytäänkö valitusta tapauksesta keräämään vaadittua dataa)
- Resurssit (onko tutkijalla tarvittavat resurssit tutkimuksen toteuttamiseen)
- Käytettävissä oleva aika (tutkimuskohde pitää suhteuttaa käytettävissä olevaan aikaan; jos aika on rajallinen, on järkevää pyrkiä rajoittamaan tapauksen laajuutta)

Tämän tutkielman osana toteutettu tapaustutkimus oli yhdistelmä intensiivistä, kuvailevaa ja uuden löytämiseen suuntautunutta lähestymistapaa. Rowleyn (2002) mukaan ”uuden löytämiseen” suuntautuneessa (exploratory case study) tapaustutkimuksessa tutkimuskysymysten ei tarvitse olla alussa vielä muotoutunut lopulliseen muotoonsa, mutta tutkimuksen tarkoitus pitää silti olla määritelty. Tutkimuksen tekeminen on monimuotoinen ja iteratiivinen prosessi,

joka ei välttämättä etene juuri niin kuin on suunniteltu. Intensiiviselle tapaustutkimukselle ei ole yhtä vakiintunutta kaavaa. Esimerkiksi tutkimuskysymyksiä muokataan, tarkennetaan ja hiotaan useassa vaiheessa. (Eriksson & Koistinen, 2014.)

Tutkimusyksikkö oli tässä tutkielmassa yritys Y. Yrityksen nimi on salassapitosyistä anonymisoitu. Tapaustutkimuksen pyrkimyksenä oli ymmärtää uutta, vähän tutkittua ilmiötä. Pitkittäistutkimus olisi ollut oiva vaihtoehto tutkimusaiheen kannalta, mutta ei käytännöllinen opinnäytetyöhön. Tapausyrityksen valinta tehtiin teorian pohjalta määritettyjen ehtojen mukaisesti, mutta osin myös käytännön syistä päädyttiin tutkimaan vain yhtä tapausyritystä. Ensimmäisen haastattelun haastattelurunko muotoiltiin akateemisen kirjallisuuden avulla. Tutkimuskysymykset olivat tässä vaiheessa tutkimusta hahmoteltu, mutta tutkimuskysymykset muotoiltiin lopulliseen muotoonsa vasta ensimmäisen haastattelun jälkeen. Haastattelukierroksia järjestettiin yhteensä kolme.

Yin (1994) korostaa, että hyviä tuloksia saavuttaakseen tapaustutkimuksen tutkimusmenetelmien pitää olla hyvin suunniteltu. Seuraavat viisi kohtaa ovat olennaisia tutkimuksen onnistumisen kannalta: 1. tutkimuskysymykset 2. ennakko-oletukset odotetuista tuloksista 3. Tutkimusyksikkö ennakko-oletusten testausta varten 4. Sisäinen logiikka, jonka mukaan tutkimustulokset ovat yhdistettävissä ennakko-oletuksiin 5. Kriteeristö, jonka mukaan tuloksia analysoidaan. Alla kuvaillaan, miten nämä viisi kohtaa on huomioitu tässä tutkielmassa.

1. *Tutkimuskysymykset:*

   Miten pienen kasvuyrityksen tietoturvainvestointitarve muuttuu yrityksen kasvaessa?
   Miten tietoturvainvestointitarpeita arvioidaan suhteessa kasvuun pienissä kasvuyrityksissä?

2. *Ennakko-oletus odotetuista tuloksista:*

   Tietoturvainvestointeja ei ole priorisoitu kovinkaan korkealle suhteessa muihin liiketoiminnan kehittämistoimiin. Pienissä kasvuyrityksissä edetään kasvu ja tuotto edellä, ja riskienhallinta ml. yrityksen tietoturvainvestoinnit ovat huomattavasti pienemmässä roolissa. Tietoturvainvestointien merkitys on pieni tai niihin ei kiinnitetä lainkaan huomiota. Tietoturva aiheuttaa investointitarpeita myöhemmin, yrityksen jo kasvettua huomattavasti suurempaan kokoluokkaan, kun ulkopuoliset tahot (esimerkiksi asiakkaat tai yhteistyökumppanit) alkavat vaatia yritykseltä todisteita riskienhallinnasta ja tietoturvasta.

3. *Tutkimusyksikkö ennakko-oletusten testausta varten:*

Tutkimusyksikköä valittaessa seuraavat kriteerit olivat tärkeitä: Yrityksen piti olla voimakkaasti kasvuhakuinen ja /tai sillä piti olla näyttöä kasvusta, koska tutkielmassa selvitettiin yrityksen tietoturvainvestointien ja kasvun välistä dynamiikkaa. Vahvasti kasvuhakuiset yritykset ovat usein nuoria, innovatiivisia, vahvasti kansainvälisille markkinoille suuntautuvia korkean teknologian yrityksiä (Huovinen, 2018; Kollmann ym., 2016). Nämä kriteerit täyttyivät tapausyrityksessä. Tapausyrityksen kohdalla piti tehdä myös valinta, kuinka suuria kasvuyrityksiä tutkielmassa tutkitaan. Tutkielma selvitti pienten kasvuyritysten tietoturvainvestointitarpeita, joten tapausyritys ei saanut olla liian suuri. Tapausyritystä ja sen valintaperusteita kuvaillaan lisää kappaleessa 4.4

4. *Sisäinen logiikka, jonka mukaan tutkimustulokset ovat yhdistettävissä ennakko-oletuksiin:*

   Valittu tapausyritys kuului tutkimuksen kohderyhmään. Datan keräys ja analysointi toteutettiin järjestelmällisesti etsien tukea tai vastaväitteitä ennakko-oletuksille. Ennakko-oletukset oli muotoiltu aikaisemman tutkimuskirjallisuuden ja tietoturva-asiantuntijoiden kommenttien tuella.

5. *Kriteeristö, jonka mukaan tuloksia analysoidaan:*

   Tuloksia analysoitiin teoriataustaa ja ennakko-oletuksia vasten. Analysointiprosessia kuvaillaan tarkemmin kappaleessa 4.3 datan analysointi. Rowley (2002) ohjeistaa huomiomaan ainakin seuraavat kohdat, joita analyysissa on noudatettu:
   1. Analyysi perustuu koko tutkimusaineistoon
   2. Analyysissa esitetään erilaisia perusteltuja, kilpailevia tulkintoja havainnoille
   3. Analyysi kohdistuu tutkimuksen kannalta olennaisiin asioihin
   4. Analyysi pohjautuu tutkijan asiantuntemukseen, mutta on mahdollisimman objektiivinen ja puolueeton

4.2 Datan keräys

Kvalitatiivisessa tutkimuksessa voidaan tehdä harkinnanvaraista, teoreettista tai tarkoituksenmukaista poimintaa. Tällöin tutkimus perustuu melko pieneen tutkittavien määrään. Kvalitatiivisessa tutkimuksessa aineisto rajataan teoreettista kattavuutta silmällä pitäen. Kriteerinä on aineiston teoreettinen

kiinnostavuus tutkimusongelman ratkaisussa tilastollisten kriteerien sijaan. Jäsentynyt teoreettinen viitekehys ohjaa aineiston keruuta. Kvalitatiivisen tutkimuksen pohjalta ei ole tarkoitus tehdä yleistäviä päätelmiä kuten tilastollisessa tutkimuksessa; yleistyksiä tehdään aineiston sijaan tulkinnoista. Tapaustutkimus voi koostua sekoituksesta erilaisia lähestymistapoja, sillä tutkimuksessa voidaan yhdistää niin kvantitatiivisia kuin kvalitatiivisia menetelmiä. (Rowley, 2002; Eskola & Suoranta, 1998.) Yleistettävyyttä parantavat vertailuasetelmat, joita tehdään muihin tutkimustuloksiin ja tulkintoihin nähden. Järkevä aineiston kokoaminen on hyvä yleistettävyyden kriteeri (Eskola & Suoranta, 1998).

Tutkielma oli aluksi tarkoitus toteuttaa monitapaustutkimuksena, mutta päädyin lopulta toteuttamaan tutkielman empiirisen osion syventymällä vain yhteen tapaukseen. Tutkimusmateriaali koostui yrityksen edustajien haastatteluista ja heidän tutkijan käyttöön luovuttamista yrityksen dokumenteista. Tutkimusaineiston keräyksessä hyödynnettiin myös yrityksen verkkosivuja ja blogia. Yrityksen jakamat dokumentit ja verkkosivuilta kerätty data, yhdistettynä haastatteluihin, mahdollisti kerätyn datan vahvistamisen eri lähteistä (engl. triangulation), mikä parantaa tiedon luotettavuutta (Rowley, 2002). Tapausyritys valikoitui lopulta osin henkilökohtaisten verkostojen avulla. Tämä oli kerätyn tutkimusmateriaalin kattavuuden kannalta hyvä asia, sillä haastattelijan ja haastateltavien välillä oli tärkeää vallita luottamus. Molemmat haastateltavat kuuluivat tapausyrityksen perustajajäseniin. Aihepiiri oli hyvin sensitiivinen. Haastateltava on halukkaampi kertomaan myös arkaluonteisista asioista, kuten investointipäätöksistä, jos hän luottaa haastattelijaan (Kotulic & Clark, 2004). Hirsjärven ja Hurmeen (2009) mukaan, kun haluamme saada selville, minkälaisia mielipiteitä, uskomuksia ja käsityksiä ihmisillä on tai miksi he toimivat tietyllä tavalla, heidän kanssaan keskustelu on luonnollinen lähestymistapa.

Tutustuin laajalti tutkielman aihepiiriin ennen tutkielman aloittamista. Tutkimuskirjallisuutta haettiin kattavasti eri tietokannoista, kuten Google Scholar ja Scopus. Valtaosa käytetyistä lähteistä on peräisin laadukkaista akateemisista julkaisusta, mutta tutustuin myös joihinkin ei-akateemisiin julkaisuihin tutkimusta tehdessä kuten konsulttiyhtiöiden raportteihin (mm. Ponemon Institute, Microsoft, Marsh, E&Y, KPMG) ja valtiollisten tutkimuslaitosten raportteihin (Etla, VTT, TEM). Konsulttiyhtiöiden raportit tarjoavat usein tuoreempaa tietoa yritysten tietoturvan nykytilasta, joten niistä oli hyötyä yleiskuvan luomisessa. Yksityisten konsulttiyritysten esittämiin lukuihin oli toki syytä suhtautua varauksella. Valtiollisten tutkimuslaitosten raportit taas toivat ajankohtaista tietoa suomalaisten kasvuyritysten nykytilasta. Hakua kohdennettiin aihepiirin kannalta olennaisiin asioihin käyttämällä hakusanoja kuten tietoturvainvestointi, kasvuyritys, riskienhallinta, liiketoiminnan kasvu jne. (ja englanninkielisiä vastinpareja). Lähteiden laatua arvioitiin viittausten lukumäärän ja julkaisualustan perusteella.

Haastattelujen toteutus

Kvalitatiivisen tutkimuksen yhteydessä esitetään usein kysymys, kuinka monta haastattelua olisi tehtävä. Tutkimuksen kannalta on tärkeää se, että tutkija tavoittaa riittävän syvän kuvan tutkimuskohteesta. Haastateltavia tulee olla sen verran, että tutkimustehtävä tekee oikeutta tutkittaville ja tutkimuskohteelle. (Syrjälä, Ahonen, Syrjäläinen & Saari, 1994.) Tässä tutkielmassa haastattelut toteutettiin kolmessa erässä aikavälillä 27.8.2020 – 30.9.2020. Haastatteluihin osallistui kaksi tapausyrityksen kolmesta perustajajäsenestä. Ideaalitilanteessa olisin haastattelut kaikkia yrityksen perustajajäseniä ja kahta palkattua työntekijää, mutta se ei ollut tällä kertaa mahdollista. Haastattelujen laatu oli toisaalta hyvä, sillä haastateltavat yrityksen perustajajäseninä olivat luonnollisesti hyvin perillä siitä, mitä yrityksessä tapahtuu.

Haastattelut toteutettiin puolistrukturoituna haastatteluna eli teemahaastatteluna. Teemahaastattelu perustuu ennalta määriteltyyn kysymysrunkoon, jota täydennetään haastattelutilanteessa tarkentavilla kysymyksillä (DiCicco-Bloom & Crabtree, 2006). Lomakehaastatteluun verrattuna haastateltavien määrä voidaan pitää pienenä ja haastattelemalla saatu tieto on syvempää (Hirsjärvi & Hurme, 1988). Teemahaastattelussa tutkija tekee kysymykset ja haastateltava voi vastata kysymyksiin omin sanoin (Koskinen, Alasuutari & Peltonen, 2005).

Ensimmäinen haastattelu pidettiin tapausyrityksen operatiivisen johtajan (COO) kanssa. Haastattelun tarkoituksena oli luoda laaja yleiskuva yrityksen toimintatavoista, kasvutavoitteista, kilpailuympäristöstä, riskienhallinnan ja tietoturvan nykytilasta sekä yrityksen tulevaisuuden suunnitelmista. Tutkimusaihe ja tutkimuskysymykset järjestettiin haastattelurungon (liite 1) muotoon, joka rakennettiin aihepiirin tutkimuskirjallisuuden avulla. Haastattelurunko antaa haastattelulle muodon ja varmistaa, että tutkija esittää tarvittavat kysymykset. Kysymyksiä ei välttämättä käydä läpi samassa järjestyksessä teorian kanssa, mutta saadut vastaukset voidaan tulkita myöhemmin teorian avulla. (Koskinen ym., 2005.) Ensimmäinen haastattelu pyrittiin toteuttamaan mahdollisimman sensitiivisesti antamalla haastateltavalle tilaa kertoa näkemyksiään omin sanoin. Järvisen ja Järvisen (2011) mukaan tutkimuksen onnistumisen kannalta on tärkeää, että tutkijalla on hyvä ymmärrys tutkimusaiheesta. Tutkijan pitää osata kuunnella ja lukea rivien välistä, sillä hänen pitää osata ottaa vastaan ja tunnistaa myös ristiriitainen informaatio.

Toisessa haastattelussa haastateltiin yrityksen teknistä johtajaa (CTO). Toista haastattelua varten haastattelurunkoa supistettiin jättämällä pois ensimmäisessä haastattelussa jo käsiteltyjä yleisiä organisaatioon liittyviä asioita ja toisaalta fokusoitiin keskustelua hieman enemmän yrityksen päätöksentekoon, investointiprosesseihin ja tietoturvaan (liite 2). Toisessa haastattelussa haastateltavaa pyydettiin kertomaan oma näkemyksensä haastattelurungon mukaisista asioista, mutta ei kerrottu, mitä ensimmäinen haastateltava oli vastannut, jotta mahdolliset eriävät näkemykset nousisivat vapaasti esiin.

Kolmanteen haastatteluun osallistuivat sekä yrityksen tekninen johtaja että operatiivinen johtaja. CTO joutui poistumaan haastattelusta hieman ennen kuudetta skenaariota, joten kahta viimeistä skenaarioista kommentoi vain COO. Kolmannen haastattelun tukena oli erilaisia investointiskenaarioita, joihin haastateltavia pyydettiin ottamaan kantaa (liite 3).

Haastattelut järjestettiin etänä Skypen välityksellä. Haastattelut nauhoitettiin ja litteroitiin myöhemmin saman viikon aikana. Kaikissa haastatteluissa käytiin läpi haastattelurungon mukaiset aihealueet. Haastattelujen keskipituus oli noin 75 minuuttia.

4.3 Datan analysointi ja luotettavuuden arviointi

Eisenhardtin (1989) mukaan tulosten analysointivaihe on tapaustutkimuksissa sen tärkein, mutta samalla haastavin vaihe, sillä suuren laadullisen datamäärän analysointi kattavasti perustellen on erittäin haastavaa ja toisaalta myös tutkijasta riippuvaisempaa verrattuna esimerkiksi kvantitatiivisen tutkimuksen määrämuotoisempiin analyysimenetelmiin. Eriksson & Koistinen (2014) jakavat aineiston analyysin tavoitteet kolmeen kohtaan: laaja aineisto pitää järjestää jollakin tavoin (esimerkiksi luokittelemalla tai tyypittelemällä) yhtenäiseksi kokonaisuudeksi. Toiseksi, aineistoa pitää analysoida (esimerkiksi sisällön analyysillä) ja kolmanneksi, analyysissä saatuja havaintoja ja löydöksiä pitää tulkita. Hirsjärvi ja Hurme (2009) korostavat aineiston aktiivisen ja toistuvan lukemisen tärkeyttä. Heidän mukaansa onnistunut analyysi vaatii aineiston perinpohjaista tuntemista. Eskolan ja Suorannan (2000) mukaan analyysin tavoite on tuottaa uutta tietoa tutkittavasta ilmiöstä aineistoa selkeyttämällä ja tiivistämällä. Analyysivaiheessa empiirisestä aineistosta erotellaan tutkimuksen kannalta oleelliset piirteet (Eskola & Suoranta, 2000) ja niitä tarkastellaan tutkimuksen näkökulman kontekstissa (Hirsjärvi & Hurme, 2009). Aineiston analyysiä ohjaa ymmärrys aiheesta. Hirsjärven ja Hurmeen (2009) mukaan aineiston analyysi pohjautuu sen kuvailemiselle. Kuvailulla he tarkoittavat henkilöiden tai ilmiöiden ominaisuuksien kartoittamista niiden kontekstissa. Siinä missä pelkät sitaatit eivät ole tutkimuksen tuloksia, myöskään pelkät kuvaukset eivät ole osoitus syvästä analyysista (Eskola & Suoranta, 2000). Eskolan ja Suorannan (2000) mukaan laadullisen tutkimuksen tulokset muodostuvat tutkijan päätelmistä ja tulkinnoista. Eskola ja Suoranta (2000) tarjoavat tulkintojen tekemiseen kaksi lähestymistapaa: tutkija voi joko pysytellä tiukasti aineistossa, jolloin tulkinnat tehdään esimerkiksi lingvistisin keinoin, tai tutkija voi käyttää aineistoa ajattelun apuvälineenä.

Tässä tutkielmassa kerättyä aineistoa hyödynnettiin pääasiassa ajattelun apuvälineenä. Tutkimusaineistoa on järjestetty luokittelemalla ja tyypittelemällä sitä eri teemoihin haastattelurungon mukaisesti, mutta aineistoa ei koodattu. Suorassa tulkinnassa tutkija analysoi aineistoa koodaamatta sitä. Erikson & Koistinen (2014) toteavat, että suoran tulkinnan tekeminen vaatii tutkijalta kokonaisnäkemystä, lukeneisuutta ja usein myös aiempaa tutkimuskokemusta.

Suorassa tulkinnassa analyysin tekeminen kirjoittamalla saa suuren painoarvon ja kirjoittamista ajatellaan tapana tuottaa uutta tietoa. Tällöin korostuu kerronnallinen tiedon tuottamisen tapa (Eriksson & Koistinen, 2014). Kerättyä aineistoa on verrattu ja arvioitu suhteessa ennakko-oletuksiin ja tutkimuskirjallisuuteen. Tutkielmaan on poimittu sitaatteja haastatteluista, jotka tuovat taustaa tehdyille tulkinnoille. Aineiston analyysissa on noudatettu Rowleyn (2002) neuvoja:

1. Analyysi perustuu koko tutkimusaineistoon
2. Analyysissa esitetään erilaisia perusteltuja kilpailevia tulkintoja havainnoille
3. Analyysi kohdistuu tutkimuksen kannalta olennaisiin asioihin
4. Analyysi pohjautuu tutkijan asiantuntemukseen, mutta on mahdollisimman objektiivinen ja puolueeton

Rowleyn (2002) mukaan tutkijan tulee hyödyntää ennakko-oletuksiaan datan analysoinnissa. Tutkija käy läpi keräämäänsä tutkimusaineistoa etsien vahvistusta ennakko-oletuksille ja tekee analysoidun tiedon perusteella päätöksen, tukeeko kerätty tutkimusaineisto ennakko-oletuksia vai ei.

Reliabiliteetti ja validiteetti

Rowleyn (2002) mukaan aineiston analyysi ja luotettavuuden arviointi liittyvät erottamattomasti yhteen ja hän neuvoo erilaisia keinoja tutkimuksen laadun varmistamiseksi (käytettyjen konstruktioiden pätevyys, sisäinen ja ulkoinen validiteetti sekä reliabiliteetti).

Pätevä konstruktio mittaa tutkittavaa kohdetta. Konstruktion validiteettia voidaan parantaa toimimalla avoimesti. Tutkijan on kuvattava toimintatapansa riittävän tarkasti, jotta lukijan on mahdollista kuvausten perusteella arvioida tutkijan toiminnan oikeellisuus ja tutkimuksen luotettavuus. (Hirsjärvi ja Hurme, 2009; Marshall & Rossman, 2006.) Reliabiliteetti tarkoittaa tutkimuksessa käytettyjen menetelmätapojen tarkkuutta; eri tutkimusvaiheet pitäisi pystyä toistamaan uudelleen eri tapauksessa ilman että tulokset muuttuvat. Tutkimuksen reliabiliteetin osoittamisessa pätevät samat keinot kuin käytettyjen konstruktioiden pätevyyden varmistamisessa; tutkijan on kuvattava toimintatapansa ja tutkimusprosessin eteneminen riittävän tarkasti ja huolellisesti. (Rowley, 2002.) Rowley neuvoo myös käyttämään useita tietolähteitä datan keruussa sekä pyytämään keskeisiä tiedonantajia arvioimaan raportti ennen julkaisua.

Hirsjärvi ja Hurme (2009) toisaalta esittävät, että laadullista tutkimusta ei tulisi tarkastella reliabiliteetin ja validiteetin käsitteiden kautta. He näkevät näiden käsitteiden perustuvan oletukselle, että ilmiöistä on mahdollista saada täysin objektiivista tietoa, kun taas laadullinen tutkimus korostaa ilmiöiden kontekstisidonnaisuutta ja tapausten ainutkertaisuutta. Tutkimuksessa pitää pyrkiä siihen, että tutkittavien todenmukaiset käsitykset paljastuvat mahdollisimman hyvin. Tutkimuksen onnistumisen kannalta on tärkeää, että

haastateltavia on riittävästi, haastateltavat sopivat hyvin ongelmanasetteluun ja tutkija tekee itse kaikki haastattelut. (Hirsjärvi & Hurme, 1988.) Tutkijan tulee kuitenkin olla tietoinen omasta roolistaan tutkimuksessa. Tutkija vaikuttaa tekemillään valinnoilla tutkimukseen sen kaikissa vaiheissa. Kun arvioidaan laadullisen tutkimuksen luotettavuutta, arvio ei kohdistu niinkään aineiston laatuun vaan tutkijan toimintaan. Tutkijan on kuvailtava sekä tutkimuksensa eteneminen että perusteltava uskottavasti tekemänsä valinnat. (Hirsjärvi ja Hurme, 2009; Marshall & Rossman, 2006.)

Tässä luvussa on kuvattu, miten tutkielman toteutus eteni. Haastattelujen apuvälineenä hyödynnetyt haastattelurungot ovat liitteinä raportin lopussa, jotta lukija voi halutessaan arvioida niiden sopivuutta suhteessa tutkimusaiheeseen. Tutkimusmateriaalina hyödynnettiin aineistoa eri lähteistä, haastateltavia oli useampi kuin yksi ja haastateltavilta pyydettiin arvio tapausyrityksen analyysista ennen tutkielman palauttamista. Toteutin itse tutkijana kaikki haastattelut. Tuloksissa viitataan tarkasti lähteeseen, mistä haastattelusta / dokumentista tieto on peräisin. Haastattelut litteroitiin ja luettiin useaan kertaan analyysin yhteydessä. Ensimmäisen haastattelun alustavan analyysin tuella rakennettiin toisen ja kolmannen kierroksen haastattelut. Kerätty data on vahvistettu mahdollisuuksien mukaan eri lähteistä. Haastatelluilta kysyttiin näkemystä samoihin asioihin ja osin eri muotoiluilla, jotta mahdollinen kysymyksen muotoilun aiheuttama harha (framing bias) ei vääristäisi tuloksia. Rowley (2002) suosittaa myös seuraavia toimenpiteitä tutkimuksen laadun varmistamiseksi, joita olen noudattanut:

- Tapaustutkimuksen tietovarasto: Selkeästi järjestetty tietovarasto, johon on kerätty tutkimuksessa hyödynnetty aineisto. Tämän tutkielman yhteydessä tietovarasto tallennettiin yliopiston tarjoamaan pilvipalveluun. Tietovarastoon on tallennettu tapausyrityksen luovuttama dokumentaatio, haastattelujen muistiinpanot, haastattelujen tallenteet ja tutkimusaineiston analysointimateriaalia.
- Todistusketju: Raportissa viitataan oikein kerättyyn tutkimusaineistoon. Todistusaineiston pitää olla saatavilla tapaustutkimuksen tietovarastossa, jotta raportin esittämät tiedot voidaan tarvittaessa vahvistaa. Yhteys kerätyn tutkimusaineiston ja tutkimusraportin väittämien välillä pitää olla selkeä ja läpinäkyvä. Raportoidussa viittauksissa on maininta henkilöön / dokumenttiin, jota viittaus koskee.

4.4 Tutkittava tapaus: Yritys Y

Tapausyrityksen valintaperusteet: Tutkielmassa selvitettiin pienten kasvuyritysten tietoturvainvestointeja ja -investointitarpeita, joten seuraavat kriteerit olivat olennaisia:

- Tapausyritys oli joko startup-yritys tai kasvuhakuinen pk-yritys

- Yritys oli pieni (alle 20 työntekijää)
- Yrityksen piti pyrkiä ja investoida kasvuun
- (Yritys oli saanut ulkopuolista pääomarahoitusta)
- Yrityksellä piti olla toimintaa digitaalisessa ympäristössä, jotta tietoturvainvestoinneilla oli merkitystä
- (Yritys tähtäsi kansainvälistymiseen)
- Yrityksellä oli jo liiketoimintaa

Valittu tapausyritys Y täytti hyvin edellä mainitut kriteerit. Tapausyritys Y oli vahvasti kasvuhakuinen, pieni, suomalainen startup-yritys. Yrityksen toimiala oli IT / verkkokauppa. Yritys oli nuori (alle kaksi vuotta), mutta se oli jo palkannut työntekijöitä. Alla kuvaillaan lyhyesti valitun tapausyrityksen kannalta keskeisiä tekijöitä. Taulukko 4 sisältää haastateltavien lyhyet roolikuvaukset. Liitetiedostossa 4 esitellään tapausyritystä tarkemmin ja pureudutaan syvemmin yrityksen keskeisiin toimintatapoihin ja yrityskulttuuriin.

1. Perustiedot
    a. Toimiala: IT/verkkokauppa
    b. Perustamisvuosi: 2019
    c. Ketä haastattelen: operatiivinen johtaja (COO) ja tekninen johtaja (CTO)
    d. Henkilöstön määrä: kolme perustajajäsentä + 2 työntekijää
2. Organisaatio ja päätöksenteko
    a. Hierarkia ja rakenne: ”Äärimmäisen matala”, ei merkittävää hierarkiaa
    b. Hallinto: Hallituksessa kolme perustajajäsentä + pääomasijoittaja
    c. Päätöksenteko: Merkittävät päätökset pyrittiin tekemään yhdessä, mutta pienemmissä asioissa jokaisella oli lupa toimia itsenäisesti
3. Toimialan kasvunäkymät
    a. Näkymät: Myynti oli juuri lähtenyt paremmin käyntiin, Kiinasta oli löytynyt yhteistyökumppaneita, yritys oli juuri palkannut yhden työntekijän lisää (myyntiin). Kaiken kaikkiaan kasvunäkymät olivat ”lupaavat”
    b. Uhat & Mahdollisuudet: Kansainvälisesti erittäin kilpailtu, mutta kasvava toimiala
4. Yrityksen kasvuhakuisuus ja kasvustrategia
    a. Kasvuhakuisuus: Erittäin voimakkaasti kasvuhakuinen
    b. Kasvustrategia: Aggressiivinen kasvustrategia, tukena pääomarahoitusta. Investoi merkittävästi myyntiin ja markkinointiin
    c. Tavoitteet ja motiivit: Voimakas kasvu: ”markkina haltuun”, voitollisuus tai riskien välttäminen ei vielä yrityksen nykyisessä kasvuvaiheessa ollut tärkeää

TAULUKKO 4 Haastateltavien roolikuvaukset

Rooli	**Roolikuvaus**	**Tietoturvaosaaminen**
Operatiivinen johtaja (COO) (1. ja 3.haastattelu)	Kuului yrityksen perustajajäseniin. "*…titteli ei ehkä ihan vastaa mun toimenkuvaa tällä hetkellä… Kaikki tekee vähän kaikkea, mutta enemmän mä teen noita kaikkia teknisiä juttuja, mutta myös kaikkee hallinnollista sun muuta. Rooli on vähän satunnainen.*" Koulutukseltaan insinööri ja ammatilliselta taustaltaan ohjelmistokehittäjä.	COO oli käynyt itsenäisesti tietoturvakursseja verkossa ja opiskellut asiaa, mutta mitään alan tutkintoa ei häneltä varsinaisesti löytynyt. Tietoturvan perusteet olivat hänellä hallussa: hän oli opiskellut asiaa koulussa ja omatoimisesti paljon enemmän. Aikaisemmista työpaikoista oli kertynyt myös tietotaitoa tietoturva-asioihin liittyen.
Tekninen johtaja (CTO) (2. ja 3.haastattelu)	Kuului yrityksen perustajajäseniin. Vastasi järjestelmien kehitys- ja ylläpitotyöstä, mutta rooli oli siirtynyt ajan myötä yhä enemmän myyntiin ja markkinointiin. Koulutukseltaan insinööri ja ammatilliselta taustaltaan ohjelmistokehittäjä.	Tietoturvan perusteet olivat hyvin hallussa: oli opiskellut asiaa koulussa ja omatoimisesti paljon enemmän. Aikaisemmista työpaikoista oli kertynyt tietotaitoa tietoturva-asioihin liittyen.
Muu henkilöstö (Ei haastateltu), kuvaus perustuu COO:n ja CTO:n kertomuksiin	Erikoistuminen yrityksen sisällä oli toistaiseksi vähäistä. ”Kaikki osallistuivat kaikkeen” ja työtehtävät vaihtelivat, mutta ensisijaisesti pyrittiin tekemään roolien sisäisiä tehtäviä. Selkein rooli löytyi myynti- ja markkinointipuolelle palkatulta työntekijältä. Osalla rooli painottui enemmän tekniseen puoleen ja osalla enemmän myyntiin ja markkinointiin. Kaikki työntekijät olivat korkeakoulutettuja taustaltaan (AMK / yliopisto).	Ei alan koulutusta tai merkittävää kokemusta. Tietoturvaan liittyvät tekniset asiat ja kouluttaminen olivat pääasiassa COO:n ja CTO:n vastuulla.

5 TULOKSET

Tutkielman osana toteutettiin pienimuotoinen tapaustutkimus, jossa selvitettiin pienen, voimakkaasti kasvuhakuisen, suomalaisen startup-yrityksen tietoturvainvestointitarpeita, investointistrategiaa ja investointiprosessia. Tulokset raportoidaan seuraavassa järjestyksessä: Luku 5.1 pohjustaa tuloksia esittelemällä tapausyrityksen toimintatapoja riskienhallinnan ja tietoturvan saralla. Luku 5.2 kertoo tietoturvainvestoinneista tapausyrityksessä: yrityksen tietoturvainvestointistrategiasta ja investointiprosessista. Luvussa 5.3 esitetään, miten yrityksen tietoturvainvestointitarpeet muuttuvat yrityksen kasvaessa. Luku 5.4 sisältää yhteenvedon tuloksista. (Yrityksen tekniseen johtajaan viitataan lyhenteellä CTO ja operatiiviseen johtajaan lyhenteellä COO.)

5.1 Riskienhallinta ja tietoturvakulttuuri tapausyrityksessä

Riskienhallinta oli haastattelujen aikaan tapausyrityksessä vielä hyvin epämuodollista ja epäsäännöllistä. Rahoitusta hakiessa sitä oli vähän alustettu, mutta riskienhallintaa ei ollut vielä integroitu syvemmin yrityksen toimintaan. Riskienhallinta ei näkynyt erityisen paljon päivittäisessä tekemisessä, joka vei valtaosan ajasta; tulevaisuuden kannalta oli mietitty suuria linjoja, mutta muuten johdon fokus oli nykyhetkessä. CTO:n mukaan riskienhallinta näkyi parhaiten yrityksen toiminnassa siten, että asioita suunniteltiin etukäteen ja asioista otettiin selvää, kun lähdettiin tekemään jotain uutta. SWOT-analyysia hyödynnettiin riskienhallinnan työkaluna "isommissa haaroissa" ja apuvälineenä kokonaiskuvan kartoittamisessa asioissa, kuten yritystoiminnan laajentaminen, mihin suuntaan yritystä viedään jne. Muodollinen riskienhallintaprosessi nähtiin tulevaisuudessa hyödyllisenä, ja riskienhallintaa olikin jo yritetty viedä yrityksessä asteittain muodollisempaan suuntaan.

Asiakkaat, toimittajat tai muut yhteistyökumppanit eivät olleet vielä toistaiseksi esittäneet vaatimuksia riskienhallinnan suhteen. COO:n mukaan oletettavasti yrityksen seuraava rahoituskierros vaatii todisteita riskienhallinnasta (riskienhallinta-analyysi). Tulevien rahoituskierrosten vaatimukset olivat siten suurin motivaattori kehittää riskienhallintaa.

Merkittävimmät riskit olivat ulkopuolisia uhkia, joihin yritys ei voinut itse vaikuttaa. Erilaiset tuntemattomat riskit (Sommer ym., 2009) korostuivat; erityisesti haastatteluissa nousi esiin kansainvälistymiseen liittyviä haasteita, kuten poliittinen tilanne kohdemaissa, kulttuurierot, lainsäädäntö ja tullit. Tietoturvariskit priorisoitiin korkealle riskien joukossa. Tietoturva nähtiin yrityksen toimintaedellytysten perustana ja pohjapilarina, jonka päälle rakennetaan järjestelmiä eikä toisinpäin. Taulukossa 5 listataan haastateltavien mainitsemia keskeisimpiä riskejä.

TAULUKKO 5 Haastatteluissa esiin nousseita riskejä

Riski:	**Riskin nosti esiin:**	**Liittyy mihin:**	**Riskin kuvaus:**
Ongelmat tullissa	COO / CTO	Kansainvälistyminen	Tullisäädökset eri maissa ym. voivat vaikeuttaa yrityksen toimintaedellytyksiä.
Kulttuurierot	COO / CTO	Kansainvälistyminen	Kohdemaan kulttuurierot voivat aiheuttaa hankaluuksia.
Vierasmaalainen lainsäädäntö	COO / CTO	Kansainvälistyminen	Lainsäädännön muutokset, vastuukysymykset ym. voivat aiheuttaa ongelmia.
Poliittinen tilanne kohdemaassa	CTO	Kansainvälistyminen	Kohdemaan poliittiset levottomuudet ym. muutokset ulkomaisten yritysten toimintaedellytyksissä voivat aiheuttaa ongelmia.
Tuote / palvelu ei toimi	COO	Liiketoiminta	Yrityksen palvelu ei toimi halutulla tavalla.
Myynti ei lähde käyntiin	COO	Liiketoiminta	Yrityksen palvelulle ei ole riittävästi kysyntää.
Yrityksen rooli ekosysteemissä	COO	Liiketoiminta	Palvelu kilpailee suuria verkkokauppa-alustoja vastaan, eli toimii yhtenä välikätenä lisää osana suurta ekosysteemiä. Riskinä on, että merkittävät alustajärjestelmät alkaisivat jostain syystä estää heidän yrityksensä toimintaa.
Tietoturva ja järjestelmän stabiilius	COO / CTO	Tietoturva	Tietoturva ja järjestelmän stabiilius koetaan merkittävänä tulevaisuuden riskinä. "Tällä hetkellä ei vielä erityisen merkittävä riski" COO 1. haastattelu

Tapausyrityksessä karsastettiin hierarkkista organisaatiorakennetta ja keskinäisen luottamuksen merkitys korostui. Henkilöstölle annettiin yrityksessä paljon vapautta ja vastuuta. Tapausyrityksessä ei haluttu edetä kieltämisen kautta. Yrityksen ensimmäinen rahallinen investointi tietoturvaan – salasananhallintajärjestelmä – otettiin hyvin vastaan, koska sen tarve ja hyödyllisyys oli perusteltu.

> ”Ei, ei oo tarvetta kieltää mitään. Luotetaan siihen, että jos joku lähtee ylipäätään roottaamaan omaa kännykkäänsä tms., nii se tietää, mitä on tekemässä.” COO 3. haastattelu

Tietoturvan nykytilasta haastatelluilla oli yhtenäinen näkemys: asiat olivat melko hyvällä mallilla molempien mukaan. Asenne oli hyvin luottavainen ja itsevarma.

> ”Mitäs muuta. Aika hyvin meil on, mä veikkaan et meil on niiku keskimääräistä, tän kokoista yritystä, paremmat… Ku mä ite näistä jonkin verran tiiän, nii mä oon niitä… Niitä laittanu… Mut siis aika… Sillee kaikki perusasiat on kyl kunnossa. -- ”Tietoturvan nykytila… Mä sanoisin et se on ihan hyvä. Ei oo oikeestaa... ihan hirveästi nyt semmosia mitään kovin kriittisiä kehityskohteita oo…” COO 1. haastattelu

> “Ainaki se on tähän asti toiminu, kyl se ihan varmaan hyvällä mallilla on, että tota, en mä siitä sen enempää osaa sanoo, ts. osaa eritellä sitä sillee, että… se on ihan hyvä, uskoisin…” CTO 2. haastattelu

Tietoturva-asiat haluttiin lähtökohtaisesti pitää yrityksen sisällä ja hoitaa itse mahdollisimman paljon. Kuka tahansa saattoi yrityksessä tarttua esimerkiksi tiedonkäsittelyyn liittyviin ongelmiin, mutta ensisijaisesti tietoturvatiimi yrityksessä oli COO + CTO (COO:n rooli tietoturva-asioissa korostui). Tietoturvan merkitys nähtiin tärkeänä ja olennaisena osana liiketoimintaa. Sitä ei voinut sivuuttaa tai poissulkea. Molempien haastateltavien mukaan tietoturvaa ei voinut erottaa kaikesta muusta tekemisestä, sillä tietoturvalliset toimintatavat olivat olennainen osa kehitystyötä ja suunnittelua.

Tietoturvakäytänteitä, menetelmätapoja tai yhteisiä sääntöjä ei ollut dokumentoitu kirjalliseen muotoon, mutta joistain yhteisistä käytännöistä oli sovittu: esimerkiksi joka paikkaan vaadittiin eri salasanat ja salasanoja ei saanut tallentaa salaamattomina. Käyttöoikeuksien hallintaa oli pohdittu ja toteutettu. Yrityksessä oli otettu käyttöön yhteinen salasananhallintajärjestelmä. Yritys salasi kaiken tietoliikenteensä, palvelimia päivitettiin säännöllisesti ja yrityksessä pidettiin huolta, että käytössä olevat salausjärjestelmät eivät olleet vanhentuneita.

Kaikki tekivät yrityksessä töitä etänä, ja kaikilla oli sitä myötä myös omat laitteensa. Yritys ei ollut vielä hankkinut yrityslaitteita työntekijöille eikä hankintaan vielä lähitulevaisuudessa ollut resursseja. Tätä ei kuitenkaan nähty tietoturvan kannalta ongelmana ja tietoturvasyiden takia ei ollut yleisesti jätetty asioita tekemättä tai ottamatta teknologioita käyttöön. Tietoturvaa mietittiin käyttöön otettavia teknologioita ja työkaluja valittaessa; esimerkiksi se, että teknologian tarjoaja oli yksi suurimmista, koettiin yleensä hyvänä merkkinä.

Yrityksessä ei ollut vaatimuksia henkilöstön käyttämille laitteille tai ohjelmistoille, ja henkilöstön tietoturvakäyttäytymistä ei valvottu. Siitä ei esimerkiksi ollut vielä varmaa tietoa ensimmäisen haastattelun aikaan, olivatko kaikki yrityksessä ottaneet hankitun salasananhallintajärjestelmän käyttöön. Tietoturva-asioissa, kuten muissakin asioissa, korostui keskinäinen luottamus ja luottamus henkilöstön riittävään osaamiseen.

5.2 Tietoturvainvestoinnit tapausyrityksessä

Tapausyrityksellä ei ollut kirjallista tietoturvainvestointistrategiaa. Tietoturvainvestointeja ei yrityksessä ollut vielä ensimmäisen haastattelun aikaan juuri mietitty. Yritys oli tehnyt vain yhden suoran rahallisen investoinnin tietoturvaan: salasananhallintajärjestelmä. Muuten tietoturva pyrittiin huomioimaan osana turvallista ohjelmistokehittämistä, mutta erillisiä investointeja tietoturvaan ei ollut juuri tehty. Tietoturvan huomioimiseen ja kontrollien rakentamiseen käytettyä aikaa ja vaivaa ei pidetty varsinaisina investointeina, vaan osana normaalia ohjelmistokehitystyötä. Taulukko 6 kuvaa haastateltavien mainitsemia tietoturvainvestoinneissa painotettavia asioita suhteessa muihin investointeihin. Taulukossa käytetään esimerkkinä muusta investoinnista markkinointikampanjaa, koska markkinointikulut olivat yrityksessä henkilöstökulujen jälkeen merkittävimmässä roolissa.

TAULUKKO 6 Tietoturvainvestoinnit suhteessa muihin investointeihin

	Tietoturvainvestointi	**Muu investointi (esim. markkinointikampanja)**
Tuotto-odotus	Ei mitattu	ROI
Investoinnin syy	Lainsäädännön vaatimus, asiakkaan vaatimus	Kasvu, rahallinen tuotto
Toteutus	Mieluiten itse, avoimen lähdekoodin ratkaisuilla	Yhteistyökumppanin kanssa
Investointipäätös	Keskustelun kautta	Keskustelun kautta
Painotettavia tekijöitä	Täyttää minimivaatimukset, tasapaino eri ominaisuuksien välillä; ennen kaikkea turvallisuuden ja hinnan tasapaino	Tuotto-odotus
Keskeisimmät resurssirajoitteet	Aika, (raha), (motivaatio)	Raha
Investoinnin asema tärkeysjärjestyksessä	Vain pakolliset investoinnit toteutetaan (mutta priorisoidaan korkealle)	Priorisoidaan korkealle, merkittävin kustannuserä henkilöstökulujen jälkeen

Tietoturvainvestointitarve tuli tapausyrityksessä ensisijaisesti yrityksen ulkopuolelta: keskeisellä sijalla olivat lainsäädännön vaatimukset ja asiakkaan vaatimukset. Tietoturvainvestoinneissa korostui ensisijaisesti investoinnin kyky täyttää sille asetetut vaatimukset. Investoinnin kustannukset olivat sen jälkeen tärkein tekijä. Tietoturvainvestoinneille ei asetettu tuotto-odotusta tai käytetty muitakaan mittareita. Asiantuntijoiden suosituksille ei annettu juuri painoarvoa investointipäätöstä tehtäessä. Investointi tietoturvaan toteutettiin, jos oli pakko, mutta vapaaehtoiset investoinnit jäivät muiden investointien jalkoihin (pl. salasananhallintajärjestelmä). Yrityksen voimakas kasvuhakuisuus näkyi myös investointipäätöksissä. Yritys investoi mieluummin suoraan kasvua tuoviin

asioihin, kuten henkilöstön palkkaukseen ja markkinointiin. Muissa investoinneissa korostui investoinnin tuotto-odotus (raha).

> ”Ei varsinaisesti mitään rahallisia investointeja oo, paitsi ainut maksullinen työkalu on toi salasananhallinta, ei mitään muuta maksullista löydy. (ei ainakaa kyl tuu mielee et ois…) Kaikki, muuten ne tietoturvainvestoinnit on ollu, et on ollu noin niinku hyvät tietoturvakäytännöt.” COO 1. haastattelu

Tapausyrityksessä meni ”satasten” kohdalla raja hankinnoissa, joita harkittiin jo enemmän. Pakollisten tietoturvainvestointien kohdalla investointilaskelmat koettiin melko turhiksi. Ensisijaisesti yrityksessä investoitiin kasvua tuoviin asioihin; tietoturvan piti olla riittävällä tasolla, mutta jos ei ollut mitään pakottavaa syytä investoida resursseja tietoturvaan, muut asiat menivät edelle.

> ”Tuotto-odotusta… Öö… Niiku rahallista tuotto-odotusta… varmaan sitä pystyiski… tai siis totta kai kaikkee voi aina laskeskella ja sillee, mutta en mä ite nää että sitä kannattais… tai sillee, että se tuotto-odotus on niinku se, että ei tule mitään tietovuotoja, ja että hommat toimii, niin ku on suunniteltu. Nii se on se. Mut varmasti sille vois jonku rahallisen arvon laskee… mut sit taas se on vähän sellanen, mikä nyt vaan pitää olla ja hoitaa, nii en mä tiiä, onko siinä sit, et saat jonku lukeman sun naaman eteen, nii mitä lisäarvoo se tuo sitte..” CTO 2. haastattelu

> ”Tietoturva on semmonen kohde, mihin pistetään justiinsa vaan se vaadittu” COO 3. haastattelu

Tietoturvainvestoinneille oli haastateltavien mukaan vaikea laittaa rahallista arviota. ”Ylimääräisiä” (vapaaehtoisia) investointeja tietoturvaan ei koettu kilpailuetua tuovina asioina tai erityisen hyödyllisinä. Tietoturva kuitenkin pyrittiin huomioimaan päivittäisessä tekemisessä ja kehitystyössä. Tietoturvainvestoinneissa tärkeää oli tasapaino eri ominaisuuksien välillä: ennen kaikkea turvallisuuden ja hinnan tasapaino. Ensin katsottiin, että vaatimukset tietoturvan suhteen täyttyvät, ja vasta sen jälkeen hintaa.

> ”Hinta on harvoin ongelma näissä. Tosi monet on open sourcea ja ilmaisia noista nii se harvoin on hinnasta kii… Kai se on taas se tasapaino eri ominaisuuksien välillä. Turvallisuuden ja hinnan tasapaino. Pitää miettiä sellanen sopiva…” COO 3. haastattelu

Ensimmäisessä haastattelussa yrityksen operatiiviselta johtajalta kysyttiin näkemystä yrityksen investointitarpeista eri tietoturvan osa-alueilla (estämiskyky, havaitsemiskyky, palautumiskyky). Ensimmäisen haastattelun aikaan COO näki estämiskyvyn ehdottomasti tärkeimpänä. Estämiskyvyn koettiin olevan yleisesti hyvällä tasolla, mutta yrityksen palautumiskyvyssä ja havainnointikyvyssä nähtiin puutteita. COO kuitenkin koki, että puutteiden korjaaminen ei todennäköisesti vaatisi rahallista investointia, vaan investoinnit voitaisiin toteuttaa avoimen lähdekoodin ratkaisuilla ilmaiseksi. COO:lla oli hallussaan riittävä tekninen osaaminen tarvittavien kontrollien toteuttamiseksi, mutta suurimpana esteenä nähtiin ajan puute. Myös CTO näki toisessa

haastattelussa estämiseen keskittyvät suojaavat kontrollit tärkeimpänä. Toisaalta kolmannen haastattelun kohdalla COO:lta kysyttäessä, miksi hän näki estämiskyvyn tärkeimpänä, suhtautuminen asiaan oli muuttunut: yrityksen palautumiskykyyn panostaminen nähtiin nyt tietoturvan kannalta tärkeimpänä tekijänä. Ensimmäisessä haastattelussa yrityksen operatiivinen johtaja kommentoi yrityksen varautumista tietoturvauhkiin palautumiskyvyn osalta seuraavasti:

> "Palautumiskyky on semmone missä meiän pitäis skarppaa… Et ois tota tietokannan palauttaminen ja tämmönen… Nii se pitäis olla, et siihe ois iha selvät prosessit. Ja se ois pitäny harjotella et se toimii. Se on kyllä yks semmone mikä pitäis tehä, mut ei oo vielä ollu aikaa." COO 1. haastattelu

> ” -- Ja tietoturvainvestointeja… Ei varsinaisesti oo mitään, mihin tarvis investoida tällä hetkellä ni… Oikeastaan, no ainoot on just ne, että sais paremmat, ne tota, paremmat palautusjärjestelmät, että pystyy palautumaan, ja sitte kaikki menee salassa ja kaikki tiedot häviäis, nii siihe sais suoraviivaisen järjestelmän et saa palautettua. Ja se ois testattu, että se toimii. Nii se on se, mihin pitäis investoida. Mut seki on periaatteessa ajan investointia... Ei minkään, mikä tuota rahaa vaatis, lähinnä omaa aikaa… Öö… Ja oliks siin viel jotain muuta mitä sitte oli kehitys… Olihan siinä vielä joku muuki. Mut ei varsinaisesti oo mitään tietoturvainvestointeja noin niinku mietittykkään. Ainakaan mitään rahallisia investointeja. Ei oo oikeastaan mitään, mistä saa hirveästi hyötyä.” COO 1. haastattelu

Aika esiintyi keskeisimpänä resurssirajoitteena. Myös motivaatio toteuttaa ei-kriittiseksi koettuja investointeja tietoturvaan oli matala. Pääpaino ensimmäisen haastattelun aikaisissa suojaavissa teknisissä kontrolleissa oli estämisessä. Havaitsemiseen ja tunnistamiseen liittyviä kontrolleja COO kommentoi seuraavasti:

> ”Joo toi detective on kans semmonen, eli sä huomaat, jos nyt jotain tapahtuu, nii on kans semmone, mitä pitää parantaa, mut tällä hetkellä, niiku kaikki lokataa, mut se on semmosta et siel ei oo mitään hälytystä, et hei, nyt tapahtuu jotain outoo. Et sinne pitäis asentaa. Asentaa sitte joku, mikä tarkkailee sitä et nyt tapahtuu jotain outoo. Et se on kans kyllä…” COO 1.haastattelu

Ensimmäisen haastattelun edetessä COO alkoi kiinnittää enemmän huomiota nykyisin puutteisiin. Kolmannen haastattelun kohdalla (n. kuukausi myöhemmin), yrityksen tietoturvainvestointistrategiasta (ja strategian painotuksesta) kysyttäessä, yrityksen suojausprioriteettien painotus oli muuttunut. Palautumiskyky ja käyttäjien tietoturvakoulutus olivat nousseet ykköspriorioteeteiksi.

> “Palautumiskyky, palautumiskyky on tietoturvan kannalta ehdottomasti se tärkein. Ehdottomasti palautumiskyky. Ja sitte käyttäjien tietoturvakoulutus. Ne on niinku ne kaks.” CTO 3. haastattelu

Puutteiden korjaamiseen vaadittavien tietoturvainvestointien kohdalla korostuivat resurssien rajallisuus (pääasiassa aika) ja ”tee-se-itse”-

toteuttamistapa. Tietoturvakäytänteissä ja teknologioissa nähtiin parantamisen varaa, mutta koska ongelmat eivät olleet kriittisiä, niiden korjaaminen saattoi odottaa. Käyttäjien tietoturvakoulutuksen tärkeys hyvän tietoturvan kannalta tiedostettiin, mutta siihen ei vielä yrityksen nykyisessä kasvuvaiheessa panostettu kuitenkaan resursseja. Tietoturvakoulutuksia ei ollut järjestetty yrityksen sisäisesti vielä haastattelujen aikaan, vaan ne nähtiin tarpeellisena vasta joskus tulevaisuudessa.

Investointien priorisointi

Oli osin tapauskohtaista, priorisoitaisiinko yrityksessä investointien kohdalla tuotto-odotus, kasvu vai tietoturva-asiat. Kriittiset ja tärkeät investoinnit tietoturvaan oltiin valmiita toteuttamaan kustannuksista suuremmin välittämättä ja nopealla aikataululla, sillä tietoturva nähtiin toiminnan kulmakivenä. Vapaaehtoiset ja vähemmän tärkeät investoinnit tietoturvaan saivat sen sijaan odottaa, ja muut investoinnit menivät edelle. Tietoturvan huomioiminen kuului yrityksessä tärkeänä osana ohjelmistokehitystyöhön, mutta tietoturva-asioihin käytettyä aikaa ei koettu järkevänä eritellä. CTO vastasi seuraavalla tavalla kysymykseen investointien priorisoinnista (tietoturva vrt. markkinointi):

> "Nii se on vähän… ei varmaan voi sillee sanoa, että automaattisesti menis jompi kumpi edelle… riippuu taas tilanteesta, toises tilanteessa voi mennä toinen edelle ja toises toinen, et se just, jos siellä on joku hirvee tietoturva-aukko ja sitte rahaa on tilillä 500€ jäljellä ja sen korjaaminen maksaa 500€, nii kyl se ny varmaan käytetään siihen sitte." CTO 2. haastattelu

Tilannetta, jossa tärkeä investointi tietoturvaan kaatuisi hallituksessa jonkun vastustukseen, ei pidetty realistisena. Pakolliset tietoturvainvestoinnit tehtiin, oli tilanne mikä tahansa. COO ja CTO olettivat, että tietoturvainvestoinnin saa kyllä läpi yrityksen hallituksessa, jos sen pystyi perustelemaan, että investointi oikeasti tarvittiin. Esim. tietoturvasertifiointia ei pidetty tarpeellisena.

> "Se on ihan totta. Joo no niin… Että… Ja myöskin, että ei halua tehdä tietoturvainvestointia… Riippuu varmaan aika paljon myös siitä investoinnistakin. Jos se on taas joku sellainen et se pitää olla, niin sit se tehään... Sit se pitää vaan hankkia ja pitää saada hoidettua. Sit taas, jos se on joku semmoinen vapaaehtoinen juttu, nii ehkä se sit menee sinne markkinointiin tai säästöön, jos ei saa kaikkii mukaan, nii ei sit auta." CTO 3. haastattelu

Tietoturvainvestointien arviointi (investointipäätöstä tehtäessä):

Investointipäätöstä tehtäessä painotettiin asiakkaan ja lainsäädännön vaatimuksia. Asiantuntijoiden suosittelulle tai muille vastaaville asioille ei annettu painoarvoa. Lähtökohtaisesti yrityksessä haluttiin ottaa asioista itse selvää.

> "Eniten vaikuttaa asiakkaiden vaatimukset. Sit vaikuttaa aika paljon se mitä tehään. Jos asiakas haluu, että vaik joku integraatio meidän ja heidän välillä on… Siinä on

> vaikka joku tietty… Tietty salausmenetelmä, nii se tehää sen mukaan…" COO 3. haastattelu

Erilaiset kvantitatiiviset menetelmät (ROI, ROSI, UM ym.) tietoturvainvestointeja arvioitaessa nähtiin sinänsä käyttökelpoisina työkaluina:

> "Kyl toi vois toimiakki. Joo, kyl tosta varmasti jonkinnäköisen arvion saa tehtyä… Mahdollisesti joo. Jotain tommosta vois käyttää, jos tarvii." COO 3. haastattelu

Toistaiseksi näitä menetelmiä ei kuitenkaan nähty nykyhetkessä tarpeellisina. Suurin osa investointipäätöksistä pystyttiin tekemään keskustelun kautta, ilman erillisiä työkaluja tai laskelmia.

> "Luulen että tässä vaiheessa se on aika selvää, että mitä me tarvitaan ja mitä me ei tarvita… Että mä luulen et nää on kans vähän semmoisia, että näitä tarvii vasta sit ku on oikeesti vähän isompi firma, ja pitää oikeesti miettiä, että mikä nyt on tarpeellinen ja mikä ei. Ku tällä hetkellä se on sillee vielä aika selkeetä, ilman sen kummempia laskuja." COO 3.haastattelu

Mitä haasteita investointiprosessiin liittyi?
Raha, aika (ja motivaatio) olivat keskeisimmät resurssirajoitteet; rahaa ei haluttu käyttää kuin pakollisiin tietoturvainvestointeihin, muuten investoinnit tehtiin kasvu edellä. Tapausyrityksessä tarvittavan osaamisen puute ei aiheuttanut ongelmia. Kaikkia mahdollisia investointityyppejä (esim. tietoturvasertifiointi, tietoturvavakuutukset) ei nähty nykyhetkessä, eikä lähitulevaisuudessa, tarpeellisina, joten niitä ei olisi hankittu, vaikka yrityksellä olisi ollut tarvittavat resurssit. Raha olisi siinä tapauksessa suunnuttu muihin investointeihin.

Tietoturvainvestointiprosessi
Tarvittavan tietoturvainvestointiprosessin kannalta, sillä oli suuri merkitys, koettiinko investointi tietoturvaan pakolliseksi vai vapaaehtoiseksi. Pakollinen investointi ei edellyttänyt "kummoista prosessia" ja toisaalta vapaaehtoisia investointeja tietoturvaan ei toistaiseksi juuri tehty. Vapaaehtoisten tietoturvainvestointien kohdalla raha ja aika käytettiin mieluummin muihin asioihin. Investointi salasananhallintajärjestelmään oli poikkeus, sillä investointipäätös perustui vapaaehtoisuuteen ja tuli yrityksen sisältä (COO oli todennut työkalun hyödylliseksi aiemmassa työpaikassaan). Hankitun salasananhallintajärjestelmän kohdalla investointiprosessi eteni seuraavasti:

1. *Investointitarve syntyy*: Salasananhallintajärjestelmän tapauksessa investointitarve tuli (poikkeuksellisesti) yrityksen sisältä. COO koki, että hallintatyökalusta olisi hyötyä, ja koska investointi ei vaatinut rahallisesti merkittäviä panostuksia, se oli helppo hankkia koko yrityksen käyttöön.
2. *Vaihtoehtojen tarkastelu*: Seuraavana vuorossa oli minimivaatimusten määrittäminen ja vaihtoehtojen haku (verkkohaku; avoimen lähdekoodin ratkaisuja suosittiin).

3. *Vaihtoehtojen karsiminen*: COO katsoi, mitkä vaihtoehdoista täyttävät minimivaatimukset (sopivuus, hinta-laatusuhde, hyvät arvostelut). Jäljelle jäävät vaihtoehdot järjestettiin hinnan mukaan ja kaikista kalliimmat ratkaisut hylättiin.
4. *Ominaisuuksien vertailu*: Tämän jälkeen COO vertaili jäljellä olevien työkalujen joukosta minimivaatimukset ylittäviä ominaisuuksia, joille saattaisi olla yrityksessä käyttöä, työkalun laatua suhteessa hintaan ja käyttäjäarvosteluja.
5. *Valinta ja hankintapäätös*: Lopulta COO teki valinnan edellä kuvatun kriteeristön perusteella. Salasananhallintajärjestelmä oli rahallisesti pieni investointi, joten COO saattoi tehdä hankintapäätöksen itsenäisesti ja tiedottaa hankinnasta muille jälkikäteen.

Salasananhallintajärjestelmän kohdalla investointiprosessi oli helppo ja nopea verrattuna esimerkiksi jo toteutettuihin isomman rahan markkinointikampanjoihin. Salasananhallintajärjestelmää ei pidetty hankintahetkellä varsinaisesti edes investointina, joten COO saattoi tehdä päätöksen itse ja tiedottaa asiasta hankinnan jälkeen muille.

> "Ei ollut tarvetta kysellä muilta asiasta. Ite katoin mikä on paras ja otin sen." COO 1. haastattelu

Suhtautuminen eri tietoturvainvestointityyppeihin

Kolmannessa haastattelussa haastateltavilta kysyttiin suhtautumista eri tietoturvainvestointityyppeihin. Investointityyppien kohdalla oli suuria eroja, koettiinko ne tarpeellisiksi vai ei.

Tietoturvasertifiointia ei nähty hyödyllisenä, joten siihen ei pidetty mielekkäänä käyttää rahaa. Sertifiointia ei nähty hyödyllisenä myöskään markkinointi turvallisuudella tms. mielessä.

Tietoturvavakuutuksia ei vielä tässä vaiheessa yrityksen kasvua koettu tarpeelliseksi. Yrityksellä oli vastuuvakuutuksia, jotka kattoivat CTO:n mukaan joitain tietoturva-asioita.

Maksullisen tietoturvakoulutuksen kohdalla mielipiteissä oli eroja. COO ei nähnyt sitä kovin mielekkäänä investointina, koska netissä oli ilmaiseksi niin paljon hyvää koulutusmateriaalia saatavilla. CTO ei tyrmännyt yhtä jyrkästi asiaa, jos koulutuksen laadukkuudesta oli takeita. Myös näkemyksessä tietoturvakoulutuksen tarpeellisuudesta ja ajankohdasta oli eroja. CTO:n mukaan koulutus voi olla jossain vaiheessa "ihan varteenotettava" investointi, myös maksullinen. Haastatteluhetkellä yritys pärjäsi kuitenkin vielä omin resurssein. COO suhtautui asiaan nihkeästi.

Taulukko 7 kuvaa tapausyrityksen suhtautumista eri tietoturvainvestointityyppeihin.

> "Tollasesta (tietoturvasertfiointi) ei oo kyllä meille mitään arvoa tällä hetkellä. Loppukäyttäjät ei tiedä näistä mitään, en usko, että on fiksua investoida." COO 3. haastattelu

”Se on ihan totta. Joo ei oo niinku… Jos se maksais kympin, nii sitte niiku mietittäis, ja siltiki vois olla, että en hankkis…” CTO 3. haastattelu

TAULUKKO 7 Tapausyrityksen suhtautuminen eri tietoturvainvestointityyppeihin

Investointityyppi	**Ajankohta**	**Resurssirajoite**	**Tarpeellisuus**
Laiteinvestointi (esim. yrityslappärit)	Kun tarvittavat resurssit kasassa (toistaiseksi moni muu investointi menee vielä edelle)	Raha	Tarpeellinen mutta ei vielä nykyhetkessä tai lähitulevaisuudessa tarvittavia resursseja
Tietoturva-asiantuntijan palkkaus	Edellyttää huomattavaa kasvua	Raha	Tarpeellinen mutta ei vielä nykyhetkessä tai lähitulevaisuudessa resursseja (joku saattaa myös erikoistua yrityksen sisältä)
Maksullinen tietoturvakoulutus	Ei haluta käyttää rahaa nykyhetkessä, mahdollisesti tulevaisuudessa (edellyttää huomattavaa kasvua)	Raha, motivaatio	Ei vielä nykyhetkessä tarpeellinen. Suhtautumisessa eroja; CTO kannattaa varauksellisesti, COO ei pidä järkevänä käyttää asiaan rahaa
Ei-pakollinen investointi teknologiaan (esim. web-applikaatioiden haavoittuvuusskanneri)	Edellyttää huomattavaa kasvua	Raha, aika, motivaatio	Ei vielä hetkeen tarpeellisia, lisäksi mahdollisuus hyödyntää avoimen lähdekoodin ratkaisuja
Tietoturvasertifiointi	-	Motivaatio, (raha)	Ei tarpeellinen
Tietoturvavakuutus	Edellyttää huomattava kasvua	Motivaatio	Ei tarpeellinen toistaiseksi

5.3 Yrityksen tietoturvainvestointitarpeiden kehitys yrityksen kasvaessa

Haastatteluissa kävi ilmi, että hyvin useiden tietoturvainvestointityyppien kohdalla, niitä ei nähty yrityksen nykyhetkessä tarpeellisina, saati ihan lähitulevaisuudessa. Pakolliset investoinnit oltiin valmiita toteuttamaan kustannuksista huolimatta, mutta lähtökohtaisesti tietoturva-asioihin ei mieluiten käytetty rahaa, vaan asioita toteutettiin tarvittaessa mahdollisimman paljon itse ja erinäisillä avoimen lähdekoodin ratkaisuilla. COO esimerkiksi koki, että systemaattinen lähestymistapa yhteisiin sovittuihin tietoturvakäytäntöihin

(yhteisten pelisääntöjen kirjaaminen kirjalliseen muotoon, seuranta ja valvonta yms.) ei ollut vielä yrityksessä ajankohtaista. CTO suhtautui asiaan vähemmän jyrkästi, ja koki yhteisistä käytännöistä sopimisen ja henkilöstön koulutuksen tietoturva-asioista jo nyt jossain määrin hyödylliseksi. CTO:n mukaan monia asioita (ml. tietoturva) pystyi vielä tässä vaiheessa yrityksen kasvua ”ripotella” eri henkilöille, mutta kasvun edetessä pidemmälle yrityksessä oli jo oltava joku asiaan erikoistunut vastuuhenkilö, sillä tietoturva-asiat eivät olisi enää yhtä helposti hallittavissa.

Haastateltavilla oli eriävä näkemys tietoturvakouluttamisen tarpeesta ja ajankohdasta. CTO näki yleisten linjausten tekemisen tietoturvan suhteen jo nyt hyvänä ideana ja järkevänä, COO:n mukaan asialla ei vielä ollut kiirettä. CTO ja COO hoitaisivat lähtökohtaisesti itse nykytilanteessa muiden kouluttamisen, jos se toteutettaisiin. COO:n mukaan tiimin pienuuden takia vielä ei ollut tarpeellista pitää tietoturvakoulutuksia henkilöstölle. Henkilöstön kouluttaminen tietoturva-asioissa koettiin tarpeelliseksi vasta myöhemmin, kun yrityksen henkilömäärä on moninkertaistunut nykyisestä. Lukuina mainittiin +10 henkilöstä jopa sataan henkilöä, jolloin tietoturvakoulutusta pitää vasta harkita: ”varmaan siinä vaiheessa vois jotain koulutustakin harkita”. Tällöin oletuksena oli, että koulutuksen luultavasti järjestäisi yrityksen sisäisesti (palkattu tai yrityksen sisäisesti erikoistunut) tietoturva-asiantuntija.

> ”No sanotaan sitte joskus myöhemmin, ku meil alkaa olla enemmän ihmisii, sit pitää alkaa jo enemmän tekee sitä… Just tietoturvakäytännöt ja social engineerinki näkökulmasta, ja siitä et kaikki oikeesti sit käyttää sitä salasananhallintajärjestelmää…. Se on semmoista varautumista, et pitää jossain vaiheessa tehä, mut meil on ny nii pieni tiimi, nii ei viel tarvi semmost organisoimaa… organisoivaa tapaa…” COO 1. haastattelu

Kolmannen haastattelun aikana keskustelu eteni seuraavasti:

> COO: Työtekijäraja.. Ihan todella vaikeeta… Sanotaanko että haitari on 20–100.
>
> CTO: Nii mä voisin sanoo ehkä että 10–100. Tai siis 10 - ääretön.
>
> COO: Kyl sataan mennessä melkeen pitää olla jo joku… Mut nii joku semmone…
>
> CTO: Nii no siis. On se varmaan todennäköisesti jo aikaisemminkin.

Ei-pakollisiin tietoturvainvestointeihin (eli esim. yrityksen sisältä tullut investointiehdotus) ei vielä nykyisessä kasvuvaiheessa haluttu yrityksessä käyttää juurikaan rahaa, mutta se nähtiin tulevaisuudessa mahdollisena. Asiat toteutettiin tarvittaessa mieluiten itse, hyödyntämällä erilaisia avoimen lähdekoodin ratkaisuja.

> “Siinä vaiheessa (ehkä) sit. Jos rahaa on, niin joo, mut tässä vaiheessa ei… Ei, kyl ne sitte ite toteutetaan, jollain avoimen lähdekoodin jutuilla… Että en laittais viittä tonnia tietoturvaskanneriin, ja en usko, että ihan lähitulevaisuudessakaan, mutta ehkä joskus mahdollisesti.” CTO 3. haastattelu

Yritykseen haluttiin tietoturvaan erikoistunut vastuuhenkilö jossain vaiheessa, mutta nykyisessä kasvuvaiheessa yritys koki pärjäävänsä vielä nykyisin resurssein. Tulevaisuudessa yritykseen palkattava DevOps-asiantuntija saa COO:n mukaan vastuulleen myös tietoturvan, koska he ovat yleensä asiasta hyvin perillä. Erillisen tietoturva-asiantuntijan palkkaamista yrityksen ulkopuolelta ei koettu välttämättömänä, sillä oli mahdollista, että joku yrityksen sisältä siirtyisi myöhemmin tarvittaessa kokoaikaisesti tietoturvasta vastaavaksi henkilöksi.

Merkittävimmät tulevaisuuden riskit, jotka edellyttivät investointia tietoturvaan

CTO piti merkittävimpänä uhkana henkilöstön tekemiä virheitä ym. organisaation sisältä tulevia asioita. COO:n mielestä merkittävin uhkakuva oli sosiaalinen manipulointi (social engineering). Tietoturva ja järjestelmän stabiilius koettiin merkittävänä tulevaisuuden riskinä, mutta ei vielä yrityksen nykyisessä kasvuvaiheessa. Teknisen velan kasautuminen ajan myötä nähtiin riskinä:

> ”No sitte alkaa tulla eri riskejä mieleen. Tai enemmän nää.. Ööö.. No sit mä sanoisin. Sit alkaa nousee enemmän toi tietoturva myöhemmin ja ylipäätänsä se kuinka stabiili se meiän järjestelmä on. Täl hetkel se ei viel oo niin merkittävä riski. Jos servu menee vaik minuutiks pariks alas tai jotain semmoista, ei oo kyllä käyny pitkään aikaan, mutta joku semmone, nii se ei oo tässä vaiheessa nii iso riski. Sit jos jossain vaiheessa kasvetaan, se alkaa olla jo huomattavasti, huomattavasti pahempi tilanne. Eli sanotaanko et alkaa noi tekniset asiat nousee pintaan… Tai niist tulee riskejä. Jos tässä vaiheessa tehään sitä technical debttiä, nii ku usein startupeissa meinaa käydä, nii ne sitte kasautuu myöhemmin… (riski)” COO 1. haastattelu

Tietoturvakoulutuksista keskusteltaessa COO näki tietoturvakoulutuksen sosiaalista manipulointia vastaan tärkeimpänä. Koulutus toteutettaisiin oletettavasti vastaavalla tavalla kuin hänen edellisessä työpaikassaan (koulutus oli järjestetty lyhyinä videoina, jotka henkilöstön piti kuitata katsotuksi.) COO ja CTO kokivat molemmat yleisesti aikaisemmista työpaikoista kertyneen hyvää kokemusta tietoturva-asioihin liittyen.

5.4 Yhteenveto tuloksista

Riskienhallinta oli haastattelujen aikaan tapausyrityksessä vielä hyvin epämuodollista ja epäsäännöllistä. Tietoturvan nykytilasta haastatelluilla oli yhtenäinen näkemys: asiat olivat melko hyvällä mallilla ja merkittäville lisäinvestoinneille tietoturvaan ei tässä vaiheessa kasvua ollut tarvetta. Tietoturva-asiat ja osaaminen haluttiin pitää yrityksen sisällä.

Tietoturvainvestointipäätöstä tehtäessä painotettiin asiakkaan ja lainsäädännön vaatimuksia. Asiantuntijoiden suosituksille tai muille vastaaville asioille ei annettu painoarvoa. Lähtökohtaisesti yrityksessä haluttiin ottaa asioista itse selvää.

Tarvittavan tietoturvainvestointiprosessin kannalta, sillä oli suuri merkitys, koettiinko investointi tietoturvaan pakolliseksi vai vapaaehtoiseksi. Pakollinen investointi ei edellyttänyt ”kummoista prosessia” ja toisaalta ei-välttämättömiä investointeja tietoturvaan ei toistaiseksi juuri tehty.

Yrityksen sisällä ei ollut erityistä tietoturvainvestointitarvetta tai halukkuutta lisäinvestointeihin. Pakottavat ja välttämättömät tietoturvainvestoinnit hoidettiin, mutta vapaaehtoiset investoinnit jäivät investointien priorisoinnissa muiden investointien taakse. Ensisijaisesti investoitiin kasvua tuoviin asioihin.

Investointipäätökset tehtiin tapausyrityksessä keskustelun kautta. Käytössä ei ollut viitekehyksiä tai työkaluja. Erilaisiin kvantitatiivisiin menetelmiin tietoturvainvestoinnin kannattavuuden arvioimiseksi (ROI, ROSI, UM ym.,) suhtauduttiin lähtökohtaisesti positiivisesti ja menetelmiä voitaisiin yrityksessä hyödyntääkin tarvittaessa.

Tietoturvainvestointien ei koettu tuovan suoraa kilpailuetua. Investointityyppien välillä oli eroa, kuinka merkitykselliseksi ne koettiin; osa tietoturvainvestoinneista koettiin vain isojen organisaatioiden asioiksi. Hyvin monet tietoturvainvestoinnit koettiin tarpeelliseksi vasta myöhemmässä vaiheessa, kun yritys on kasvanut jo huomattavasti suurempaan kokoluokkaan (mm. laiteinvestoinnit, yrityksen sisäinen tietoturva-asiantuntija).

COO ei ollut halukas investoimaan rahaa henkilöstön tietoturvakoulutukseen, CTO näki sen potentiaalisesti mahdollisena: ei vielä yrityksen nykytilanteessa, mutta sitten kun työntekijöitä olisi enemmän. Tietoturvaskannerit ym. ratkaisut, joille ei ollut pakottavaa tarvetta olivat mahdollisia investointeja joskus tulevaisuudessa, kun yritys on kasvanut suuremmaksi, mutta ei vielä.

CTO piti merkittävimpinä uhkina tietoturvallisuuden kannalta henkilöstön tekemiä virheitä ym. organisaation sisältä tulevia asioita. COO:n mielestä merkittävin uhkakuva oli sosiaalinen manipulointi (social engineering). Tietoturva ja järjestelmän stabiilius koettiin merkittävänä tulevaisuuden riskinä, mutta ei vielä yrityksen nykyisessä kasvuvaiheessa.

Seuraavassa luvussa käsitellään näitä tapaustutkimuksen havaintoja ja pohditaan tulosten merkitystä.

6 POHDINTA

Tutkielman tavoitteena oli selvittää yrityksen tietoturvainvestointien ja organisaation kasvun välistä dynamiikkaa: miten yrityksen johdon näkemys tietoturvainvestointien tarpeesta muuttuu yrityksen kasvaessa ja miten investointitarpeita arvioidaan suhteessa kasvuodotuksiin (pienissä kasvuyrityksissä). Tulosten perusteella voidaan sanoa, että yrityksen tietoturvainvestointitarpeiden ja odotetun kasvun välillä on selkeästi havaittava yhteys. Selkeimmin asia ilmeni tietoturvainvestoinnin koetun tarpeellisuuden suhteen: koettiinko investointi kriittiseksi (tai pakolliseksi) vai vähemmän tärkeäksi (tai vapaaehtoiseksi). Myös ohjaavien- ja ennaltaehkäisevien käytänteiden sekä henkilöstön tietoturvakoulutuksen koetun tarpeellisuuden yhteys yrityksen kasvuun oli selkeästi havaittavissa.

Resurssien rajallisuus ja laajat tehtävänkuvat näkyivät tapausyrityksessä. Myös tietoturvan parantamiseen suunnattuja kehittämistoimia piti hoitaa tee-se-itse-toteutuksella. Roolijako vastasi yrityksessä hyvin kasvuteorioiden kuvausta (Lewis & Churchill, 1983; Picken, 2017). Yrityksen ollessa vielä pieni, niin asioita pystyi CTO:n mukaan vielä "ripotella tässä vaiheessa"; kaikki osallistuivat vähän kaikkeen. Liika erikoistuminen yrityksen sisällä ei vielä nykyisessä kasvuvaiheessa ollut mahdollista.

Rooli-identiteettien vaikutus päätöksentekoon (Mathias & Williams, 2017) oli tapausyrityksessä huomattava: tietoturvainvestointien tarpeellisuuden perustelu ei ollut tapausyrityksessä tietoturva-asiantuntijan ongelma, sillä tietoturvainvestoinneista päättävät istuivat itse yrityksen hallituksessa ja vastasivat yrityksen tietoturvakontrollien ja -käytänteiden toteuttamisesta.

Henkilöstön tietoturvakoulutus ja systemaattinen lähestymistapa tietoturva-asioihin koettiin tarpeelliseksi vasta tulevaisuudessa. Tässä asiassa oli tosin näkemyseroja ajankohdan ja toteutustavan suhteen yrityksen COO:n ja CTO:n välillä. Yrityksen pieni koko nähtiin jossain määrin suojaavana tekijänä, kuten mm. (Ng & Feng, 2006) tutkimuksessa. Tietoturvariskejä ei koettu tapausyrityksessä vielä niin merkittäväksi asiaksi, että suojautuminen olisi vaatinut systemaattisia menetelmätapoja ja henkilöstön tietoturvakoulutusta.

COO:n asennemuutos tärkeimmistä tietoturvakontrolleista kysyttäessä (estämiskyky vrt. palautumiskyky), oli hyvä esimerkki oppimisen ja uuden tiedon vaikutuksesta toimintatapoihin: yrityksen suunta muuttuu tarvittaessa hyvin ketterästi ja nopeasti, kuten kävi osin jo haastattelujen aikana. Päätöksentekijät ovat vahvasti sidoksissa ympäristöönsä, ja saavat sieltä vaikutteita (Heidt ym., 2019). Sama ilmiö näkyi myös CTO:n haastattelussa. CTO reagoi toisessa haastattelussa kirjallisesti dokumentoitujen tietoturvakäytänteiden puutteeseen, ja piti tarpeellisena lisätä asia työlistalle. Muutkin selitykset ovat mahdollisia, mutta näissä tapauksissa haastattelun rooli oli ilmeinen. Tieto ei todennäköisesti ollut missään nimessä kokonaan uutta, mutta se toimi herätteenä, jolloin asiaan saatettiin reagoida.

Tapausyrityksen suhtautuminen tarvittaviin tietoturvainvestointeihin oli monelta osin hyvin reaktiivinen: vaadittiin ulkoinen ärsyke (esim. asiakkaan tai lainsäädännön vaatimus), jotta ryhdyttiin toimenpiteisiin. Mutta näin ei ollut kaikissa tapauksissa. Yrityksen sisäisten tietoturvainvestointipäätösten taustatekijöistä nousi esiin haastateltavien aikaisemmista työpaikoista ja internetin tietoturvakoulutuksista kertynyt oppi (mm. salasananhallintajärjestelmä; COO oli todennut työkalun hyödylliseksi aiemmassa työpaikassaan).

Monien tietoturvainvestointityyppien kohdalla suurin rajoite oli motivaatio: tietoturvavakuutukset, tietoturvasertifioinnit, maksulliset tietoturvakoulutukset ym. eivät olleet haastateltavien mukaan nykyisessä kasvuvaiheessa tarpeellisia. Osan investoinneista kohdalla resurssirajoitteina esiintyivät aika (mm. yrityksen palautumiskyvyn parantaminen, havaitsemiskyky), osassa raha (yrityslaitteet henkilöstölle, tietoturvaan erikoistuneet henkilöresurssit). Monet teknologiaan kohdistuvista investoinneista haluttiin toteuttaa mieluiten avoimen lähdekoodin ratkaisuja hyödyntämällä, jolloin keskeisin resurssirajoite oli aika. Suorat rahalliset investoinnit taas esimerkiksi yrityskannettaviin eivät olleet vielä nykyisessä kasvuvaiheessa mahdollisia, sillä moni muu asia meni edelle. Tapaustutkimuksen tulokset vastaavat Moore ym., (2005) tutkimuksen tuloksia. Moore ym., (2005) tutkimuksessa yritysten tietoturvainvestointien pääpaino oli aukkojen täyttämisessä organisaation nykytilan ja tavoitellun aseman välillä (tietoturvan kannalta). Tapausyrityksessä kriittiset tietoturva-aukot oltiin valmiita paikkaamaan heti, mutta vähemmän kriittiset investoinnit saivat odottaa. Tietoturvainvestointipäätöksiä tehtäessä asioita katsottiin kokonaisuutena prosessien kannalta, yksittäisten investointipäätösten kustannusten ja hyödyn mittaamisen sijaan. Investointipäätöksiä ei tehty kvantitatiivisin menetelmin laskemalla esimerkiksi tuottoa investoinnille (ROI), mutta COO näki sen mahdollisesti tulevaisuudessa hyödyllisenä. Nämä havainnot tukevat Moore ym., (2005), Weishäupl ym., (2018) ja Heidt ym., (2019) tutkimusten tuloksia. Kvantitatiiviset menetelmät tietoturvainvestointipäätösten tukena koettiin turhan raskaana prosessina, jonka tuoma lisäarvo yrityksen nykyisessä kasvuvaiheessa nähtiin korkeintaan marginaalisena, ja siten turhana.

Tapausyritys budjetoi IT-kuluja, kuten palvelinkuluja, mutta tietoturvaa ei ollut eritelty ja sitä ei nähty lähitulevaisuudessa tarpeelliseksi. Havainto on linjassa Heidt ym., (2019) tulosten kanssa, tosin Heidt ym., (2019) tutkimuksessa moni pk-yritys ei lainkaan budjetoinut IT-kuluja. Tapausyrityksen päätöksentekoprosessi tietoturvainvestoinneissa, joka oli useimmissa tapauksissa hyvin helppo ja nopea vrt. perinpohjainen analyysi, vastasi yhtä lailla Heidt ym., (2019) tuloksia.

Tapaustutkimuksen tulokset vahvistavat Cavusoglu ym., (2015), Heidt ym., (2019) ja Weishäupl ym., (2018) tunnistaman normatiivisen paineen (esim. paine liikekumppaneilta) ja pakottavan tarpeen (lainsäädännön asettamat vaatimukset) merkittävän roolin investointipäätöksen ajurina. Weishäupl ym., (2018) tulosten mukaisesti valtion asettama sääntely myös määritti

investointikohteen ja investoinnin rajat – COO:n sanoin: ”tietoturvaan pistetään just se vaadittu”. Asiantuntijoiden suosittelu (Chao ym., 2019) ja laumateoria ei saanut vahvaa tukea, mutta toisaalta tapausyrityksessä tietoturvainvestointipäätösten tekijät eivät olleet tietoturva-asiantuntijoita. Parhaiten käytänteiden seuraaminen mainittiin tapausyrityksessä, mutta asiantuntijoiden suosittelulle tai muiden organisaatioiden käytännöille ei annettu suurta painoarvoa. Joitain käytänteitä oli kuitenkin omaksuttu haastateltavien aikaisemmista työpaikoista yrityksen käyttöön.

Tapausyrityksen tietoturvainvestointistrategia noudattaa jossain määrin (Carias ym., 2019) suosittamaa strategiaa (kyberresilienssi), vaikka konteksti on eri. Carias ym., (2019) mukaan yrityksen on alussa järkevää painottaa investointeja teknisiin kontrolleihin, mutta teknisten kontrollien saavuttaessa riittävän tason, siirtää painopistettä yhä enemmän ihmisiin ja prosesseihin. Henkilöstön tietoturvakoulutuksen merkitystä ei pidä aliarvioida ja toisaalta teknisten kontrollien tuomaa suojaa ei pidä yliarvioida. Paras investointistrategia ei silti ole investoida yhtä paljon kaikkiin kontrolleihin (Nazareth & Choi, 2015). Low (2017) mukaan pk-yrityksiin kohdistuu erityisesti sähköpostihuijauksia ja kiristyshaittaohjelmia. Henkilöstön tietoturvakoulutus on välttämätöntä uhkiin varautumisessa. Beharan ym., (2007) mukaan organisaation on tehokkaampaa investoida tasaisesti useaan erilaiseen tietoturvakontrolliin. Pienillä kasvuyrityksillä on mahdollisuus valita oma tietoturvainvestointistrategiansa, mutta tärkeintä olisi, että investoinnit tietoturvaan eivät jää kasvun jalkoihin, vaan pysyvät tasaisesti mukana. Tapausyrityksellä oli siinä mielessä erittäin tervetullut suhtautuminen tietoturvaan, että asiaan suhtauduttiin vakavasti. Vaikka rahallisia investointeja ei pidetty erityisen tarpeellisina ainakaan toistaiseksi, yritys kuitenkin käytti aikaa tietoturvan pohtimiseen ja suunnittelemiseen. Tekniset kontrollit olivat yrityksen kokoon nähden hyvällä tasolla, mutta ihmisten kouluttaminen ja yhteisten tietoturvakäytänteiden suunnitteleminen oli jäänyt vähemmälle huomiolle.

Tulokset vastasivat kokonaisuudessaan pitkälti ennakko-oletuksia, jota vasten tutkimuksen tuloksia on analysoitu (s. 53). Tietoturva-asioita oli tapausyrityksessä mietitty jopa hieman enemmän kuin oli alkuperäinen olettamus. Investoinnit tietoturvaan jäivät kuitenkin useissa tapauksissa muiden investointien taakse, kuten ennakko-oletus oli.

6.1 Tulosten merkitys

Kasvuyrityskontekstissa korostuvat tuntemattomat riskit (Sommer ym., 2009). Riskiympäristö muuttuu jatkuvasti, ja yritys kohtaa kasvaessaan oletettavasti paljonkin riskejä, joita on vielä nykyhetkessä mahdotonta ajatella. Tämä näkyy myös suhtautumisessa ja varautumisessa riskeihin. Aloittava startup-yritys ei voi mitenkään välttyä moniltakaan riskeiltä, mutta voimakas kasvuhakuisuus lisää riskejä myös tietoturvan osalta, jos perusta ei ole kunnossa.

Tietoturvariskeihin liittyviä negatiivisia seurauksia ja tarvittavia suojakeinoja ei ole aina helppo ymmärtää. Johdolla ei ole välttämättä kunnollista käsitystä potentiaalisten vahinkojen suuruusluokasta, jos riski realisoituu (Cavusoglu, 2010). Tapausyrityksen johto suhtautui tietoturva-asioihin vakavasti, mikä on erittäin tärkeää tietoturvakulttuurin kehittymisen, seurannan ja valvonnan kannalta (Hu ym., 2012). Aloittavia yrityksiä tulisi neuvoa kiinnittämään huomiota tietoturvainvestointeihin alusta alkaen. Pieniä kasvuyrityksiä tulisi kouluttaa, että turvalliset toimintatavat voidaan rakentaa osaksi yrityksen kulttuuria liiketoimintatavoitteiden kärsimättä.

Kasvuyrityskulttuurilla on vaikutusta riskienhallinnan toimintatapoihin. Tapausyrityksessä karsastettiin hierarkkista organisaatiorakennetta ja luottamuksen merkitys korostui. Organisaatiokulttuuria voi kuvata hyvin egalitaristiseksi (Karyda ym., 2006). Startup-yrityksillä ja muilla pienillä kasvuyrityksillä on ainutlaatuinen mahdollisuus lähteä rakentamaan oikeanlaista tietoturvakulttuuria alusta alkaen yrityksen toimintaan. Pienillä kasvuyrityksillä on mahdollisuus integroida turvalliset toimintatavat syvästi yhteen yrityksen strategian ja tavoitteiden kanssa. Tämä tarkoittaa sitä, että yrityksen alussa tekemillä pienillä investoinneilla, useissa tapauksissa lähinnä ajan muodossa, voi olla myöhemmin valtava merkitys yrityksen kasvaessa. Useimmat startup-yrityksistä ovat alussa hyvin pieniä, joten on tyypillistä, että kaikki tuntevat toisensa ja ovat toistensa kanssa tekemisissä. Mitä aikaisemmin ihmiset otetaan mukaan projektiin, sitä helpompaa on saavuttaa heidän tukensa (Zinatullin, 2016). Käyttäjät voivat olla arvokas resurssi riskienhallinnan käytänteiden määrittelyssä (Karyda ym., 2006): yrityksen kasvaessa työntekijät voivat neuvoa uusia työntekijöitä alusta alkaen yrityksen turvallisuuskäytänteisiin, koska he ovat itse sitoutuneet noudattamaan niitä.

Sisäinen läpinäkyvyys (Street & Meister, 2004) on pienissä organisaatioissa usein hyvällä tasolla. Tietoturvakontrolleja implementoitaessa on vielä helppo keskustella yhdessä asianomaisten kanssa, miten esitetty ratkaisu vaikuttaa kunkin työtehtäviin, ja mitä ongelmia siinä mahdollisesti on. Näin tietoturva on mahdollista integroida yrityksen liiketoimintaan tehokkaasti ja suhteellisen vaivattomasti.

Toinen vaihtoehto on, että tämä ainutlaatuinen mahdollisuus laiminlyödään joko tietoisesti tai tiedostamattomasti. Yrityksen kasvaessa tietoturva tuodaan myöhemmin pakotetusti mukaan, ja ihmisten tukea ei ole enää yhtä helppo saada kuin alussa. Turvalliset käytänteet voidaan hyvinkin kokea työtä rajoittavaksi tekijäksi, joten negatiinen suhtautuminen voi olla hyvinkin mahdollista (Weishäupl ym., 2018). Ongelmat kasautuvat ja alkuvaiheen pienet tekemättä jätetyt investoinnit näkyvät kasvavina riskeinä ja tietoturvaongelmina.

Ihminen on tunnetusti useimmissa tapauksissa ketjun heikoin lenkki tietoturvan kannalta (Carias ym., 2019). Tapausyritys osoittaa, että tietoturvan tasoa voidaan parantaa organisaatiossa suhteellisen pienin investoinnein, usein jopa ilman rahallista investointia. Internetissä on tarjolla paljon avoimeen lähdekoodiin perustuvia tietoturvaratkaisuja ja koulutuksia. Tärkeintä on

yrityksen sisäinen tahtotila hyödyntää näitä mahdollisuuksia. Investointia tietoturvaan ei pidä ajatella vain uhkien, vaan myös mahdollisuuksien kannalta. Yrityksen ollessa pieni myös kirjallisesta dokumentaatiosta (kuten tietoturvapolitiikka) ei oletettavasti tulisi kovin pitkää ja raskasta tekstiä, vaan se olisi mahdollista mukauttaa kevyeen muotoon yrityksen tarpeita vastaavaksi.

Jotta yritys voi integroida tietoturvalliset toimintatavat pienin investoinnein toimintaansa, edellyttää se toki, että aloittavassa yrityksessä on päättävässä asemassa henkilö, joka nostaa asian esille. Tapausyrityksen etuna on osaaminen tietoturva-asioiden saralla. Yrityksessä on ymmärrystä tietoturvasta ja kykyä toteuttaa tarvittavia kontrolleja (myös teknisiä) omin voimin. Näin ei välttämättä ole asia monen muun vastaavassa kasvuvaiheessa olevan yrityksen kohdalla, jolloin tarvittavat investoinnit oletettavasti edellyttävät apua yrityksen ulkopuolelta (ja siten myös rahallisia investointeja).

6.2 Tutkielman rajoitteet ja jatkotutkimusaiheita

Tutkielman rajoitukset on toki otettava huomioon tuloksia arvioitaessa. Tutkielman empiirisessä osiossa tutkittiin vain yhtä aloittavaa startup-yritystä, joten tuloksia ei voida yleistää. Toisessa pienessä kasvuyrityksessä asiat on voitu hoitaa hyvin eri tavalla ja erilaiset resurssirajoitteet (kuten osaaminen) korostua. Lisäksi on huomioitava, että tässä tutkielmassa keskityttiin johdon näkemyksiin investointitarpeen kehittymisestä. Ei ole lainkaan varmaa, että johdon olettamukset pitävät pitkällä aikavälillä paikkaansa. Jatkotutkimuksen kannalta pitkittäistutkimus olisi siis kiinnostava osa-alue tietoturvainvestointien ja yrityksen kasvun välistä yhteyttä tutkittaessa: pätevätkö tapausyrityksen johdon oletukset investointitarpeesta, ja miten tapausyrityksen tietoturvainvestointitarve muuttuu yrityksen kasvaessa? Jäävätkö tarvittavat tietoturvainvestoinnit nopean kasvun jalkoihin vai onko tietoturva mahdollista integroida yrityksen toimintaan syvällä tasolla niin kuin tässä pohdinnassa oletetaan?

Toinen mahdollinen jatkotutkimusaihe on yrityksen riskinsietokyvyn (siedettävän riskitason) suhde yrityksen kasvuun: tapaustutkimuksen tulokset antavat aihetta olettaa, että aloittavien yritysten riskinsietokyky (ml. tietoturvariskit) on alussa korkealla, mutta lähtee yrityksen kasvun myötä laskuun. Yrityksen kasvaessa tärkeää on säilyttää siedettävän riskitason tasapaino. Riskitaso voi ajan myötä kasvaa yli siedettävän tason, jos yritys ei investoi tietoturva-asioihin. Jatkotutkimuksissa voitaisiin myös selvittää tarkemmin resurssien rajallisuuden yhteyttä yrityksen siedettävään riskitasoon. Myös yrityksen päätöksentekologiikan (kuvio 3) vaikutusta yrityksen tietoturvainvestointistrategiaan olisi kiinnostavaa selvittää.

7 YHTEENVETO

Tapaustutkimusten haasteena pidetään yleistettävyyden haastetta. Erikssonin ja Koistisen (2014) mukaan yleistämisen ongelma liittyy nimenomaisesti tilastolliseen yleistämiseen, sillä tapaustutkimus keskittyy yleensä yhden tai muutaman tapauksen tutkimiseen, jolloin koko populaatiota kuvaavan luotettavan tilastollisen yleistämisen tekeminen on lähes mahdotonta. Tämä tutkielma ei pyri todistamaan, että kaikissa pienissä kasvuyrityksissä suhtauduttaisiin tietoturvainvestointeihin samoin tavoin ja menetelmin. Tutkielmassa sen sijaan esitetään, miten yhdessä pienessä kasvuyrityksessä ilmeni tietoturvainvestointien ja yrityksen kasvun välinen dynamiikka.

Tietoturvainvestoinneista on toistaiseksi tehty melko vähän empiiristä tutkimusta. Tietoturvainvestointeja on tutkittu eri kokoluokan yrityksissä, mutta tutkimukset ovat painottuneet melko suuriin organisaatioihin ja pienet kasvuyritykset ovat jääneet paitsioon. Etenkin kasvun suhdetta tietoturvainvestointeihin on tutkittu hyvin vähän, jos lainkaan. Tämä tutkielma pyrki valaisemaan toistaiseksi vähän tutkittua aihepiiriä. Tutkielman empiirisessä osiossa syvennyttiin yhden pienen kasvuyrityksen tietoturvainvestointeihin ja tulevaisuuden tietoturvainvestointitarpeisiin.

Tutkielman tuloksia ei pidä yrittää yleistää kokonaisuudessaan kaikkiin pieniin kasvuyrityksiin, koska jokaisella organisaatiolla on oma kulttuurinsa ja toimintatapansa. Tutkielman tulokset tuovat kuitenkin valoa toistaiseksi vähän tutkittuun aiheeseen. Tutkielman pyrkimyksenä oli toimia alustavana esitutkimuksena, ja selvittää, onko tutkimusaiheessa potentiaalia jatkotutkimuksille. Tulosten perusteella voidaan sanoa, että on. Tutkimus tuo uutta, käytännönläheistä tietoa tärkeästä aihepiiristä ja vahvistaa viime vuosina julkaistujen empiiristen tutkimusten tuloksia. Asiaa ei ole vielä vastaavalla tavalla tutkittu erityisen paljon. Kotulicin ja Clarkin (2004) ehdottama lähestymistapa arkaluonteisen aihepiirin tutkimiseen toimi hyvin. Staken (1995) näkemyksen mukaisesti, holistinen ymmärrys tutkittavasta tapauksesta on jo rikas tavoite sinänsä.

LÄHTEET

Adams, J. (2007). Risk Management: It's Not Rocket Science..... It's Much More Complicated. Risk Management, 54(5), 36.

Anderson, R. & Moore, T. (2006). The economics of information security. Science, 314(5799), 610-613.

Andrijcic, E., & Horowitz, B. (2006). A macro-economic framework for evaluation of cyber security risks related to protection of intellectual property. Risk analysis, 26(4), 907-923.

Anyadike-Danes, M., Bonner, K., Hart, M. & Mason, C. (2009). Measuring business growth: High-growth firms and their contribution to employment in the UK.

Arora, A., Hall, D., Piato, C. A., Ramsey, D., & Telang, R. (2004). Measuring the risk-based value of IT security solutions. IT professional, 6(6), 35-42.

Bardhan, I., Sougstad, R., & Sougstad, R. (2004). Prioritizing a portfolio of information technology investment projects. Journal of Management Information Systems, 21(2), 33-60.

Barney, J. B. (2001). Resource-based theories of competitive advantage: A ten-year retrospective on the resource-based view. Journal of management, 27(6), 643-650.

Barringer, B. R., Jones, F. F. & Neubaum, D. O. (2005). A quantitative content analysis of the characteristics of rapid-growth firms and their founders. *Journal of Business Venturing, 20*(5), 663-687.

Beebe, N. L., Young, D. K., & Chang, F. R. (2014). Framing information security budget requests to influence investment decisions. Communications of the Association for Information Systems, 35(1), 7.

Behara, R., Huang, C. D., & Hu, Q. (2007). A system dynamics model of information security investments.

Bistarelli, S., Dall'Aglio, M., & Peretti, P. (2006). Strategic games on defense trees. In International Workshop on Formal Aspects in Security and Trust (pp. 1-15). Springer, Berlin, Heidelberg.

Bodin, L. D., Gordon, L. A., & Loeb, M. P. (2005). Evaluating information security investments using the analytic hierarchy process. Communications of the ACM, 48(2), 78-83.

Bojanc, Rok & Jerman-Blažič, Borka. (2008). An economic modelling approach to information security risk management. International Journal of Information Management. 28(5), 413–422.

Bradbard, D. A., Norris, D. R. & Kahai, P. H. (1990). Computer security in small business: An empirical study. *Journal of Small Business Management, 28*(1), 9.

Brink, D. (2001). A guide to determining return on investment for e-security. RSA Security Inc.

Carías, J. F., Labaka, L., Sarriegi, J. M., & Hernantes, J. (2019). Defining a cyber resilience investment strategy in an industrial internet of things context. Sensors, 19(1), 138.

Chai, S., Kim, M., & Rao, H. R. (2011). Firms' information security investment decisions: Stock market evidence of investors' behavior. Decision Support Systems, 50(4), 651-661.

Chan, M., Woon, I. & Kankanhalli, A. (2005). Perceptions of information security in the workplace: Linking information security climate to compliant behavior. Journal of Information Privacy and Security, 1(3), 18-41.

Campbell, K., Gordon, L. A., Loeb, M. P. & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security, 11*(3), 431-448.

Cavusoglu, H., Mishra, B. & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce, 9*(1), 70-104.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). A model for evaluating IT security investments. Communications of the ACM, 47(7), 87-92.

Cavusoglu, H., Raghunathan, S., & Yue, W. T. (2008). Decision-theoretic and game-theoretic approaches to IT security investment. Journal of Management Information Systems, 25(2), 281-304.

Cavusoglu, H. (2010). Making sound security investment decisions. *Journal of information privacy and security*, *6*(1), 53-71.

Cavusoglu, H., Cavusoglu, H., Son, J. Y., & Benbasat, I. (2015). Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. Information & Management, 52(4), 385-400.

Delmar, F., & Wiklund, J. (2008). The effect of small business managers' growth motivation on firm growth: A longitudinal study. *Entrepreneurship theory and practice*, *32*(3), 437-457.

DiCicco-Bloom, B., & Crabtree, B. F. (2006). The qualitative research interview. Medical education, 40(4), 314-321.

Dor, D., & Elovici, Y. (2016). A model of the information security investment decision-making process. Computers & security, 63, 1-13.

Drucker, P. F. (2020). The essential drucker. Routledge.

Eisenhardt, K. M. (1989). Building theories from case study research. Academy of management review, 14(4), 532-550.

Eisenhardt, K. M., & Martin, J. A. (2000). Dynamic capabilities: what are they? *Strategic management journal*, *21*(10-11), 1105-1121.

Eriksson, P., & Koistinen, K. (2014). Monenlainen tapaustutkimus. Kuluttajatutkimuskeskus.

Eskola, J., Suoranta, J. (1998). Johdatus laadulliseen tutkimukseen. 2. painos. Vastapaino. Tampere.

Farouk, A., & Saleh, M. (2011). An explanatory framework for the growth of small and medium enterprises. In International Conference of System Dynamics Society (pp. 1-29).

Fenz, S., Ekelhart, A., & Neubauer, T. (2011). Information security risk management: In which security solutions is it worth investing?. Communications of the Association for Information Systems, 28(1), 22.

Gabrielsson, P., & Gabrielsson, M. (2013). A dynamic model of growth phases and survival in international business-to-business new ventures: The moderating effect of decision-making logic. *Industrial Marketing Management*, *42*(8), 1357-1373.

Gage, D. (2012). The venture capital secret: 3 out of 4 start-ups fail. Wall Street Journal, 20.

Gal-Or, E., & Ghose, A. (2005). The economic incentives for sharing security information. Information Systems Research, 16(2), 186-208.

Gibb, A., & Davies, L. (1990). In pursuit of frameworks for the development of growth models of the small business. International Small Business Journal, 9(1), 15-31.

Gillham, B. (2010). Case Study Research Methods. London, GBR : Continuum International Publishing.

Marsh & Microsoft. (04.11.2020). 2019 Global Cyber Risk Perception Survey. Haettu osoitteesta: https://www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf

Gordon, L. A. & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC), 5*(4), 438-457.

Gordon, L. A., & Loeb, M. P. (2002b). Return on information security investments: Myths vs. realities. *Strategic finance*, *84*(5), 26.

Greiner, L. E. (1989). Evolution and revolution as organizations grow. *Readings in strategic management* (pp. 373-387). Palgrave, London.

Hambrick, D. C., & Crozier, L. M. (1985). Stumblers and stars in the management of rapid growth. Journal of business venturing, 1(1), 31-45.

Hamill, J. T., Deckro, R. F., & Kloeber Jr, J. M. (2005). Evaluating information assurance strategies. Decision Support Systems, 39(3), 463-484.

Hanks, S. H., Watson, C. J., Jansen, E., & Chandler, G. N. (1994). Tightening the life-cycle construct: A taxonomic study of growth stage configurations in high-technology organizations. Entrepreneurship theory and Practice, 18(2), 5-29.

Hausken, K. (2006). Returns to information security investment: The effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability. Information Systems Frontiers, 8(5), 338-349.

Heidt, M., Gerlach, J., & Buxmann, P. (2019). A Holistic View on Organizational IT Security: The Influence of Contextual Aspects During IT Security Decisions. In Proceedings of the 52nd Hawaii International Conference on System Sciences.

Herath, H. S., & Herath, T. C. (2008). Investments in information security: A real options perspective with Bayesian postaudit. Journal of Management Information Systems, 25(3), 337-375.

Herath, T. & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems, 47(2), 154-165.

Hirsjärvi, S. & Hurme, H. (1988). Teemahaastattelu Yliopistopaino.

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2009) Tutki ja kirjoita. (15. uud. painos) Helsinki: Tammi.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*(4), 615-660.

Huang, C. D., Hu, Q., & Behara, R. S. (2006). Economics of Information Security Investment in the Case of Simultaneous Attacks. In WEIS.

Huang, C. D., Hu, Q., & Behara, R. S. (2008). An economic analysis of the optimal information security investment in the case of a risk-averse firm. International journal of production economics, 114(2), 793-804.

Huang, C. D., & Behara, R. S. (2013). Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints. International Journal of Production Economics, 141(1), 255-268.

Huovinen, P. (2018). Voimakkaasti kasvuhakuiset pk-yritykset. Helsinki: Työ- ja elinkeinoministeriö. Haettu osoitteesta http://urn.fi/URN:ISBN:978-952-327-296-5

Ioannidis, C., Pym, D., & Williams, J. (2009). Investments and trade-offs in the economics of information security. In International Conference on Financial Cryptography and Data Security (pp. 148-166). Springer, Berlin, Heidelberg.

Ioannidis, C., Pym, D., & Williams, J. (2012). Fixed costs, investment rigidities, and risk aversion in information security: A utility-theoretic approach. In Economics of Information Security and Privacy III (pp. 171-191). Springer, New York, NY.

ISO/IEC. (2005). ISO/IEC 27002: 2005 information technology-security techniques–code of practice for information security management.

Kahneman, D., & Tversky, A. (1979). Prospect Theory: An Analysis of Decision under Risk. Econometrica, 47(2), 263-292.

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2006). Formulating information systems risk management strategies through cultural theory. Information Management & Computer Security.

Knapp, K. J., Marshall, T. E., Kelly Rainer, R. & Nelson Ford, F. (2006). Information security: Management's effect on culture and policy. Information Management & Computer Security, 14(1), 24-36.

Kollmann, T., Stöckmann, C., Hensellek, S., & Kensbock, J. (2016). European startup monitor 2016. Universität Duisburg-Essen Lehrstuhl für E-Business.

Kort, P. M., Haunschmied, J. L., & Feichtinger, G. (1999). Optimal firm investment in security. Annals of Operations Research, 88, 81-98.

Koskinen, I., Alasuutari, P., Peltonen, T. (2005). Laadulliset menetelmät kauppatieteissä. Tampere. Vastapaino.

Kotiranta, A., Pajarinen, M., & Rouvinen, P. (2016). Miltä startupit näyttävät tilastojen valossa? (No. 66). ETLA Report.

Kotulic, A. G. & Clark, J. G. (2004). Why there aren't more information security research studies. *Information & Management, 41*(5), 597-607.

Kapur, M., Tuteja, A., Bahl, M., Gupta, A. & Shetty, S.A. (2017). KPMG Cyber Crime Survey Report, Insights and perspectives

Kupi, E., Keränen, J., & Lanne, M. (2009). Riskienhallinta osana pk-yritysten strategista johtamista.

Larja, L., & Räisänen, H. (2019). Yritysten digitalisaatio ja kasvu: Pk-yritysbarometrin näkökulmia.

Lester, D. L., Parnell, J. A., & Carraher, S. (2003). Organizational life cycle: A five-stage empirical scale. *The international journal of organizational analysis*.

Levie, J., & Lichtenstein, B. B. (2010). A terminal assessment of stages theory: Introducing a dynamic states approach to entrepreneurship. Entrepreneurship Theory and practice, 34(2), 317-350.

Lewis, V.L., & Churchill, N.C. (1983). The five stages of small business growth. *Harvard Business Review, 61(*3), 30-50.

Littunen, H., & Tohmo, T. (2003). The high growth in new metal-based manufacturing and business service firms in Finland. *Small business economics*, *21*(2), 187-200.

Liu, D., Ji, Y., & Mookerjee, V. (2011). Knowledge sharing and investment decisions in information security. Decision Support Systems, 52(1), 95-107.

Loch, K. D., Carr, H. H. & Warkentin, M. E. (1992). Threats to information systems: Today's reality, yesterday's understanding. *Mis Quarterly,* , 173-186.

Low, P. (2017). Insuring against cyber-attacks. Computer Fraud & Security, 2017(4), 18-20.

Luger, M. I., & Koo, J. (2005). Defining and tracking business start-ups. Small Business Economics, 24(1), 17-28.

Mahmood, M. A., & Mann, G. J. (1993). Measuring the organizational impact of information technology investment: an exploratory study. Journal of management information systems, 10(1), 97-122.

Mars, G. (1996). Human factor failure and the comparative structure of jobs. Journal of Managerial Psychology.

Mathias, B. D., & Williams, D. W. (2017). The impact of role identities on entrepreneurs' evaluation and selection of opportunities. Journal of Management, 43(3), 892-918.

Matsuura, K. (2003). Information security and economics in computer networks: An interdisciplinary survey and a proposal of integrated optimization of investment. In Computing in Economics and Finance (Vol. 48, pp. 1-13).

McKenna, F. P. (1993). It won't happen to me: Unrealistic optimism or illusion of control?. British Journal of Psychology, 84(1), 39-50.

McMahon, R. G. (1998). Stage models of SME growth reconsidered. *Small Enterprise Research*, *6*(2), 20-35.

Mizzi, A. (2010). Return on information security investment-the viability of an anti-spam solution in a wireless environment. IJ Network Security, 10(1), 18-24.

Moore, T., Dynes, S. & Chang, F. R. (2015). Identifying how firms manage Cybersecurity investment. Dallas: Southern Methodist University.

Nazareth, D. L., & Choi, J. (2015). A system dynamics model for information security management. Information & Management, 52(1), 123-134.

Ng, B. Y. & Feng, A. E. (2006). An exploratory study on managerial security concerns in technology start-ups. *PACIS 2006 Proceedings,* 29.

O'Farrell, P. N., & Hitchens, D. M. (1988). Alternative theories of small-firm growth: a critical review. *Environment and Planning A*, *20*(10), 1365-1383.

Parker, S. C., Storey, D. J. & Van Witteloostuijn, A. (2010). What happens to gazelles? the importance of dynamic management strategy. *Small Business Economics, 35*(2), 203-226.

Penrose, E. (1959). The Theory of the Growth of the Firm. Blackwell Scientific Publications. Oxford.

Pettigrew, A. M. (2014). The politics of organizational decision-making. Routledge.

Picken, J. C. (2017). From startup to scalable enterprise: Laying the foundation. Business Horizons, 60(5), 587-595.

Purser, S. A. (2004). Improving the ROI of the security management process. Computers & Security, 23(7), 542-546.

Raggad, B. G. (2010). Information security management: concepts and practice. CRC Press.

Rhee, H., Ryu, Y. U. & Kim, C. (2012). Unrealistic optimism on information security management. Computers & Security, 31(2), 221-232.

Rikama, S. (2016). Voimakkaasti kasvuhakuiset pk-yritykset. Helsinki: Työ- ja elinkeinoministeriö. Haettu osoitteesta: http://urn.fi/URN:ISBN:978-952-327-212-5

Rowley, J. (2002). Using case studies in research. *Management research news*.

Rue, R., Pfleeger, S. L., & Ortiz, D. (2007). A Framework for Classifying and Comparing Models of Cyber Security Investment to Support Policy and Decision-Making. In WEIS.

Ryan, J. J., & Ryan, D. J. (2006). Expected benefits of information security investments. Computers & Security, 25(8), 579-588.

Schatz, D., & Bashroush, R. (2017). Economic valuation for information security investment: a systematic literature review. Information Systems Frontiers, 19(5), 1205-1228.

Scott, M., & Bruce, R. (1987). Five stages of growth in small business. Long range planning, 20(3), 45-52.

Shao, X. (2015). Understanding information systems (IS) security investment in organizations. Tampere: Juvenes print.

Shao, X., Siponen, M. & Pahnila, S. (2019). To calculate or to follow others: How do information security managers make investment decisions? University of Hawai'i at Manoa.

Simon, H. A. (1955). A behavioral model of rational choice. *The quarterly journal of economics*, *69*(1), 99-118.

Smallbone, D., Leig, R., & North, D. (1995). The characteristics and strategies of high growth SMEs. International Journal of Entrepreneurial Behavior & Research.

Sonnenreich, W., Albanese, J., & Stout, B. (2006). Return on security investment (ROSI)-a practical quantitative model. Journal of Research and practice in Information Technology, 38(1), 45.

Standards Australia & Standards New Zealand. (2004). AS/NZS 4360: 2004: risk management.

Straub, D. W. & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly,* 441-469.

Street, C. T., & Meister, D. B. (2004). Small business growth and internal transparency: The role of information systems. *MIS quarterly*, 473-506.

Sommer, S. C., Loch, C. H., & Dong, J. (2009). Managing complexity and unforeseeable uncertainty in startup companies: An empirical study. Organization Science, 20(1), 118-133.

Soo Hoo, K. J. (2000). How much is enough: a risk management approach to computer security.

Stake, R. E. (1995). The Art of Case Study Research. Sage.

Storey, D. J. (2016). Understanding the small business sector. Routledge.

Suhonen, T. (2019). ISO/IEC 27001-sertifioinnin hankintaperusteet ja sertifiointielimen valintaperusteet. (pro gradu -tutkielma, Jyväskylän yliopisto).

Syrjälä, L., Ahonen, S., Syrjäläinen, E., Saari, S. (1994). Laadullisen tutkimuksen työtapoja. 1.- 2. painos. Helsinki. Kirjayhtymä.

Tanaka, H., Matsuura, K., & Sudoh, O. (2005). Vulnerability and information security investment: An empirical analysis of e-local government in Japan. Journal of Accounting and Public Policy, 24(1), 37-59.

Tatsumi, K. I., & Goto, M. (2010). Optimal timing of information security investment: A real options approach. In Economics of Information Security and Privacy (pp. 211-228). Springer, Boston, MA.

Tsiakis, T., & Stephanides, G. (2005). The economic approach of information security. Computers & security, 24(2), 105-108.

Von Solms, R. (1998). Information security management (3): The code of practice for information security management (BS 7799). Information Management & Computer Security,

Weinstein, N. D., & Klein, W. M. (1996). Unrealistic optimism: Present and future. Journal of Social and Clinical Psychology, 15(1), 1-8.

Weishäupl, E., Yasasin, E., & Schryen, G. (2018). Information security investments: An exploratory multiple case study on decision-making, evaluation and learning. Computers & Security, 77, 807-823.

Westerlind, K. (2004). Evaluating return on information technology investment.

Whitman, M. E. & Mattord, H. J. (2011). Principles of information security Cengage Learning.

Wiklund, J., Davidsson, P., & Delmar, F. (2003). What do they think and feel about growth? An expectancy–value approach to small business managers' attitudes toward growth. Entrepreneurship theory and practice, 27(3), 247-270.

Wiklund, J., Patzelt, H., & Shepherd, D. A. (2009). Building an integrative model of small business growth. Small Business Economics, 32(4), 351-374.

Willemson, J. (2006). On the gordon & loeb model for information security investment.

Yin Robert, K. (1994). Case study research: design and methods. *Sage publications*.

Zinatullin, L. (2016). The Psychology of Information Security: Resolving conflicts between security compliance and human behaviour. IT Governance Ltd.

LIITE 1 HAASTATTELURUNKO

1. haastattelu

1. Organisaatio
    a. Toimiala (yleiskuva, näkymät, kilpailu, uhat ja mahdollisuudet)
    b. Palvelu, tuote, idea, liiketoimintamalli
    c. Ketä haastattelen? Mikä rooli?
    d. Organisaation ikä
    e. Henkilöstön lkm, kasvu, koulutustausta
    f. Organisaatiorakenne (hierarkkinen / matala)
2. Yrityskulttuuri
    a. Hallinto (keskitetty / hajautettu / jaettu)
    b. Päätöksenteko
    c. Viestintätapa (muodollinen / ei muodollinen)
    d. Viestintäkanavat
    e. Luottamus
3. Yrityksen johtamistapa / strateginen suunnittelu
    a. Yrityksen johtamistapa (formaali vai epäformaali toimintamalli)
    b. Strateginen suunnittelu; nimetyt tavoitteet ja visio muutaman vuoden tähtäimellä
    c. Operatiivisen päivittäisjohtamisen toteutus, vallan ja vastuun jakautuminen, käytössä olevat mittarit
    d. Käytössä olevat johtamisen tai toiminnan ohjauksen mallit
    e. Kasvuhakuisuus (historia, tulevaisuuden suunnitelmat)
4. Riskienhallinta
    a. Riskienhallinnan merkitys yrityksen toiminnalle: Missä roolissa kokonaiskuvan kannalta? Miten? Kuka? Miksi? Mihin tarkoitukseen? jne.
    b. Toimintaan liittyvät merkittävimmät riskit
    c. Riskienhallinnan menettelytavat, käytännöt ja prosessit (muodollinen / epämuodollinen), käytetäänkö aikaa tulevaisuuden uhkien ennakointiin vai keskitytäänkö hoitamaan päivittäisiä ongelmia, miten riskienhallinta on integroitu johtamiseen, riski-informaation hyödyntäminen johtamisen tukena, käytetyt työkalut jne.
    d. Muodollisen riskienhallintaprosessin tarve
    e. Riskienhallinnan motivointi (lainsäädäntö, asiakasvaateet, oman toiminnan kehittäminen, sattuneet vahingot, vakuutusyhtiöt ja muut kumppanit)
    f. Tietoturvan suhde riskienhallintaan
    g. Tulevaisuuden riskit, joiden merkitys kasvaa
5. Tietoturva

   a. Suhtautuminen tietoturvaan yleisesti (johto, työntekijät)
   b. Tietoturvapolitiikka / sovitut tietoturvakäytännöt (information security policy)
   c. Tietoturvan nykytila (meneillään olevat kehitysprojektit jne.)
   d. Merkittävimmät uhat
   e. Varautuminen uhkiin
   f. Tietoturvapoikkeamat (onko ollut? Seuraukset?)
   g. Kokemus, tietotaito (johto, työntekijät)
   h. Vastatoimet (proaktiivinen, reaktiivinen, estäminen vs. palautumiskyky, kontrollit preventive vs. detective), tärkeimmät suojattavat kohteet luokiteltu jne.
   i. Miten? (Teknologia / ihmiset / sertifiointi / vakuutukset / koulutus jne.)
   j. Liiketoiminnan tarpeiden ja tietoturvan suhde (alignment to business needs)
   k. Kumppanit, toimittajat, asiakkaat (esitättekö, onko teille esitetty tietoturvavaatimuksia jne.)
6. Päätöksenteko / investointiprosessi
   a. Kuka, ketkä päättää? Miten? (Muodollisuus /epämuodollisuus)
   b. Investointibudjetit – kehittämistoimet, teknologia, tietoturva ym. eritelty?
   c. Suhtautuminen kustannuksiin, investointien priorisointi (kasvu / voitollisuus / riskien välttäminen)
   d. Käytetyt mittarit
   e. Tietoturvainvestoinnit
      i. Tavoitteet
      ii. Tuotto-odotus (Miten mitataan? Mitataanko?)
      iii. Yhteys kasvuun (riskienhallinta edellä vai kasvu edellä, ajatellaanko tietoturvainvestointeja kasvun kannalta)

LIITE 2 HAASTATTELURUNKO

2.haastattelu

1. Organisaatio ja yrityskulttuuri
    a. Ketä haastattelen? Mikä rooli?
    b. Toimiala (uhat ja mahdollisuudet)
    c. Viestintätapa (muodollinen / ei muodollinen)
    d. Luottamuksen merkitys
2. Yrityksen johtamistapa / strateginen suunnittelu
    a. Yrityksen johtamistapa (formaali vai epäformaali toimintamalli)
    b. Strateginen suunnittelu; nimetyt tavoitteet ja visio muutaman vuoden tähtäimellä
    c. Operatiivisen päivittäisjohtamisen toteutus, vallan ja vastuun jakautuminen, käytössä olevat mittarit
    d. Käytössä olevat johtamisen tai toiminnan ohjauksen mallit
    e. Kasvuhakuisuus (historia, tulevaisuuden suunnitelmat)
3. Riskienhallinta
    a. Riskienhallinnan merkitys yrityksen toiminnalle: Missä roolissa kokonaiskuvan kannalta? Miten? Kuka? Miksi? Mihin tarkoitukseen? jne.
    b. Toimintaan liittyvät merkittävimmät riskit
    c. Tulevaisuuden riskit, joiden merkitys kasvaa
    d. Riskienhallinnan menettelytavat, käytännöt ja prosessit (muodollinen / epämuodollinen), käytetäänkö aikaa tulevaisuuden uhkien ennakointiin vai keskitytäänkö hoitamaan päivittäisiä ongelmia, miten riskienhallinta on integroitu johtamiseen, riski-informaation hyödyntäminen johtamisen tukena, käytetyt työkalut jne.
    e. Muodollisen riskienhallintaprosessin tarve
    f. Tietoturvan suhde riskienhallintaan
        i. Sisäinen tietoturvatiimi (nyt, tulevaisuudessa)
        ii. Ulkoistukset ICT / tietoturva (nyt, tulevaisuudessa)
4. Tietoturva
    a. Suhtautuminen tietoturvaan yleisesti (johto, työntekijät)
    b. Tietoturvapolitiikka / sovitut tietoturvakäytännöt (information security policy)
    c. Tietoturvan nykytila (meneillään olevat kehitysprojektit jne.)
    d. Liiketoiminnan tarpeiden ja tietoturvan suhde (alignment to business needs)
    e. Merkittävimmät uhat
    f. Varautuminen uhkiin
    g. Tietoturvapoikkeamat (onko ollut? seuraukset?)

h. Kokemus, tietotaito (johto, työntekijät)
i. Vastatoimet (proaktiivinen, reaktiivinen, kontrollit: estäminen, palautumiskyky, havaitseminen), tärkeimmät suojattavat kohteet luokiteltu jne.
    i. Miten? (Teknologia / ihmiset / sertifiointi / vakuutukset / koulutus jne.)
j. Kumppanit, toimittajat, asiakkaat (esitättekö, onko teille esitetty tietoturvavaatimuksia jne.)
    i. Uhkatiedon / menetelmätapojen jakaminen kumppaneiden kesken (nyt, tulevaisuudessa)
k. Teknologia, nykyiset järjestelmät, rajapinnat
    i. Millä perusteilla valittiin nyt käytössä olevat järjestelmät ja työkalut? Mietittiinkö valinnassa tietoturva-aspekteja?

5. Päätöksenteko / investointiprosessi
    a. Kuka, ketkä päättää? Miten? (Muodollisuus /epämuodollisuus. päätösvallan jakautuminen)
    b. Investointibudjetit – kehittämistoimet, teknologia, tietoturva ym. eritelty? (nyt, tulevaisuudessa)
    c. Suhtautuminen kustannuksiin, investointien priorisointi (kasvu / voitollisuus / riskien välttäminen jne.)
    d. Käytetyt mittarit
    e. Tietoturvainvestoinnit
        i. Tavoitteet
        ii. Tuotto-odotus (Miten mitataan? Mitataanko?)
        iii. Yhteys kasvuun (riskienhallinta edellä vai kasvu edellä, ajatellaanko tietoturvainvestointeja kasvun kannalta)

LIITE 3 HAASTATTELURUNKO

3.haastattelu
Skenaario 1, investointipäätöstä tehtäessä painotettavat tekijät:

Mitkä asiat ovat tärkeitä investointipäätöstä tehtäessä ja arvioitaessa yleisesti? oma osaaminen, verkkohaku, kaverin suosittelu, hinta, tuotto-odotus, asiantuntijoiden suosittelu, jne. Mitkä tekijät vaikuttavat eniten tietoturvainvestointipäätöksiin? Esim. Muiden kokemukset, asiantuntijoiden suositukset, raha, lainsäädäntö ym.

Skenaario 2, konfliktitilanne:

Kaikki päätöksentekoon osallistuvat henkilöt eivät halua tehdä (tietoturva)investointia, vaikka suoraa vaihtoehtoista investointikohdetta ei ole (raha jää säästöön). Miten toimitaan? Annetaanko asian olla ja jätetään myöhemmäksi tms.? Onko tilanne realistinen?

Esim 1: 7900€ investointi sertifikaattiin (OWASP ASVS)
OWASP – ASVS = Open Web Application Security Project – Application Security Verification Standard
"Tehokas tapa varmentaa ja osoittaa verkkopalvelun tietoturvan taso"

Esim 2: Investointi koulutukseen:
"En halua mitään ylimääräisiä koulutuksia, muutenkin kädet täynnä jne."

Skenaario 3, valintaperusteet samaan kategoriaan kuuluvien tietoturvainvestointien välillä:

Mitä asioita tietoturvainvestointipäätöksessä painotetaan? Painotetaanko turvallisuutta vaiko hintaa? Hyötyä? jne. (Saman tyypin tietoturvainvestointien välillä; esim. pitää tehdä valinta eri haittaohjelmien torjuntaohjelmistojen välillä)

Esim 1: Tunnettu, laadukas, hyvät arviot, tietoturva-asiantuntijoiden suosittelema, kalliimpi kuin kilpailevat ratkaisut

Esim 2: Vähemmän tunnettu, uusi, ei vielä merkittävästi käyttäjäarvioita, keskimääräistä edullisempi

Skenaario 4, tietoturvainvestoinnit suhteessa vaihtoehtoisiin investointikohteisiin:

Vaihtoehtoisia investointeja: Toinen investointikohde tuo suoraa kasvua, liikevaihtoa ym., Toinen investointi korkeintaan epäsuorasti. Miten

toimitaan? (tietoturvainvestointi verrattuna esimerkiksi palvelinkapasiteetin laajentamiseen, markkinointikampanja tms.) Investointi kohteeseen, joka kasvattaa riskiprofiilia, mutta tuo myös kasvua ja rahaa jne. Miten hyötyä mitattaisiin? Miten sitä arvioidaan? Miten sitä suhteutetaan muihin investointeihin? Menevätkö muut investoinnit automaattisesti edelle, jotka tuovat kasvua ja rahaa taloon?

Esim 1: Markkinointikampanja, 5000€

Esim 2: Tietoturvaskanneri, verkkopalvelun tietoturva; automaattinen haavoittuvuuksien testaus 5000€

Skenaario 5, Käytetyt työkalut investointipäätöksen tukena:

Esim. RICE-priorinsointityökalun hyödyntäminen vrt. joku muu, viitekehykset, industry best practises jne. Millä asioilla merkitystä? Helppokäyttöisyys, entuudestaan tuttu jne. Onko ylipäätään tarvetta?

Skenaario 6, Valinta erilaisten taloudellisten investointimallien välillä (ROI, UM, ym.,):
Näettekö nämä mahdollisesti käyttökelpoisina? Mitä hyötyjä? Mitä ongelmia? jne.

Skenaario 7, (Tietoturva)investointistrategia:

Miten kuvailisitte yrityksenne tietoturvainvestointistrategiaa? Painotus; esim. kyberresilienssi, palautumiskyky, estäminen, havainnointikyky, koulutus jne. Keinot; tekniset kontrollit, käyttäjien tietoturvakoulutus jne.

LIITE 4 Tapausyrityksen toimintatavat ja yrityskulttuuri

Tämän liitetiedoston tarkoituksena on pohjustaa tapausyrityksen tapaa tehdä päätöksiä, jotta lukija voi halutessaan paremmin ymmärtää, miten tietoturvainvestoinnit ilmenivät yrityksessä suhteessa kokonaiskuvaan.

Yrityksen syntyhistoria

Yritys on perustettu maaliskuussa 2019. Rahoitusta yritys sai ensimmäisen kerran kesällä 2019. Yrityksen alkuperäinen idea ja liiketoimintamalli muuttui radikaalisti joulukuussa 2019. Liiketoimintamallin merkittävä muutos on hyvä esimerkki perustajien yrittäjämäisestä suuntautumisesta (mm. Gabrielsson & Gabrielsson, 2013; Lewis & Churchill, 1983), josta useat organisaation kasvuteoriat puhuvat. Yrityksessä reagoitiin ketterästi muutoksiin ympäristössä ja mukautettiin omaa tekemistä (Picken, 2017).

> ”Ei, se (idea) on itseasiassa muuttunut erittäin paljon. Alkuperäinen idea oli --, mutta sitten siihen sillä hetkellä tuli markkinoille tuli just Suomeen kilpailija siihen. Niin siinä ei ollut enää järkeä lähteä siihen, koska heillä oli niin pitkä etumatka, se ei ollut enää fiksua. Sitte muutaman välivaiheen kautta tuli semmonen idea, että tällaiselle ois kysyntää… -- * Sanoi että tälläiselle olisi yleisesti tarvetta mutta tämmöstä ei oo vielä olemassa. Ja sit se (idea) rakentu tähän.” COO 1. haastattelu

Toiminta oli hyvin dynaamista ja ketterää. Yrityksen selviytymisen ja menestymisen kannalta on elintärkeää, että yritys osaa sekä löytää että luoda uusia mahdollisuuksia kasvaa ja tehdä liiketoimintaa (Gabrielsson & Gabrielsson, 2013). Liiketoimintamahdollisuuksia etsittiin aktiivisesti ja niihin tartuttiin tilaisuuden tullen. Yritys löysi pääomasijoittajan ottamalla kontaktia alan tekijöihin. Liiketoimintamalli syntyi keskustelemalla alan toimijoiden kanssa; mitä asioita kaivattaisiin ja mille olisi tarvetta. Pickenin (2017) mukaan startup-vaiheessa tärkeintä on määritellä yrityksen liiketoimintamalli ja todistaa sen toimivuus käytännössä.

Liiketoimintamalli, Kasvustrategia, Uhkakuvat ja Mahdollisuudet

Yritys toimi verkkokauppa-alalla. Yrityksen liiketoimintamalli oli hyvin mukana nykyisissä kehitystrendeissä ja suuntasi tulevaisuuteen. Yrityksen kasvustrategia vastasi hyvin Pickenin (2017) mallia. Yritys oli nyt startup- ja siirtymävaiheiden risteyskohdassa, jossa se testaa liiketoimintamallin toimivuutta ja rakentaa pohjaa liiketoiminnan skaalautuvuudelle.

> ”No, kasvu tavallaan ja semmonen skaalautuvuus, yritetty rakentaa tätä systeemiä muutenki niin, että pystyttäis skaalaamaan, ja tota, avaamaan uusia markkina-alueita. Et nyt me ollaan tohon Kiinaan keskitytty, mutta nimetyt tavoitteet… täytyy sanoo et

> meil ei oo kyl mitenkään kauheen tarkasti mitään vuositavoitteita asetettu, mutta tota, kasvu on niinku se ykköstavoite.″ CTO 2. haastattelu

Yrityksellä oli innovatiivinen liiketoimintamalli, jota kukaan Suomessa ei ollut vielä toistaiseksi lähtenyt tekemään. Tavoiteltu kohdemarkkina oli erittäin kilpailtu, mutta yritys tähtäsi omaan siivuunsa osana suurta kansainvälistä ekosysteemiä. Kansainvälistyminen oli yrityksen liiketoimintamallin ytimessä ja sen tähtäimessä olivat erityisesti ″eksoottiset″ markkinat (Suomen katsantokannasta).

Liiketoimintamallin lisäksi yrityksen alkuresursseilla ja valitulla kasvustrategialla on huomattava vaikutus yrityksen kasvuun (Storey, 2016; Littunen & Tohmo, 2003). Tapausyrityksessä ei vielä tiedetty voiko toiminnasta saada kannattavaa, sillä vastaavaa ei ollut aikaisemmin toteutettu. Erilaiset tuntemattomat riskit (Sommer ym., 2009) korostuivat; erityisesti haastatteluissa nousi esiin kansainvälistymiseen liittyviä haasteita, kuten poliittinen tilanne kohdemaissa, kulttuurierot, lainsäädäntö ja tullit.

Yrityksessä oli tehty kahden vuoden ″target-suunnitelma″ ja viiden vuoden suurpiirteinen suunnitelma. COO totesi ensimmäisessä haastattelussa, että tällä hetkellä yritys seurasi vielä aika hyvin tavoitteiden saavuttamisen suhteen kahden vuoden target-suunnitelmaansa. Target-suunnitelma sisälsi karkean budjetoinnin. Yrityksellä ei ollut erillisiä investointibudjetteja vaan yksi firman kassa.

Yritys oli voimakkaasti kasvuhakuinen ja valittu kasvustrategia oli hyvin aggressiivinen. Littusen ja Tohmon (2003) mukaan nopean kasvun yritysten perustajat aloittavat liiketoiminnan usein eri motiivein kuin muiden yritysten perustajat. Nopeasti kasvavien yritysten perustajien keskuudessa korostuvat tilannesidonnaiset ja muut ″vetotekijät″. Keskeisessä roolissa tapausyrityksen kasvustrategiassa oli toiminnan skaalaus ja uusien markkina-alueiden avaus. Kasvustrategiassa pyrittiin hyödyntämään mahdollisuuksien mukaan ulkoista rahoitusta, jonka kautta voitiin kasvattaa yrityksen resursseja, sitä kautta lisätä myyntiä, palkata lisää työntekijöitä jne., ja näin toteuttaa itseään ruokkiva kasvun kierre. Rahoituskierrokset olivat ensisijainen rahoituksen lähde. Ulkoinen rahoitus oli erittäin tärkeää valitun kasvustrategian kannalta. Yrityksessä oli mukana yksityinen pääomasijoittaja, jonka lisäksi yritys oli saanut rahoitusta mm. Business Finlandin Tempo-ohjelman kautta. Uuden henkilöstön palkkaus, kansainvälistymiseen liittyvät investoinnit ja markkinointi oli priorisoitu korkealle investointien joukossa. Myynti oli lähtenyt kunnolla käyntiin 2020 kesällä.

> ″Markkina haltuun ja kovaa kasvua. Sitten kun vasta hyvin jalansijaa markkinalla, niin vasta sitten voi alkaa nostamaan rahaaki sieltä. Että, eka kasvu, kasvu edellä.″-- ″Joo no totta kai kasvua haetaan, että huono startuppi olis, jos ei haettais.″ ″ Kasvu on niiku se tavoite. Ei niinkään se voitto tässä vaiheessa, eikä itse asiassa voitto vielä moneen moneen vuoteen tarkoitus, vaan se että kasvaa.″ COO 1. haastattelu

Yrityskulttuuri

> ”Organisaatiorakenne on meillä erittäin matala, että periaatteessa ei oo mitään johtajia tai työntekijöitä. Kaikki aika lailla niinku samalla lähtöviivalla. Ei paljoo aleta näin pienessä yrityksessä tommosta hierarkkiaa tekemään.” COO 1. haastattelu

Kaikki yrityksessä työskentelivät etänä ja yrityksellä ei ollut omaa toimistoa. Viestintätapa oli hyvin vapaa ja epäformaali. Yritys hyödynsi Scrum-menetelmän mukaisia lyhyitä kehitysjaksoja toiminnanohjauksessa. Kaikki työntekijät osallistuivat viikoittaisiin scrum-palavereihin. Keskinäisellä luottamuksella oli toiminnanohjauksessa merkittävä rooli. Itsenäinen työnteko vei suurimman osan ajasta: luottamusta ja vastuuta annettiin jokaiselle.

Päätöksenteko

Päätöksiä tehtiin pääasiassa yhdessä. Poikkeustilanteissa voitiin tehdä päätöksiä ilman, että kaikki osallistuivat. ”*Ihan triviaaleja asioita ei tarvitse kysellä, jokaisella lupa tehdä omia päätöksiä.*” COO 1.haastattelu. CTO korosti, että itsenäisesti tehdyt päätökset piti pystyä kuitenkin aina perustelemaan myös muille. Kaikilla perustajajäsenillä oli nimenkirjoitusoikeudet eli valtuudet toimia yrityksen nimissä.

> ”Luottamuksesta vielä sen verran. Mihinkään mikromanagerointiin ei lähdetä, että jos jollekin annetaan joku homma, niin siihen luotetaan, että se hoidetaa, eikä sitä tarvitse sit erikseen kysellä… Että meneekö ja miten sujuu jne. Jokainen saa tehdä itsenäisesti päätöksiä. Perustajajäsenistä kaikilla prokura-oikeudet. Saa tehdä koko firman puolesta päätöksiä.” COO 1. haastattelu

Kupi ym., (2009) esittävät, että yrittäjyyteen kuuluu rohkeus tehdä päätöksiä: yritystoiminnan kannalta on lopulta tärkeämpää tehdä päätöksiä kuin kuluttaa huomattavasti aikaa päätöksen tueksi tarvittavan taustatiedon hankkimiseen ja eri ratkaisuvaihtoehtojen arvioimiseen. Keskivertoa nopeammin kasvavissa yrityksissä on usein yrittäjämäisesti suuntautunut tiimi, joka osallistuu strategiseen suunnitteluun ja päätöksentekoon (Littunen & Tohmo, 2003). Tapausyrityksen vahvuutena oli matala organisaatio ja päätöksenteon notkeus. Päätöksiä voitiin tehdä ja toteuttaa nopealla aikataululla. Tehdyt päätökset dokumentoitiin yrityksessä tehtävienhallintaohjelmisto JIRA:an. Kasvu oli priorisoitu ensimmäiseksi myös investointipäätöksissä. ”Kymppien” investointeja tai kuluja ei pitänyt erityisemmin pohtia, mutta yrityksen nykyhetkessä raja meni ”jossain satasissa”. Silloin mietittiin, oliko asia / investointi tarpeellinen vai ei. Investointipäätösten tukena ei toistaiseksi käytetty mitään työkaluja tai viitekehyksiä. Merkittävimmät investoinnit henkilöstökulujen lisäksi painottuivat yrityksessä markkinointiin.

Yhteistyökumppanit ja asiakkaat

Tapausyrityksellä oli kolme yhteistyökumppania kohdemaassa: pääyhteistyökumppani, markkinointitiimi ja lakipalvelut. Kumppanit olivat keskisuuria organisaatioita. Kumppanit eivät olleet esittäneet toistaiseksi vaatimuksia riskienhallinnan, saati tietoturvan osalta. Yhteistyösopimuksiin oli kirjattu tapausyrityksen puolelta joitain tietoturvaan liittyviä velvoitteita, kuten velvoite informoida kumppaneita tietomurron tai muun kyberhäiriötilanteen yhteydessä. Maksupalvelunvälittäjä hoiti luottokorttitietoihin ym. liittyvät tietoturva-asiat.

> ”Aa joo, meil on maksuvälittäjäpalveluntarjoaja välissä (*) nii meiän ei periaatteessa tarvii välittää noista mitää. Se periaatteessa hoitaa ne kaikki, meiän ei tarvii periaatteessa niistä tietää mitää. Ne hoitaa sen meiän puolesta ja edellytyksenä on että niil on sit asiat kunnossa, meiän ei tarvii välittää siitä.” COO 1. haastattelu