TURUN KAUPPAKORKEAKOULU
Turku School of Economics

TIIVISTELMÄ

X	Pro gradu -tutkielma
	Lisensiaatintutkielma
	Väitöskirja

Oppiaine	Tietojärjestelmätiede	Päivämäärä	23.2.2011
Tekijä(t)	Antti Lehtimäki	Matrikkelinumero	
		Sivumäärä	108
Otsikko	”Se on ihan sellainen strateginen valinta…”: Jatkuvuudenhallinnan rooli suurissa suomalaisissa yrityksissä.		
Ohjaaja(t)	KTT Jonna Järveläinen		

Tiivistelmä

Ihmiset huollattavat autojaan, hankkivat varashälyttimiä ja ostavat erilaisia vakuutuksia. He pyrkivät luontaisesti välttymään ikäviltä yllätyksiltä ja hallitsemaan elämänsä tasapainoa, sillä odottamattomat negatiiviset tapahtumat aiheuttavat aina ongelmia ja erilaisia vahinkoja. Yritykset hyötyvät hyvästä varautumisesta ja valppaudesta yhtä lailla, sillä hallitsemalla jatkuvuuttaan ne voivat välttää häiriöt kokonaan tai minimoida niiden haittavaikutukset. Yritysten tapauksessa jatkuvuudenhallinta ei kuitenkaan ole yhtä luonnollista, sillä niiden pääkiinnostus kohdistuu ydinliiketoiminta-alueisiin. Tämä tutkimus tarkasteleekin jatkuvuudenhallinnan roolia suurissa suomalaisissa yrityksissä. Samalla pyritään löytämään erilaisia jatkuvuudenhallinnan ilmenemismuotoja sekä hyviä käytäntöjä.

Jatkuvuudenhallinta on prosessi, joka tulee aloittaa luomalla jatkuvuussuunnitelma. Suunnitelman laatiminen sisältää tietyt perusosat, jotka toteuttamalla suunnitelmasta tulee käyttökelpoinen ja organisaation liiketoiminnallisia tavoitteita tukeva. Siihen sisältyy esimerkiksi uhkien ja heikkouksien ja vaikutusten analysointia, liiketoimintaprosessien priorisointia, riskien ehkäisystrategioiden valintaa, koulutusta, testausta, tarkastusta sekä lopulta ylläpitoa, joka aloittaa prosessin alusta. Vaiheiden toteutustapa kertoo jatkuvuudenhallinnan merkityksestä yritykselle.

Suunnittelun toteutustavan ohella jatkuvuudenhallinnan roolista kertoo se, missä määrin yritys pyrkii parantamaan toipumisnopeuttaan, joustavuuttaan häiriöiden suhteen sekä sulauttamaan jatkuvuudenhallintaprosesseja ja -ideologiaa henkilöstönsä jokapäiväiseen toimintaan. Lisäksi rooliin vaikuttaa myös todellisen toiminnan suhde lainsäädäntöön ja muihin jatkuvuudenhallinnan ulkoisiin vaatimuksiin. Strategisen jatkuvuudenhallinnan tulee tukea liiketoimintastrategian tavoitteita tehostamalla poikkitoiminnallisesti yrityksen kykyä vastustaa häiriöitä ja tarjoamalla vakaan pohjan yrityksen kilpailukyvylle. Sen tulee huomioida teknisten ratkaisujen ohella myös ihmiset, koska ongelmat ovat usein pohjimmiltaan sosiaalisia.

Tutkimuksen johtopäätöksenä voidaan todeta, että jatkuvuudenhallinnan rooli suurissa suomalaisissa yrityksissä on vaihteleva. Havaintojen perusteella organisaatiot jakautuvat kolmeen eri luokkaan: 1. niihin, joille jatkuvuudenhallinta on liiketoiminnan mahdollistaja 2. niihin, joille jatkuvuudenhallinta on tukitoiminto sekä 3. niihin, joille jatkuvuudenhallinta on strateginen tekijä. Liiketoiminnan mahdollistajana jatkuvuudenhallintaan suhtaudutaan lähinnä välttämättömänä pahana, kun taas strategisessa roolissa sitä pidetään liiketoiminnan menestystekijänä. Tukitoiminto-rooli on edellisten yhdistelmä ja jatkuvuudenhallinnan laatu vaihtelee yrityksen eri osien välillä.

Asiasanat	Jatkuvuudenhallinta, jatkuvuussuunnitelma, toipumissuunnitelma, strategia, häiriö
Muita tietoja	

Turun yliopisto
University of Turku

”SE ON IHAN SELLAINEN STRATEGINEN VALINTA…”

Jatkuvuudenhallinnan rooli suurissa suomalaisissa yrityksissä

Tietojärjestelmätieteen pro gradu -
tutkielma

Laatija:
Antti Lehtimäki

Ohjaaja:
KTT Jonna Järveläinen

23.2.2011
Turku

Sisällys

Kuvioluettelo

Taulukkoluettelo

1 JOHDANTO

1.1 Tutkimuksen taustaa

Tämä tutkimus käsittelee suurten suomalaisten yritysten jatkuvuudenhallintaa. Käsite on puettu teoreettiseksi viitekehykseksi vasta melko äskettäin, mutta käytännössä se on ollut olemassa jo todella pitkään. Jokainen ihminen toimii enemmän tai vähemmän tiedostamattaan jatkuvuudenhallinnan periaatteiden mukaisesti. Pyrimme luontaisesti varjelemaan elämäämme ja omaisuuttamme erilaisin toimintatavoin ja apuvälinein. Huollatamme auton säännöllisesti, jotta matka ei katkeaisi yllättäen, hankimme hälyttimiä varkaiden varalta ja vakuutamme kotimme. Niin yksittäiset ihmiset kuin yrityksetkin haluavat hallita jatkuvuuttaan välttyäkseen ikäviltä yllätyksiltä ja vähentääkseen niiden aiheuttamia haittavaikutuksia.

Hyviä esimerkkejä tapauksista, joissa jatkuvuudenhallinnalla on voitu vähentää liiketoiminnan häiriöitä ja tappioita ovat suomalaisahtaajien lakko maaliskuussa 2010, Eurooppaa kiusannut vulkaaninen tuhkapilvi huhtikuussa 2010 sekä Australian tulvat tammikuussa 2011. Loppukesällä 2010 Suomessa riehuneet voimakkaat myrskyt aiheuttivat päänvaivaa esimerkiksi tietoliikenne- ja sähköverkkojen kaatumisen vuoksi. Syksyllä 2010 taas uutisotsikoihin nousivat pankkien palkan- ja eläkkeenmaksujärjestelmien häiriöt. Kaikki edellä mainitut ongelmat olisivat olleet vältettävissä tai niiden vaikutus liiketoiminnalle olisi voinut olla toteutunutta pienempi, mikäli riskit olisi tiedostettu ja niiltä olisi suojauduttu etukäteen.

Yrityksen liiketoiminnan jatkuvuus ja häiriöiden aiheuttamat vahingot ovat hyvin riippuvaisia siitä, kuinka hyvin erilaisiin uhkatekijöihin on varauduttu. Jatkuvuudenhallinnan tehtävänä on turvata yrityksen kriittisten prosessien toimintakyky ja strategisten tavoitteiden saavuttaminen epävarmuustekijöiden vallitessa. Sillä pyritään toisaalta minimoimaan riskien haittavaikutukset, mutta myös mahdollistamaan organisaation tehokas toipuminen (Gibb & Buchanan 2006, 129). Optimaalinen tilanne on, että liiketoiminta rullaa normaalisti tilanteessa kuin tilanteessa ja haitalliset vaikutukset kyetään ehkäisemään kokonaan.

Tutkimus on osa laajempaa, tietoturvaa käsittelevää Turun Kauppakorkeakoulun tietojärjestelmätieteen projektia, jota Liikesivistysrahasto tukee. Jatkuvuudenhallintaan liittyy paljon tietoturvakysymyksiä, sillä tiedon saatavuus, luotettavuus ja eheys voivat epäonnistuessaan aiheuttaa merkittävää vahinkoa liiketoiminnalle. Myös toinen tutkija teki omaa pro gradu -tutkimustaan osana tätä projektia ja sen kohteena oli erityisesti toipumissuunnittelu. Tutkimusaiheiden yhtäläisyyksistä johtuen tutkimusaineisto kerättiin yhteistyössä ja haastattelujen kielenä pyrittiin käyttämään englantia. Toipumissuun-

nittelunäkökulma vaikutti myös siihen, että tutkimus pyrkii vastaamaan tutkimuskysymyksiin keskittyen hieman enemmän tietohallinnon jatkuvuudenhallintaan.

1.2 Tutkimusongelma

Jatkuvuudenhallinnalla voi siis olla suuri vaikutus yrityksen pitkän aikavälin tavoitteiden saavuttamiseen. Kyseinen yhteys ei ole kuitenkaan välttämättä niin selvä, että jatkuvuudenhallinta olisi juurruttanut itsensä kaikkien yritysjohtajien mieliin. Ydinliiketoiminnan tuottavuuteen ja kehittämiseen keskitytään usein niin suurella tarmolla, ettei jatkuvuudenhallinnan strategista arvoa ehditä ymmärtää. Tämä tutkimus pyrkiikin selvittämään, millainen on jatkuvuudenhallinnan rooli suurissa suomalaisissa yrityksissä. Pidetäänkö sitä strategisena ja yrityksen menestyksen kannalta tärkeänä vai onko se kenties vain operationaalista, jolla suojataan yrityksen henkilöstöä ja omaisuutta? Tulosten avulla voidaan arvioida jatkuvuudenhallinnan tasoa, siihen liittyviä asenteita sekä sitä, nähdäänkö jatkuvuus myös kilpailuetuna. Tutkimuksen pääongelma on:

- Millainen on jatkuvuudenhallinnan rooli suurissa suomalaisissa yrityksissä?

Pääongelman lisäksi pyritään vastaamaan myös seuraaviin alakysymyksiin:

- Miten jatkuvuudenhallinta voi ilmetä yrityksen toiminnassa häiriöiden ulkopuolella?
- Millaista kilpailuetua jatkuvuudenhallinnalla pyritään saavuttamaan?
- Onko jatkuvuudenhallinnassa havaittavissa hyviä käytäntöjä ja millaisia ne ovat?

1.3 Tutkimuksen rakenne

Tutkimuksen ensimmäinen kappale johdattelee lukijan aiheeseen. Siinä perustellaan tutkimuksen olemassa olo ja tärkeys sekä kuvataan tutkimuksen lähtökohtia. Johdannossa käydään läpi myös kysymykset, joihin tällä tutkimuksella pyritään löytämään vastauksia.

Toinen kappale käsittelee jatkuvuudenhallinnan teorian. Siinä määritellään, mitä jatkuvuudenhallinnalla tässä tutkimuksessa tarkoitetaan ja käydään läpi jatkuvuussuunnitteluprosessin sisältö. Jatkuvuudenhallinnan toteutuksen perustelemiseksi esitellään sen hyödyt, mutta toisaalta myös kustannukset. Tämän jälkeen käsitellään jatkuvuudenhallintaan liittyviä standardeja, lainsäädäntöä ja erityisesti tietoturva-asioita, koska niillä kaikilla on oma merkityksensä jatkuvuudenhallinnan roolin ymmärtämisessä. Lopuksi perehdytään strategiseen jatkuvuudenhallintaan ja sen ilmenemismuotoihin.

Kolmannessa kappaleessa kuvaillaan ja argumentoidaan tutkimuksen toteutusmenetelmä. Siinä kerrotaan yksityiskohtaisesti, miksi kyseiseen tutkimustapaan päädyttiin ja miten aineisto kerättiin ja analysoitiin. Samassa kappaleessa arvioidaan myös tutkimuksen luotettavuutta.

Neljännessä luvussa esitellään ja analysoidaan tutkimuksen havaintoja. Ne käsitellään teemoittain ja jokaisesta teemasta nostetaan esiin merkittävimmät esille nousseet asiat. Samalla analysoidaan havaintojen syitä ja arvioidaan niiden vaikutuksia jatkuvuudenhallinnan rooliin.

Viides luku vetää yhteen tutkimuksessa tehdyt keskeiset havainnot ja esittelee niiden perusteella tehdyt johtopäätökset. Kappaleessa todetaan myös tiedossa olevat tutkimuksen rajaukset ja pohditaan aiheita jatkotutkimukselle.

2 JATKUVUUDENHALLINTA

2.1 Määritelmä

Jatkuvuudenhallinta (*business continuity management, BCM)* on melko uusi termi tieteellisissä julkaisuissa. Se on oikeastaan kattokäsite, joka sisältää useita iäkkäämpiä riskienehkäisy- ja toipumisprosesseja kuvaavia termejä kuten kriisienhallinnan (*crisis management*) ja valmiussuunnittelun (*contingency planning*). Alun perin eri termeillä on ollut oma merkityksensä, mutta aikojen saatossa ne ovat yhdenmukaistuneet. Samoja termejä on kuitenkin usein käytetty tarkoittamaan hieman eri asioita ja joskus eri termeillä on viitattu samaan asiaan. Tämän vuoksi jatkuvuudenhallinnan tutkimus on joiltakin osin sekavaa. Määritelmistä löytyy kuitenkin myös yhtäläisyyksiä ja niiden perustavanlaatuisena ajatuksena on aina yrityksen toiminnallisuuden ylläpitäminen sekä häiriöiden hallinta. (HB 292-2006)

British Standards Institution (BCM Institute 2010) määrittelee BS 25999 -standardissaan jatkuvuudenhallinnan koko organisaation kattavaksi johtamisprosessiksi, jolla huolehditaan tärkeiden liiketoimintojen jatkumisesta ja toipumisesta häiriöiden sattuessa. Siinä tunnistetaan yrityksen liiketoiminnan uhat ja niiden toteutumisen aiheuttamat vaikutukset. Tämän analyysin pohjalta luodaan tehokkaan reagoinnin ja toipumisen mahdollistavat suunnitelmat häiriötilanteiden varalle. Suunnitelmia harjoitellaan ja koulutetaan ja ne tarkastetaan säännöllisesti ajantasaisuuden ja toimintakyvyn varmistamiseksi. Näin jatkuvuudenhallinnalla saavutetaan parempi organisationaalinen joustavuus ja toipumiskyky, joilla suojataan yrityksen arvoa (Calder 2008, 15). Lähes identtisesti ovat jatkuvuudenhallinnan määrittäneet myös Business Continuity Management Institute sekä Business Continuity Institute (BCM Institute 2010).

Herbane, Elliott ja Swartz (2004, 435) yhtyvät edelliseen määritelmään, mutta he mainitsevat erityisesti myös sen, että menestyksekkään jatkuvuudenhallinnan edellytyksenä on täydellinen ymmärrys sekä yrityksen sisäisistä että ulkoisista uhkatekijöistä. Organisaation tulee lisäksi tunnistaa inhimilliset voimavaransa ja hyödyntää niitä oikein jatkuvuuden ja toipumisen turvaamiseksi. Ihmiset ovat kuitenkin loppujen lopuksi ne, jotka suunnitelmia toteuttavat. Jatkuvuudenhallinta on Herbanen ym. (2004, 439) mukaan sosiotekninen prosessi, eli se huomioi poikkitoiminnallisesti organisaation, ihmiset ja työn muutokset.

BS 25999 -standardin määritelmä jatkuvuudenhallinnalle lähtee liikkeelle yrityksen uhista ja niiden mahdollisista vaikutuksista yritykseen. Uhkien huomioimisen kautta saavutettu toiminnallinen joustavuus vaikuttaa pitkällä tähtäimellä yrityksen arvoon. Toinen yleisesti tunnettu jatkuvuudenhallinnan määritelmä lähestyy asiaa prosessien ja resurssien näkökulmasta. Sen mukaan jatkuvuudenhallinnan tehtävä on turvata kriittis-

ten tavoitteiden kannalta oleellisten prosessien sekä niitä tukevien resurssien saatavuus, jotta halutut tavoitteet saavutettaisiin. Tämä edellyttää proaktiivista toimintaa ja ongelmien estämistä tai minimoimista jo ennen kuin ne ehtivät ilmaantua. (HB 292-2006 2006, 8; Hecht 2002, 444; Devargas 1999, 36)

Hecht (2002, 444) korostaa, että jatkuvuudenhallinta turvaa yrityksen kaikkien kriittisten liiketoimintojen toimintakyvyn perinteisen tietoteknisen fokuksen sijaan. Hän näkee myös, että jatkuvuudenhallinta on erityisesti liiketoiminnallinen asia, joka vaatii sitä koskevien ongelmien ratkaisua. Niistä tosin monet – mutta eivät kaikki – liittyvät tietotekniikkaan ja -järjestelmiin. Myös Gibbin ja Buchananin (2006, 129) mukaan jatkuvuudenhallinnan tulisi olla koko yrityksen kattava toiminto, vaikka monessa yrityksessä sen paino onkin selvästi IT-puolella. Information Technology Infrastructure Libraryn (*ITIL*) mukaan IT-palvelujen jatkuvuudenhallinta tukee koko liiketoiminnan jatkuvuudenhallintaa, eli IT on sen mukaan vain yksi, mutta tärkeä osa koko liiketoiminnan jatkuvuutta. IT-palvelujen jatkuvuudenhallinnalla vähennetään riskejä ja suunnitellaan tietojärjestelmien ja -tekniikan toipuminen. Tärkeä osa tätä prosessia on siis myös tietoturva (Long 2008, 24).

Edellisistä voidaan johtaa tässä tutkielmassa käytetty jatkuvuudenhallinnan määritelmä:

> *Jatkuvuudenhallinnalla tarkoitetaan kaikkia niitä prosesseja, joilla ensin tunnistetaan yrityksen uhkatekijät ja haavoittuvuudet, sitten arvioidaan niiden mahdolliset vaikutukset ja lopulta suunnitellaan ja toteutetaan ehkäisytoimenpiteet, joilla riskejä ehkäistään ja haitallisia vaikutuksia minimoidaan – sekä ennalta, että tarvittaessa reagoiden.*

Jatkuvuudenhallinnan tehtävänä on kehittää ja ylläpitää koko organisaation joustavuutta ja toipumiskykyä, joilla varmistetaan kriittisten tavoitteiden saavuttamiseksi tarvittavien prosessien ja resurssien jatkuva saatavuus. Tämä suojelee sidosryhmien etuja, yrityksen mainetta ja brändiä sekä arvoa tuottavia toimintoja.

2.2 Jatkuvuus- ja toipumissuunnittelu

Jatkuvuus- ja toipumissuunnittelu ovat jatkuvuudenhallinnan keskeiset prosessit, joilla pyritään turvaamaan toiminnan joustavuus ja katkeamattomuus. Liiketoiminnan jatkuvuussuunnittelu (*business continuity planning*) on sosiotekninen prosessi, jossa kehitetään ja määritellään ne toimenpiteet, joilla yritys pyrkii varmistamaan tuotannontekijöiden jatkuvan saatavuuden ja siten kriittisten liiketoimintojen jatkuvuuden myös häiriötilanteissa ja niiden jälkeen (Devargas 1999, 36).

Jatkuvuussuunnittelu liitetään yleensä nimenomaan operationaalisen toiminnan proaktiiviseen suojaamiseen ja se huomioi normaalin toiminnan edellytykset, kuten ihmiset, tiedot ja materiaalit. Jatkuvuussuunnittelu vaikuttaa usein esimerkiksi yrityksen teknologiastrategiaan määrittelemällä sen, millaiset tietokatkokset ovat enimmillään sallittuja. Prosessin tuloksena syntyy kirjallinen dokumentti, jatkuvuussuunnitelma (*business continuity plan*), joka sisältää toiminnan jatkuvuutta parantavaa ja ylläpitävää informaatiota, kuten koulutus- ja toimintaohjeita, aikatauluja, huoltotoimenpideohjeita sekä vastuita. Suunnitelma voidaan tehdä erikseen jokaiselle liiketoimintayksikölle niiden luonteesta riippuen. (BCM Institute 2010; Asnar & Giorgini 2008, 213; Calder 2008, 17, 20; Snedaker 2007, 3; HB 292-2006, 7; Herbane ym. 2004, 439)

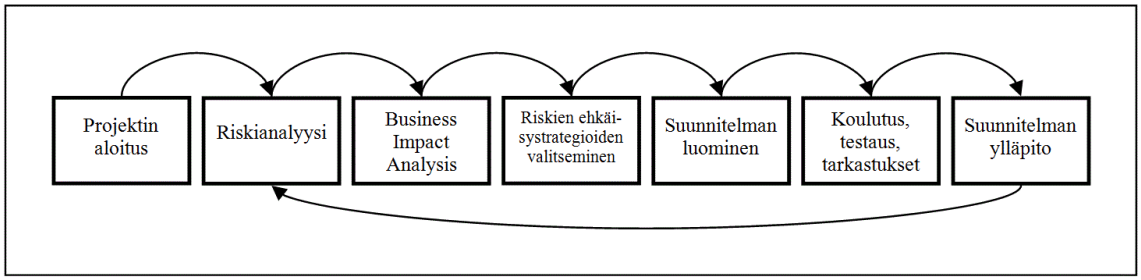
Toipumissuunnittelu (*disaster recovery planning*) on jatkuvuussuunnitteluun sisältyvä osa ja siinäkin on kyse hyvien toimintatapojen etsimisestä ja vaadittavien esivalmistelujen tekemisestä jatkuvuuden maksimoimiseksi. Toipumissuunnittelun fokus on kuitenkin informaatioteknologiassa, sen häiriötilanteissa ja reagoivassa toiminnassa (HB 292-2006, 7; Herbane ym. 2004, 438, 443). Häiriötilanne voi olla esimerkiksi palvelimet tuhoava tulipalo, verkkoyhteyksien katkeaminen, tietomurto tai vaikkapa kadonnut tietokone. Tavoitteena on luoda sellainen toipumissuunnitelma (*disaster recovery plan*), joka mahdollistaa yrityksen kriittisten toimintojen käyttämien IT-palvelujen ja tietoliikenneyhteyksien nopean palautumisen ongelmatilanteissa, jotta tärkeät prosessit voisivat jatkua vaaditulla vähimmäistasolla. Toipumissuunnitelma kuvaa tarkasti, kuinka erilaisten IT-häiriöiden sattuessa toimitaan, ketkä ovat prosessin avainhenkilöitä ja mitä resursseja tarvitaan. Näin voidaan estää häiriön leviäminen esimerkiksi sammuttamalla järjestelmiä, ehkäistä sen aiheuttamia haittoja ja käynnistää nopea palautuminen normaalitilaan (BCM Institute 2010; HB 292-2006, 7; Snedaker 2007, 4).

Herbane ym. (2004, 438-437) kuvaavat artikkelissaan jatkuvuus- ja toipumissuunnittelun lähtökohtaista eroa. Toipumissuunnitteluideologian mukaan häiriöt ovat väistämättömiä, koska niiden aiheuttajiin ei voida vaikuttaa. Jatkuvuussuunnittelu taas lähtee siitä, että kriisiä edeltää kytemisvaihe, jolloin jokin laukaiseva tekijä voi aktivoida sen. Näin ollen ehkäisemällä laukaisevia tekijöitä voidaan vähentää häiriöiden esiintymistiheyttä ja mahdollisesti myös niiden vaikutuksia.

Monille yrityksille jatkuvuudenhallinta tarkoittaa jatkuvuus- ja toipumissuunnittelun tuloksena syntynyttä arkistoitua dokumenttia, joka voidaan kaivaa esiin tarpeen vaatiessa. Sen tulee kuitenkin olla jatkuva prosessi, joka sisältää muutosten tarkkailua, suunnitelmien koulutusta, harjoittelua ja päivittämistä sekä yrityksen toiminnan parantamista, jotta ongelmat voitaisiin välttää tai niiden vaikutukset minimoida. Muuten vaarana on hämäävä turvallisuudentunne. (Laaksonen, Nevasalo & Tomula 2006, 230-233; Hecht 2002, 445)

Suunnitteluprosessi sisältää aina tietyt perusasiat. Snedaker (2007) on jakanut prosessin seitsemään eri vaiheeseen, jotka seuraavat toisiaan melko luonnollisesti. Seuraava

vaihe edellyttää usein edellisen vaiheen tietoja. Viimeinen vaihe – suunnitelman ylläpito – käynnistää prosessin aina uudelleen ja muistuttaa siitä, että yrityksen tulee jatkuvasti arvioida sen sisäisen ja ulkoisen toimintaympäristön muutoksia pitääkseen suunnitelman ajantasaisena. Hyvin samankaltaiset suunnitteluprosessin vaiheet esiintyvät myös Gibbin ja Buchananin (2006), Rittinghousen ja Ransomin (2006) sekä Devargasin (1999) julkaisuissa. Kuvio 1 esittää Snedakerin (2007, 31-35) mallin prosessista.



Kuvio 1 Jatkuvuussuunnitteluprosessi (Snedaker 2007, 31-35)

Snedakerin (2007, 31-35) jatkuvuussuunnitteluprosessin eri vaiheiden tunnistaminen ja arviointi on yksi osa jatkuvuudenhallinnan roolin tutkimusta. Mikäli organisaatio jättää toteuttamatta jatkuvuudenhallinnan perusosia tai tekee ne huonosti, ei riskien ehkäisy voi aidosti tukea yrityksen strategisten tavoitteiden saavuttamista tai muodostua itsessään kilpailueduksi. Prosessin vaiheet käydään seuraavaksi läpi tarkemmin, jotta niiden havaitseminen ja analysointi olisi tutkimuksen empiriaosiossa mahdollista. Ne antavat samalla kuvan kokonaisvaltaisen ja kilpailukykyisen jatkuvuudenhallinnan vaatimuksista. Eri vaiheiden tunteminen ja niiden tarkoituksen ymmärtäminen auttaa myös löytämään hyviä käytäntöjä, mikä on yksi tutkimuksen tavoitteista.

2.2.1 Projektin aloitus

Vaikka jatkuvuussuunnittelu on prosessi, tulee se aloittaa, kuin mikä tahansa projekti määrittelemällä vastuut, tavoitteet, vaatimukset, aikataulut ja budjetit. Mikäli jatkuvuudenhallinta ei ole syntynyt johdon aloitteesta, tulee ajatus ”myydä” myös heille. Organisaatio ei voi toteuttaa jatkuvuudenhallintaa, ellei sen johto ymmärrä jatkuvuudenhallinnan ideologiaa ja sitoudu tukemaan sitä. Johdon vakuuttaminen asiasta on kuitenkin osoittautunut haastavaksi tehtäväksi, koska heidän henkilökohtaiset intressinsä ovat toisaalla. Vaarana on, että jatkuvuudenhallinta jää vaille resursseja. Yritysjohto tulisikin kyetä motivoimaan osoittamalla jatkuvuuden suunnittelun ja johtamisen liiketoiminnallinen kannattavuus sekä sen tuoma lisäarvo. (Seow 2009, 201-202; Snedaker 2007, 3; Laaksonen ym. 2006, 229; Hecht 2002, 446)

Jatkuvuudenhallinnan aloitusvaiheessa tulee nimetä henkilö, joka on vastuussa toiminnan käynnistämisestä, jatkuvuussuunnitelman luomisesta, kommunikoinnista ja prosessin johtamisesta. Henkilön tulisi olla ylimmän johdon edustaja riittävän toimivallan ja tiedonkulun varmistamiseksi. Suuremmissa yrityksissä tehtävään voidaan nimittää useampia ihmisiä, mutta pienemmissä yrityksissä, joissa jatkuvuudenhallintatiimin muodostaminen olisi liiketoiminnan tarpeisiin ja taloudellisiin resursseihin nähden ylimitoitettua, jatkuvuudesta vastaa usein yksi henkilö oman toimensa ohella. (Tammineedi 2010, 39; Gibb & Buchanan 2006, 129; Hecht 2002, 447)

2.2.2 Riskianalyysi

Parantaakseen kriittisten prosessien ja resurssien keskeytymätöntä saatavuutta, yrityksen tulee ensin tunnistaa mahdolliset kriisit ja niiden syyt. Riskianalyysi on vaihe, joka ottaa riskienhallinnan mukaan jatkuvuudenhallintaan. Analyysi toteutetaan tunnistamalla ensin uhat, haavoittuvuudet sekä suojakeinot ja pyrkimällä sitten niiden perusteella määrittelemään uhkien toteutumisten todennäköisyydet ja vaikutukset. (Snedaker 2007, 137-141)

Uhat ovat McManuksen ja Carrin (2000) sekä Devargasin (1999, 37) mukaan voimia tai tapahtumia, joiden on mahdollista vaikuttaa yrityksen voimavaroihin epäsuotuisasti. Niitä ovat esimerkiksi inhimilliset virheet, tulipalot, tulvat, hakkerit, varkaat ja epärehelliset työntekijät. Haavoittuvuudet taas ovat yrityksen heikkoja kohtia, joita hyödyntämällä uhat voivat aiheuttaa vahinkoa. Ne myötävaikuttavat riskiin, koska ne voivat mahdollistaa riskin toteutumisen. Näin ollen uhka, joka voisi toteutuessaan aiheuttaa yritykselle vahinkoa, mutta jolla ei ole haavoittuvuutta, jota käyttää hyväksi, ei aiheuta yritykselle riskiä. Heikko kohta voi olla esimerkiksi virhe ohjelmistokoodissa tai puutteellinen kulunvalvonta. (Rittinghouse & Ransom 2006, 23; Devargas 1999, 37)

Riskien erilaiset ehkäisy- eli suojakeinot ovat mitä tahansa toimenpiteitä, käytäntöjä tai teknologioita, jotka kykenevät vähentämään yrityksen haavoittuvuutta jollekin uhkatekijälle. Suojakeinot toisin sanoen vähentävät uhan toteutumisen todennäköisyyttä tai sen haitallisia seurauksia ja siten myös riskiä. Ne ovat siis riskiin vaikuttavia tekijöitä aivan kuten haavoittuvuudetkin, mutta vaikutus on tässä tapauksessa yrityksen kannalta positiivinen. Suojakeinoja ovat esimerkiksi säännölliset koulutukset, murtohälyttimet sekä palomuurit. (Devargas 1999, 38)

Kun uhat, haavoittuvuudet ja suojakeinot tunnetaan, tiedetään teoriassa, mitkä uhista voivat toteutua. Tämän jälkeen tulee arvioida, millaiset olisivat uhan toteutumisen seuraukset. Seurauksilla tarkoitetaan niiden haittojen tai menetysten määrää, jotka voivat uhan toteutumisen vuoksi aiheutua. Devargas (1999, 38) toteaa, että seurauksilla viitataan nimenomaan yhteenlaskettuun, kaikki epäsuotuisat vaikutukset huomioon ottavaan

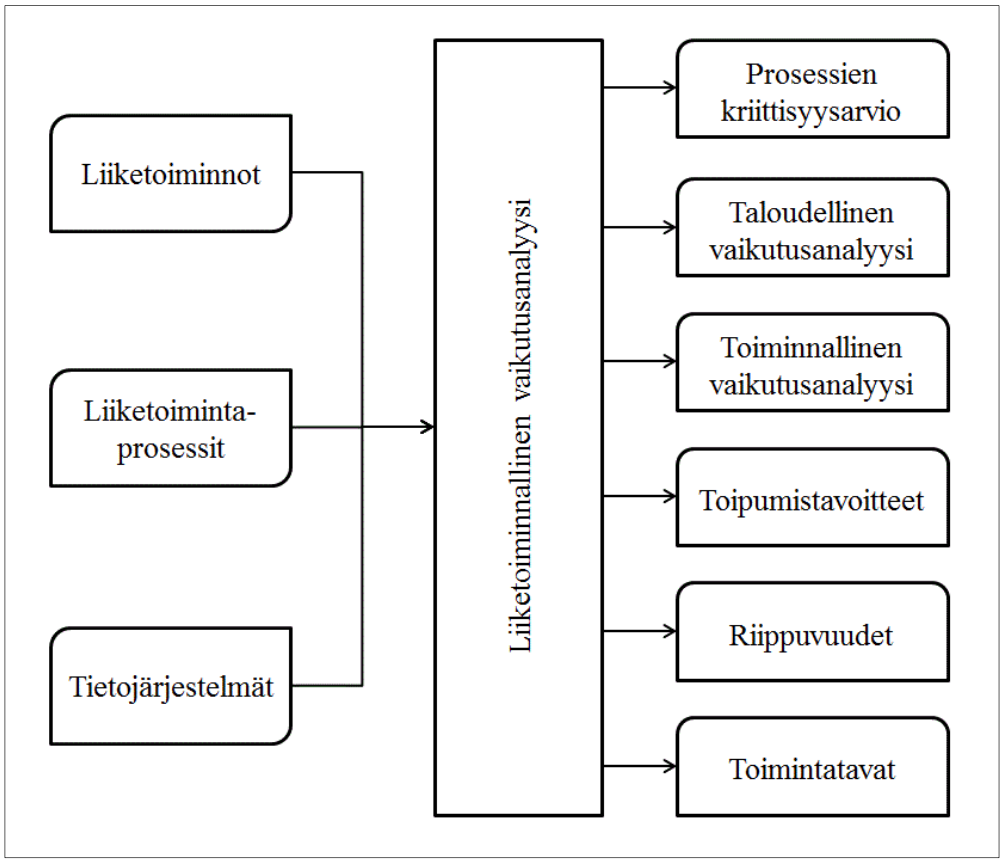
yhteishaittaan. Se sisältää siis sekä välittömät vaikutukset, kuten palvelun keskeytymisen ja toimituskatkokset, että pitkäaikaiset ongelmat, kuten maineen menetyksen. Mitä suuremmat ovat uhan realisoitumisen seuraukset, sitä vakavampi on myös riski.

Yrityksen tulisi kyetä määrittämään yksittäisten uhkien toteutumisten todennäköisyydet. Arvioinnissa pitää ottaa huomioon uhan vahvuudet, yrityksen heikkoudet sekä olemassa olevien suojakeinojen tehokkuus. Mitä suurempi on uhan toteutumisen todennäköisyys, sitä suuremmaksi riski kasvaa. Todennäköisyyksien ja seurausten arvioiminen on tärkeää, koska niillä on merkittävä vaikutus riskeiltä suojautumisen kannattavuuteen. (Devargas 1999, 38)

2.2.3 Liiketoiminnallinen vaikutusanalyysi

Riskianalyysivaiheessa seurauksia tarkastellaan uhkien näkökulmasta. Siinä etsitään tekijät, jotka voivat aiheuttaa haitallisia seurauksia ja arvioidaan, miten ne toteutuessaan vaikuttavat organisaation toimintaan. Riskianalyysin lisäksi yrityksen tulee tehdä myös erityinen liiketoiminnallinen vaikutusanalyysi (*business impact analysis*, *BIA*), joka lähestyy asiaa liiketoimintaprosessien kautta. Se on jatkuvuussuunnittelun kulmakivi. (Tammineedi 2010, 42; Snedaker 2007, 210)

Liiketoiminnallisen vaikutusanalyysin tarkoituksena on kertoa, minkälainen vaikutus tietyn prosessin toimimattomuudella on yritykselle. Sen perusteella voidaan päätellä, mitkä prosessit ovat liiketoiminnan kannalta kriittisimpiä. Suurennuslasin alla ei siis ole se, mikä aiheuttaa kyseisen ongelman. Analyysiä tehtäessä on tärkeää tutkia prosessien ja resurssien riippuvuuksia toisistaan sekä häiriön vaikutusta koko yritykseen – ei ainoastaan yksittäiseen liiketoimintayksikköön. Muuten vaarana on, että kaikki prosessit näyttävät yhtä kriittisiltä, mikä ei hyödytä päätöksenteossa ja aiheuttaa ylimääräisiä kustannuksia, koska resursseja kohdistetaan väärin. Mitä suurempi vaikutus prosessin häiriöllä on koko liiketoimintaan ja kriittisten tavoitteiden saavuttamiseen, sitä tärkeämpää on pitää se toimintakykyisenä. Liiketoiminnallinen vaikutusanalyysi luo jatkuvuudenhallinnan suunnittelulle hyvän pohjan osoittamalla tärkeät ja vähemmän tärkeät prosessit. Näin resurssit käytetään suojelemaan yrityksen kannalta merkittävimpiä prosesseja (Tammineedi 2010, 42; Snedaker 2007, 211-212; Devargas 1999, 41). Kuvio 2 havainnollistaa liiketoiminnallisen vaikutusanalyysin prosessia. Se kuvaa, kuinka yrityksen toimintoja, prosesseja ja tietojärjestelmiä analysoimalla luodaan tietoa, jota hyödynnetään häiriöttömyyden ylläpitämiseksi.



Kuvio 2 Liiketoiminnallinen vaikutusanalyysi (Snedaker 2007, 224)

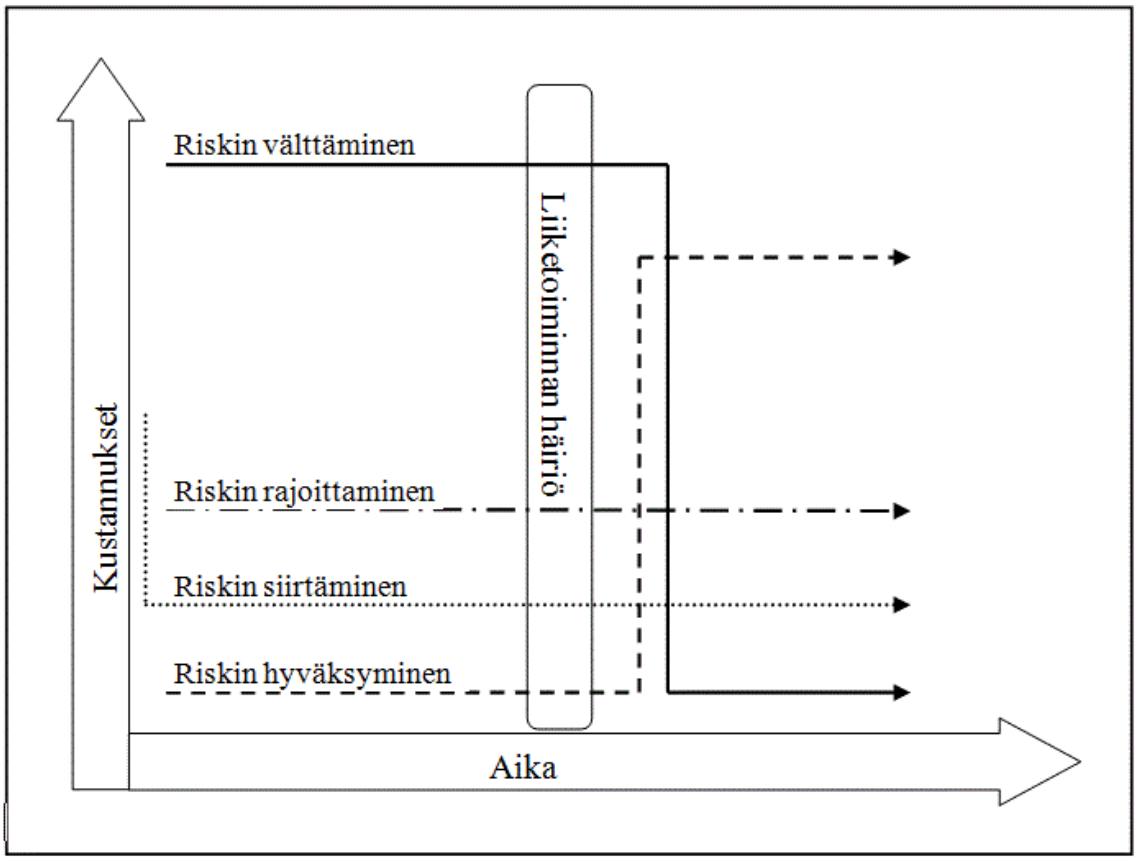
Analyysin pohjalta johdon tulee määrittää kunkin prosessin toipumistavoitteet, eli maksimaalinen häiriönsietoaika (*maximum tolerable period of outage, MTPoD*) sekä sen toipumisaika- (*recovery time objective, RTO*) ja toipumispistetavoitteet (*recovery point objective, RPO)*. Maksimaalinen häiriönsietoaika on se häiriön vaikutusaika, jonka jälkeen yrityksen toimintaedellytykset ovat peruuttamattomasti heikentyneet. Toipumisaikatavoitteella tarkoitetaan sitä aikarajaa, jonka puitteissa häiriöstä kärsinyt toiminto, tuote tai palvelu pitää saada toimimaan vähimmäisvaatimusten mukaisesti. Toipumisaikatavoitteen tulee siis olla pienempi kuin maksimaalinen häiriönsietoaika. Toipumispiste taas kertoo sen, mikä on se kauimmaisin menneisyyden ajanhetki, josta tiedot tulee voida palauttaa. Se siis määrittää, kuinka paljon dataa yrityksellä on varaa enimmillään menettää. Jollakin yrityksellä toipumispiste voi olla esimerkiksi seitsemän vuorokautta, mikä tarkoittaa, että kaikki sen tiedot tulee voida palauttaa enintään viikon takaa. (Tammineedi 2010, 42; Snedaker 2007, 210-212)

2.2.4 Riskien ehkäisystrategioiden valinta

Riskianalyysin ja BIA:n avulla yritys tunnistaa erilaiset uhat, niiden todennäköisyydet ja seuraukset sekä asettaa riskit ja prosessit tärkeysjärjestykseen. Tämän jälkeen voidaan etsiä ja arvioida ne vaihtoehdot, joita tunnistettujen riskien hallitsemiseksi, eli haitallisten vaikutusten ehkäisemiseksi on käytettävissä. Jotta yritys voisi valita haitallisten vaikutusten minimoimiseksi sovellettavat toimintatavat, sen tulee ensin valita strategiat, jolla riskejä pyritään ehkäisemään. (Sumner 2009, 2; Snedaker 2007, 262; Gibb & Buchanan 2006, 133)

Riskien erilaiset ehkäisy- eli suojakeinot pyrkivät vaikuttamaan riskiin eri tavoin: ennakoiden tai reagoiden. Ennakoivilla toimenpiteillä pyritään eliminoimaan kriittisten tavoitteiden saavuttamisen esteet jo ennalta, joten ne kuuluvat jatkuvuussuunnitelmaan. Reaktiiviset toimenpiteet taas liittyvät yleensä toipumissuunnitteluun ja syntyneen häiriötilanteen hallitsemiseen. Suojakeinon teho riippuu sen vaikutuksesta sekä riskin tasoon että riskin toteutumisen aiheuttamiin seurauksiin. Jokaiselle ehkäisytoimenpiteelle tulee aina tehdä kustannus-hyötyanalyysi, jossa riskin pienentämisellä saavutettavia odotettuja taloudellisia hyötyjä verrataan suojakeinon aiheuttamiin kustannuksiin. Näin voidaan todeta sen taloudellinen kannattavuus. Tavoitteena on, että riskeihin, joilla on sekä vakavat seuraukset että suuri todennäköisyys, kanavoidaan myös eniten resursseja. (Sumner 2009, 2; Gibb & Buchanan 2006, 133-135)

Jatkuvuussuunnittelu lähtee liikkeelle ajatuksesta, jossa riskien toteutumista pyritään ehkäisemään ja niiden vaikutuksia minimoidaan jo ennalta. Strategiat, joilla riskejä voidaan ehkäistä, ovat välttäminen (*avoidance*), siirtäminen (*transference)* ja rajoittaminen (*limitation*). Lisäksi strategiaksi lasketaan myös riskin hyväksyminen (*acceptance*), mutta sillä ei ole vaikutusta riskin tasoon. Jokaiselle riskille voi olla olemassa useita ehkäisytapoja, jotka käyttävät eri strategiaa. (Gibb & Buchanan 2006, 133-135) Niiden vaikutukset riskin tasoon kuten myös lyhyen ja pitkän aikavälin kustannukset ovat erilaisia. Kuvio 3 havainnollistaa eri strategioiden kustannusten riippuvuutta ajanhetkestä. (Snedaker 2007, 263-266)



Kuvio 3 Riskien ehkäisystrategioiden kustannusten ja ajan välinen riippuvuus (Snedaker 2007, 263)

Ensimmäinen ja lyhyellä tähtäimellä halvin strategia riskin hallitsemiseksi on sen hyväksyminen. Se ei ole varsinaisesti riskin ehkäisystrategia, sillä se ei vaikuta riskin tasoon millään tavoin. Hyväksyminen on helppo toteuttaa, koska se ei vaadi käytännössä minkäänlaisia toimenpiteitä. Samalla tulee kuitenkin tiedostaa, että yrityksen kannettavaksi jää riski siitä, että ongelmien ilmetessä vahingot ja kustannukset muodostuvat paljon suuremmiksi kuin muissa riskinehkäisystrategioissa. Riskin hyväksyminen voi olla hyvä vaihtoehto silloin, kun muut strategiat tulisivat kalliimmaksi kuin riskin toteutumisesta aiheutuvat kustannukset. (Snedaker 2007, 263-264; Gibb & Buchanan 2006, 136)

Toinen vaihtoehto riskin ehkäisystrategiaksi on riskin välttäminen. Sen tavoitteena on poistaa riski kokonaan ja siksi se onkin lyhyellä aikavälillä strategioista kallein. Riskin välttämisellä pyritään siis tilanteeseen, jossa kyseiselle riskille ei altistuta lainkaan. Se ei ole useinkaan kovin järkevä strategia, koska kustannukset nousevat herkästi hyvin korkeiksi suhteessa riskin toteutumisen aiheuttamiin haittoihin. Jos onnettomuus kuitenkin sattuu ja häiriöitä ilmenee, jäävät niiden aiheuttamat kustannukset huomattavasti riskin hyväksymisstrategian vastaavia pienemmiksi. (Snedaker 2007, 264-265)

Kolmantena ja yleisimpänä strategiavaihtoehtona on riskin rajoittaminen. Se tarkoittaa ryhtymistä riskiä ehkäiseviin toimiin, mutta tietyn riskitason hyväksymistä. Yritys

voi esimerkiksi luoda useita varmuuskopioita tietokannastaan, mutta hyväksyä sen, että kiintolevyt, joille data on tallennettu, voivat silti tuhoutua. Riskin rajoittaminen sijoittuu niin lyhyen kuin pitkänkin aikavälin kustannuksiltaan riskin välttämisen ja hyväksymisen välimaastoon, ollen ns. kultainen keskitie. (Snedaker 2007, 265; Gibb & Buchanan 2006, 135-136)

Viimeinen Snedakerin (2007, 263-266) riskin ehkäisystrategia on siirtäminen, jolloin riskiä siirretään jonkun muun kannettavaksi. Se voi tapahtua joko ulkoistamalla tai vakuuttamalla. Ulkoistaminen vähentää yrityksen riskiä, koska siten voidaan esimerkiksi hajauttaa toimintoja maantieteellisesti. Siihen liittyy yleensä sopimus myös palvelutasosta, jolloin oman toiminnan riski pienenee. Vakuuttaminen taas tarkoittaa sitä, että ulkopuoliselle taholle maksetaan siitä, että se sitoutuu maksamaan riskin toteutumisesta aiheutuneita kuluja (Snedaker 2007, 265-266; Gibb & Buchanan 2006, 135). Oleellista on kuitenkin muistaa, ettei vakuuttaminen ole automaattinen pelastus. Se saattaa korvata esimerkiksi tulipalon aiheuttamat vahingot, mutta jättää huomiotta aineettomia vahinkoja, kuten toteutumattoman myynnin ja heikentyneen luottamuksen. Lisäksi korvausten saaminen voi kestää liiketoiminnan kannalta liian kauan. Vakuuttaminen voikin olla tärkeä, muttei ainoa osa riskienhallintaa (Devargas 1999, 39).

Riskin siirtäminen sijoittuu sekä lyhyen että pitkän aikavälin kustannuksiltaan riskin rajoittamisen tienoille. Siirtämisessä on kuitenkin se ominaispiirre, että sen kustannukset jakautuvat yleensä pitkälle aikavälille esimerkiksi vuosittaisten vakuutusmaksujen muodossa, kun taas muiden strategioiden kustannukset sijoittuvat melko rajatuille ajanjaksoille. (Snedaker 2007, 265-266; Gibb & Buchanan 2006, 135)

Hecht (2002, 449) kuvaa artikkelissaan jatkuvuudenhallinnan perusongelmaa, eli kustannusten ja riskitason sopivan tasapainon löytämistä. Mitä pienempää riskiä yritys on valmis ottamaan ja mitä paremman toipumisvalmiuden se tarvitsee, sitä enemmän se joutuu investoimaan riskien ehkäisykeinoihin, kuten varmuuskopiointiin ja paloturvallisuuteen. Yrityksen tulee löytää itselleen riittävän alhainen riskitaso, joka on vielä taloudellisesti järkevä ylläpitää.

Sopivin riskien ehkäisystrategia riippuu suuresti siitä, minkälainen yritys on kyseessä ja paljonko johto on valmis riskiä kantamaan. Tietyillä aloilla riskiä halutaan välttää mahdollisimman paljon, kun taas toiset sietävät suurehkoakin epävarmuutta. Jotkut strategiat tuovat mukanaan uusia riskejä, joita ei myöskään pidä unohtaa. Strategia tulee luoda ottaen huomioon yrityksen toiminnalliset ja taloudelliset tavoitteet, käytettävissä olevat resurssit sekä riskienhallinnan tavoitteet. (Snedaker 2007, 262-263)

2.2.5 Suunnitelman luominen

Suunnitelmien luomisvaiheessa kaikki prosessin edellisissä vaiheissa kerätyt tiedot nivoutuvat yhteen ja niitä käsitellään yksityiskohtien tasolla. Jatkuvuussuunnitelman tarkoituksena on olla dokumentoitu kokoelma kaikista niistä tiedoista, joilla on jatkuvuudenhallinnalle merkitystä. Se sisältää rooleja, vastuita ja tehtäviä, joilla yritys pyrkii turvaamaan joustavuutensa ja toipumiskykynsä (Tammineedi 2010, 44). Lisäksi luodaan erillinen ylläpitosuunnitelma, josta ilmenee esimerkiksi miten organisationaaliset tai toimintaympäristöön liittyvät muutokset huomioidaan suunnitelman ylläpidossa. Häiriöiden varalta muodostetaan kommunikaatiosuunnitelma, jotta tiedetään, mistä asioista kriisitilanteessa tulee tiedottaa, kenelle informaatio suunnataan, milloin tiedon pitää liikkua ja mitä tiedotuskanavaa pitkin se siirretään (Snedaker 2007, 294, 325).

Suunnitelman luomisvaiheessa tulee muistaa myös se, ettei koko suunnitelmaa tarvitse aktivoida jokaisen häiriön kohdalla. Tämän vuoksi häiriöt luokitellaan niiden aiheuttamien seurausten perusteella esim. suuriin, keskisuuriin ja pieniin ja suunnitelmalle asetetaan aktivointikriteerejä, joiden täyttyessä avainhenkilöt tietävät ryhtyä toimiin. (Snedaker 2007, 296-297)

2.2.6 Koulutus, testaus ja tarkastukset

Suunnitelmien valmistumista seuraa koulutus-, testaus- ja tarkastusvaihe. Koulutuksella tarkoitetaan sitä, että henkilöstölle viestitään jatkuvuudenhallinnasta sekä sen hyödyistä ja tavoitteista (Gibb & Buchanan 2006, 138). Avainhenkilöiden mieliin kirkastetaan heidän roolinsa ja vastuunsa suunnitelmassa sekä opetetaan ne taidot, joita heiltä edellytetään (Snedaker 2007, 360). Testaus taas on keino arvioida jatkuvuussuunnitelman toimintatapojen toimivuutta käytännössä (Tammineedi 2010, 44). Tarkastuksissa keskitytään yleensä arvioimaan sitä, kuinka hyvin yritys tai sen tietyt järjestelmät noudattavat annettuja – esimerkiksi lakien määrittämiä – kriteerejä tai vaatimuksia. Koulutus ja testaus liittyvät vahvasti toisiinsa, koska esimerkiksi testaamisessa henkilöstöä myös koulutetaan väistämättä (Snedaker 2007, 381, 384). Riskien ehkäisystrategioiden ja toipumissuunnitelmien toimivuutta sekä koko jatkuvuussuunnitelmaa tulee testata ja tarkastaa riittävän usein ja kattavasti, jotta voidaan varmistua niiden ajantasaisuudesta (Snedaker 2007, 403-404; Gibb & Buchanan 2006, 137).

Jatkuvuussuunnitelman koulutus ja testaus vaativat aikaa, vaivaa ja rahaa, joten niiden toteuttaminen edellyttää vahvaa johdon tukea. Resurssien käyttöä ja koulutuksen tarvetta on helpompi perustella, mikäli sen tulokset sidotaan koko liiketoiminnan tavoitteisiin. Eri testaustavat vaativat vaihtelevasti resursseja, mutta vaihtelevia ovat myös niistä saatavat hyödyt. Halvin ja yksinkertaisin tapa toteuttaa suunnitelman testaus on

käydä se läpi ainoastaan paperilla, jolloin moni odottamaton asia saattaa jäädä huomaamatta (Snedaker 2007, 369-373; Gibb & Buchanan 2006, 137). Enemmän resursseja vaativia testausmuotoja ovat toiminnalliset testit, kenttäkokeet sekä kokonaisvaltainen häiriökoe, joissa suunnitelman toimivuutta testataan simulaatioilla joko yksittäisen toiminnon tai koko liiketoiminnan tasolla. Näiden kokeiden tulokset ovat melko realistisia ja monipuolisia, mutta niiden kustannukset ja yritykselle aiheuttamat häiriöt voivat joissakin tapauksissa olla hyötyjä suuremmat. (Snedaker 2007, 373-375, 384-385)

2.2.7 Suunnitelman ylläpito

Liiketoiminnalle on ominaista jatkuva muutos, jonka voivat aiheuttaa esimerkiksi muutokset teknologiassa, tietojärjestelmissä, strategiassa, lainsäädännössä tai organisaatiorakenteessa. Ne synnyttävät uusia riskejä ja asettavat vaatimuksia. Tähän kehitykseen yritysten tulee sopeutua ja se heijastuu myös niiden jatkuvuudenhallintaan. (Snedaker 2007, 403; Gibb & Buchanan 2006, 139). Jatkuvuussuunnitelma on luotu tietyllä ajanhetkellä vallinneen tilanteen ja saatavilla olleen informaation perusteella. Tilanteiden ja tietojen muuttuessa tulee siis myös jatkuvuus- ja toipumissuunnitelmien muuttua. Suunnitelmien ylläpidolla varmistetaan jatkuvuudenhallinnan kyvykkyys, tehokkuus ja ajantasaisuus. Se saavutetaan valvomalla muutoksia, arvioimalla niiden vaikutuksia suunnitelmiin sekä toteuttamalla tarvittavat ja taloudellisesti kannattavat sopeutustoimet. (Tammineedi 2010, 44).

Jatkuvuussuunnitelman ylläpidossa on oleellista myös dokumentointi ja sen hallinta. Kaikki tehdyt muutokset sekä itse ylläpitoa koskevat toimenpiteet tulee kirjata, jotta suunnitelma pysyisi ajan tasalla, eikä aiheuttaisi ylimääräisiä riskejä vanhentuneen tiedon kautta. Jatkuvuussuunnitelmien versiot tulee merkitä ja vanhat versiot korvata uusimmilla, jotta häiriön sattuessa kaikki asianosaiset toimivat samojen ohjeiden mukaisesti. Päivitykset tulee tehdä myös varmuuskopioihin, joita säilytetään eri paikassa kuin varsinaisia suunnitelmia (Snedaker 2007, 400-401). Ylläpidonkin perusperiaatteet tulee olla kirjattuna jatkuvuussuunnitelmaan (Tammineedi 2010, 44).

2.3 Hyödyt

Yritykset, jotka toteuttavat aikaa ja rahaa vaativaa jatkuvuudenhallintaa, tuskin tekisivät niin, elleivät ne kokisi sillä olevan jotakin merkitystä ja hyötyä heidän liiketoiminnalleen. Joillekin organisaatioille se voi olla jopa lakisääteinen toimintaedellytys, mutta yleisesti ottaen jatkuvuudenhallinnasta voidaan löytää monia liiketoimintaa konkreettisesti hyödyttäviä asioita. (Laaksonen ym. 2006, 229; Devargas 1999, 39-40)

Suurin peruste jatkuvuudenhallinnalle on se, että huolellisella uhka-analyysillä ja riskejä ehkäisevällä toiminnalla voidaan vähentää liiketoiminnalle haitallisten tapahtumien vaikutuksia. Sillä siis suojellaan yrityksen arvoa ja saavutettuja kilpailuetuja. Lyhyetkin toimintakatkokset voivat aiheuttaa suuria tappioita tai tulonmenetyksiä. Jatkuvuuteen pyrkiminen voi vähentää näiden katkosten esiintymistiheyttä ja toipumissuunnitelma niiden kestoa. Kilpailijoita tehokkaampi häiriöistä toipuminen ei ainoastaan vähennä yrityksen tappioita, vaan auttaa toisaalta saavuttamaan myös suurempia voittoja ja on siten kilpailuetu. Näin jatkuvuudenhallinta tekee itsestään taloudellisesti kannattavan. (Seow 2008, 204; Laaksonen ym. 2006, 229; Herbane ym. 2004, 437; McManus & Carr 2000, 28)

Suoranaisten taloudellisten vaikutuksen lisäksi jatkuvuudenhallinnalla voidaan estää luottamuksen ja siten asiakkaiden ja toimittajien menettäminen. Yrityksen joutuessa ongelmiin, eivät yhteistyökumppanit useinkaan automaattisesti katoa, vaan paljon riippuu siitä, miten ongelmat hoidetaan. Jos kilpailijatkin painivat samojen ongelmien kanssa, on jatkuvuussuunnitelman tehneillä yrityksillä hyvä tilaisuus kasvattaa asiakaskuntaansa ja parantaa luottamusta sidosryhmiensä keskuudessa. (Devargas 1999, 40)

Muita häiriöiden takia katoavia varoja voivat olla tärkeät tiedot, toimintatavat ja prosessit. Varsinkin tietoteknologian ja -järjestelmien riskit liittyvät usein tietojen saatavuuteen, eheyteen tai tietoturvaan. Ne taas ovat monen yrityksen toiminnan kannalta korvaamattoman tärkeitä (Green & Mark 2009; Devargas 1999, 40). Kaatuneet kotisivut eivät hyödytä ketään, kadonneet asiakastiedot tekevät tilausten toimittamisesta mahdotonta ja heikoksi todettu tietoturva karkottaa niin nykyiset kuin potentiaalisetkin asiakkaat.

Kriisitilanteessa yritykselle aiheutuneita vahinkoja voidaan siis välttää hyvällä jatkuvuudenhallinnalla. Kuitenkin varsinainen syy siihen, että toipumissuunnitelmat poistavat näitä haittoja on se, että niiden avulla vähennetään kriisitilanteissa tehtävää päätöksentekoa. Kun vakava häiriötilanne on jo käynnissä, ratkaisut tehdään usein liian hitaasti tai puutteelliseen tietoon pohjautuen, jolloin riski sille, että kestämätöntä vahinkoa aiheutuu, kasvaa merkittävästi. Jatkuvuudenhallintaan kuuluu uhkien ja haavoittuvuuksien analysointi, jolloin toimintaohjeet tulisi kyetä laatimaan etukäteen kaikkien kriisitilanteiden osalta. (Laaksonen ym. 2006, 234)

Yleensä jatkuvuudenhallinta koetaan kuitenkin tärkeäksi siksi, että asiakkaat ja toimittajat edellyttävät sitä. Epävarmuustekijöitä hallitsemalla yritys voi laskea riskisyyttään sidosryhmien näkökulmasta, mikä mahdollistaa esimerkiksi uusien sopimusten syntymisen ja entisten jatkumisen. Lisäksi se antaa sijoittajille ja ulkopuolisille yleisesti positiivisen kuvan yrityksestä. Jotkut sopimuskumppanit saattavat suoranaisesti vaatia jatkuvuudenhallintaa, mutta useammin se on epäsuora edellytys sille, että sopimusehdot – kuten toimitusvaatimukset – täyttyvät. (McLoughlin 2008, 106; Laaksonen ym. 2006, 229)

Toteuttamalla määrätietoista jatkuvuudenhallintaa yritys saattaa voida vaikuttaa enemmän sopimusehtoihinsa. Tämä tulee erityisesti esiin vakuutussopimuksissa, jotka on kenties mahdollista saada neuvoteltua edullisemmiksi, kun riskien toteutuminen pyritään ennaltaehkäisemään (Devargas 1999, 40). Vakuutuskustannusten pienentäminen ei kuitenkaan yleensä ole jatkuvuudenhallinnan varsinainen päämäärä, vaan sen sivutuote, jolla kuitenkin voi olla merkitystä perusteltaessa jatkuvuudenhallinnan olemassaoloa yritysjohdolle.

Erilaisten hyötyjen tiedostaminen on tärkeää, sillä strategisesti suuntautuneella jatkuvuudenhallinnalla on aina selvät tavoitteet. Sillä pyritään esimerkiksi saavuttamaan kilpailijoita parempi joustokyky tai toipumisnopeus. Pitkän tähtäimen jatkuvuudenhallintaan ei ryhdytä, ellei sen todellisia hyötyjä tunneta. Havaitut hyödyt ovat merkittäviä johdon asenteiden muokkaajia, sillä jatkuvuudenhallinta aiheuttaa myös kustannuksia (Seow 2009, 202-205). Johdon asenne taas ratkaisee pitkälti sen, minkälaisessa roolissa jatkuvuudenhallinta yrityksessä on. Havaituilla hyödyillä on siis vaikutusta tämän tutkimuksen tuloksiin.

2.4 Kustannukset

Jatkuvuudenhallinta aiheuttaa aina kustannuksia, jotka voivat olla niin välittömiä kuin välillisiäkin. Mitä matalampaa riskitasoa yritys haluaa ylläpitää, sitä suuremmaksi muodostuvat kustannukset (Hecht 2002, 448-449). Välittömiä kustannuksia syntyy erityisesti aloitus- ja toimeenpanovaiheessa. Tällöin toiminta edellyttää tiheää arviointia, suunnittelua, koulutusta, tiedotusta, valvontaa ja ylläpitoa. Riskeiltä suojautuminen edellyttää usein tietoteknisiä ratkaisuja, joten investointeja tarvitaan esimerkiksi palomuureihin ja varajärjestelmien luomiseen. Jatkuvuussuunnitelman mukaisten toimintatapojen tunteminen ja etenkin omaksuminen edellyttää paljon vuorovaikutusta ja vie aikaa. (Devargas 1999, 40)

Välillisten kustannusten suuruutta on usein haastavaa arvioida. Jatkuvuudenhallinta voi saada aikaan monia sellaisia välillisiä kustannuksia, joita ei alun perin ymmärretty ottaa edes huomioon. Esimerkki välillisistä kustannuksista on uusien toimintatapojen tai niiden hitaan omaksumisen aikaansaama työn tuottavuuden lasku. Kun vanha tuttu ohjelmisto vaatiikin yhtäkkiä käyttäjätunnuksen ja salasanan, hidastuu toiminta väistämättä. (Devargas 1999, 40)

Oleellista kustannuksissa on se, että ne eivät saa olla suuremmat kuin saavutettavat liiketoimintahyödyt. Tämän varmistamiseksi jatkuvuussuunnitteluun sisältyy kustannushyötyanalyysi, jolla arvioidaan mahdollisimman tarkasti niin jatkuvuudenhallinnan aiheuttamat kustannukset kuin sen tuomat edutkin. Tämän analyysin tekeminen ei ole aivan yksinkertainen projekti, koska esimerkiksi välilliset kustannukset eivät ole aina

suoraan muutettavissa rahaksi. Toisaalta jatkuvuudesta saatavat hyödyt voi olla hankala kohdistaa tiettyihin prosesseihin tai henkilöihin. (Devargas 1999, 40)

Kustannus-hyötyanalyysissä tunnistetaan yrityksen uhat ja haavoittuvuudet sekä suojakeinot, joita voi olla yhdelle riskille yksi tai useampia. Analyysi tulee tehdä erikseen jokaiselle riskille ja sen suojakeinolle. Erityisesti pitäisi pystyä arvioimaan yksittäisen suojatoimenpiteen kustannustehokkuus. Se selviää vertailemalla kustannuksia sekä sitä, paljonko toimenpide alentaa riskin tasoa tai pienentää sen toteutumisen aiheuttamia seurauksia. Näin kyetään arvioimaan riskiltä suojautumisen kannattavuus ja yritysjohto voi esimerkiksi päättää kantaa riskiä tietoisesti. (Gibb & Buchanan 2006, Devargas 1999, 40)

Jatkuvuudenhallinnan aiheuttamien kustannusten arvioiminen on hyötyjen tavoin tärkeää, sillä saadun informaation perusteella organisaatio kykenee perustelemaan jatkuvuuspyrkimystensä kannattavuuden. Tämä vaikuttaa erityisesti johdon asenteisiin ja jatkuvuudenhallinnan rooliin yrityksessä ja on siten tärkeää tutkimuskysymysten kannalta.

2.5 Standardit ja lainsäädäntö

Standardien tarkoituksena on antaa yrityksen sisäisille ja ulkoisille sidosryhmille varmuus siitä, että kyseinen organisaatio toimii yleisesti hyvinä ja oikeina pidettyjen toimintatapojen mukaisesti. Jatkuvuudenhallintastandardit auttavat yritystä ymmärtämään ja analysoimaan omia prosessejaan sekä parantamaan liiketoimintansa jatkuvuutta (Tammineedi 2010, 37).

Jatkuvuudenhallinnan yhdenmukaistamiseksi ja tehostamiseksi on luotu useita eri standardeja, joista tunnetuin lienee British Standards Instituten julkaisema BS25999. Se on sertifioitavissa oleva standardi, joka on saanut paljon suosiota Euroopassa, mutta kasvavassa määrin myös maailmanlaajuisesti (McLoughlin 2008, 105; Gallagher 2007, 34-35). Muita jatkuvuudenhallinnan standardeja ovat esimerkiksi BS 25777:2008 tieto- ja viestintäteknologian jatkuvuudenhallinnalle sekä ISO 22399:2007 häiriövalmiudelle ja operatiiviselle jatkuvuudenhallinnalle (ISO 2010).

Edellä mainitut jatkuvuudenhallintastandardit pyrkivät kehittämään yrityksen riskienhallintaa ja kykyä toipua häiriötilanteista. Niiden lisäksi on olemassa muitakin yrityksen jatkuvuutta edistäviä standardeja. Esimerkiksi IT on nykyisin elintärkeä toiminto, joten tietoturvastandardien noudattaminen ehkäisee samalla myös tietoturvaongelmien esiintymistä. Tunnetuin tietoturvaa koskeva standardisarja on ISO/IEC 27000, joka kokoaa yhteen yleisiä tietoturvakäytäntöjä ja ohjeistaa yritystä hallitsemaan tietoturvaa koko organisaation laajuudella. (ISO 2010; Laaksonen ym. 2006, 86-89)

Standardien sertifiointi vaatii resursseja, joiden saaminen taas edellyttää johdon tukea. Sertifikaatin saatuaankin yrityksen tulee panostaa jatkuvuudenhallintaan, jotta saavutettu taso voidaan ylläpitää ja sertifikaatti säilyttää. Sertifioinnin hyödyt tuleekin kyetä perustelemaan hyvin. Yleisimmin sen avulla pyritään saavuttamaan asiakkaiden ja toimittajien luottamusta sekä kilpailuetua. Yrityksen voi olla helpompi saada uusia asiakkaita ja säilyttää vanhoja sopimuksia luotettavalla imagolla. Lisäksi sertifikaatti voi olla asiakkaan ostopäätökseen vaikuttava tekijä vertailtaessa kilpailevia yrityksiä. (McLoughlin 2008, 106)

On yleistä, että standardeista poimitaan ainoastaan parhaat palat, eli niistä valikoidaan tiettyjä toimintatapoja tai ohjeita, joiden katsotaan soveltuvan omaan yritykseen. Jotkut organisaatiot saattavat noudattaa standardeja täysimääräisestikin, mutta eivät näe saavansa lisäarvoa hintavasta sertifikaatista. Näin voidaan kehittää organisaation toimintaa, mutta virallista, yrityksen toimintatavoista ja laadusta kertovaa merkintää ei ole. Halutessaan kuitenkin parantaa jatkuvuudenhallintapanostustensa arvoa, yritys voi esimerkiksi palkata riippumattoman ulkopuolisen tahon tekemään arvioinnin ja julkistaa sen tulokset. (McLoughlin 2008, 106)

Tietyillä aloilla jatkuvuuden suunnittelu on tehty pakolliseksi, koska sen yrityksillä on suuri vaikutus yhteiskunnan toimintaan. Tällaisia ovat vaikkapa pankit, energia- ja vesilaitokset sekä perusterveyspalveluiden tuottajat. Työ- ja elinkeinoministeriön alainen Huoltovarmuuskeskus huolehtii siitä, että yhteiskunnan taloudelliset perustoiminnot voidaan ylläpitää tilanteessa kuin tilanteessa. Se solmii yritysten kanssa sopimuksia, joilla ne sitoutuvat jatkuvuudenhallintaan. Myös Finanssivalvonnan alaisten yritysten tulee riskienhallintavaatimusten perusteella toteuttaa jatkuvuudenhallintaa ja sen laatua valvotaan. (Huoltovarmuuskeskus 2010; Laaksonen ym. 2006, 229; Sidosryhmäturvallisuus puolustusvoimissa, 2005)

Suomessa on tavallista, että vähääkään suuremmat yritykset luovat pelastussuunnitelman. Suunnitelman tarkoituksena on ehkäistä vaaratilanteiden syntymistä ja suojata henkilöstöä ja omaisuutta onnettomuuksien sattuessa. Sen yleisyys johtuu siitä, että pelastuslaki sekä valtioneuvoston asetus pelastustoimesta edellyttävät pelastussuunnitelmaa kaikilta tietyn kokoisilta rakennuksilta ja tietyn tyyppisiltä liiketoimilta. Esimerkiksi rakennuksella, jossa työskentelee samanaikaisesti vähintään 30 henkeä, tulee olla pelastussuunnitelma. Myös esim. sairaalat, yli 10 majoituspaikan hotellit, yli 500 neliömetrin myymälät sekä yli 50 asiakaspaikan ravintolat joutuvat laatimaan suunnitelman (Finlex 2011a; Finlex 2011b). Kynnys suunnitelman laatimiselle ylittyy siis käytännössä kaikissa suurissa yrityksissä.

Ulkomaisista lainsäädännöistä esimerkiksi USA:n Sarbanes-Oxley sekä terveydenhuollon Health Insurance Portability and Accountability Act (HIPAA) huomioivat jatkuvuudenhallinnan erityisesti tietoturvan osalta. Niissä määritellään vaatimuksia esimerkiksi henkilötietojen suojaukselle sekä jatkuvalle sisäiselle valvonnalle, jolla pyri-

tään havaitsemaan tietoturvauhkia. (Chung, Chung & Joo 2006, 53; Green & Mark 2006, 32) Yritysjohto voidaan saattaa lailliseen vastuuseen, mikäli organisaation vahingot johtuvat heidän huolimattomuudestaan. Niinpä jatkuvuudenhallinta on yksi johdon tapa suojautua laillisilta seuraamuksilta (McManus & Carr 2000, 28).

Standardit ja lainsäädännöt ovat tärkeitä tämän tutkimuksen kannalta, sillä niiden kautta voidaan tehdä päätelmiä jatkuvuudenhallinnan roolista. Jokainen organisaatio voi noudattaa jatkuvuudenhallintaan liittyvää lainsäädäntöä rimaa hipoen tai vaihtoehtoisesti päättää kehittää sitä pidemmälle tehden siitä kenties strategisen kilpailukeinon. Sama pätee jatkuvuudenhallintastandardeihinkin, sillä yritysten ei ole pakko noudattaa tai sertifioida niitä. Jatkuvuudella on selvästi erityinen asema niille organisaatioille, jotka toimivat standardien mukaan (Herbane ym. 2004, 441). Standardien ja lainsäädännön noudattamisaste on siis oleellista päätutkimusongelman kannalta.

2.6 Tietoturva jatkuvuudenhallinnassa

Informaatioteknologian tärkeys liiketoiminnalle on jatkuvasti kasvava ja sen myötä tietoturva on muodostunut tärkeäksi tekijäksi yrityksen jatkuvuudelle. Monet organisaatiot ovat suoraan yhteydessä toistensa tietoverkkoihin, yksityisiä henkilötietoja tallennetaan erilaisiin tietojärjestelmiin ja pankkiasioita voidaan hoitaa Internetin kautta. Lähes joka kolmas vähintään kymmenen henkeä työllistävä suomalainen yritys kertoo kuitenkin kokeneensa ongelmia tietoturvan kanssa (Tilastokeskus 2010, 44). Mikäli tietoturva pettää tai se jätetään vaille riittävää huomiota, voi seurauksena olla mm. menetettyjä asiakkaita ja työtunteja, kolhiintunut imago tai kadonneita tietokantoja ja yrityssalaisuuksia. Seuraukset johtavat lähes aina myös menetettyihin euroihin tai laillisiin seuraamuksiin. Pahimmassa tapauksessa katkolla voi olla koko liiketoiminnan tulevaisuus. Tietoturvan tehtävänä on rakentaa muuri suojattavan tiedon ja ympäröivän maailman välille ja estää tiedon saatavuuden, luottamuksellisuuden tai eheyden ongelmista johtuvia kriisejä (Laaksonen ym. 2006, 17, 19). Edellä mainitut ongelmat ovat nykyisin hyvin yleisiä, joten tietoturvan voidaan todeta olevan merkittävä osa yritysten jatkuvuudenhallintaa. Tietoturvasta voidaan siis mahdollisesti tehdä päätelmiä päätutkimuskysymykseen, eli jatkuvuudenhallinnan rooliin liittyen, joten sitä käsitellään tarkemmin IT:n joustavuuden ja toipumiskyvyn selvittämiseksi ja mahdollisten hyvien käytäntöjen löytämiseksi.

2.6.1 Mitä on tietoturva?

Tietoturva on tiedon luottamuksellisuuden (*confidentiality*), eheyden (*integrity*) ja saatavuuden (*availability*) turvaamista. Se varmistaa, ettei yritykselle tärkeää tietoa kyetä luvatta käyttämään, muokkaamaan tai tuhoamaan. Tietoturva pyrkii suojaamaan yrityksen kaikkea suojaamisen arvoista tietoa – niin digitaalista kuin paperimuotoistakin (Laaksonen ym. 2006, 17). Sen perimmäisenä tehtävänä on turvata yritystoiminnan jatkuvuus sekä minimoida tietoturvaongelmien esiintyminen ja niiden mahdolliset vaikutukset liiketoiminnalle (von Solms 1998b, 224).

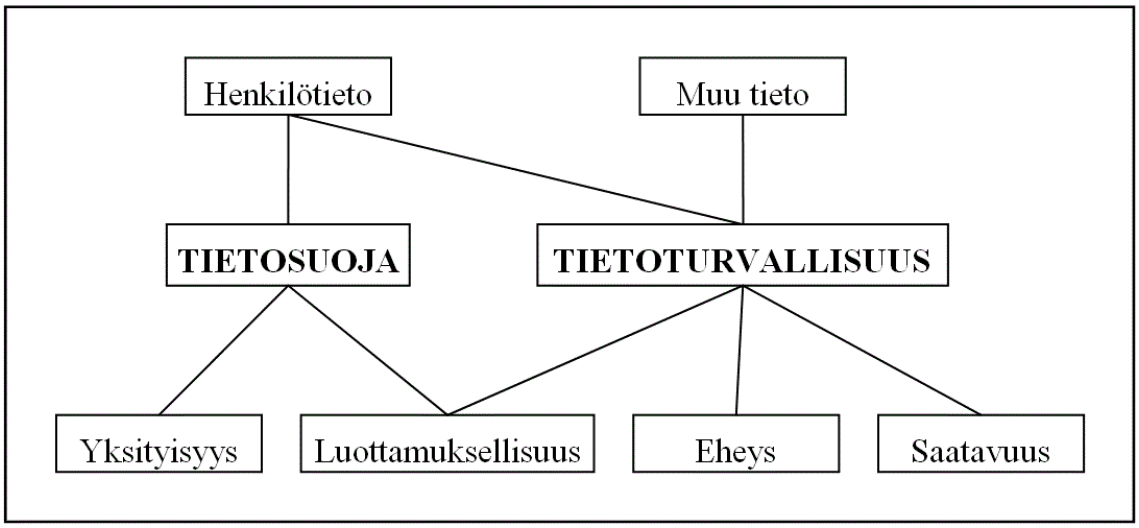
Valtionhallinnon tietoturvakäsitteistön (2003, 51) mukaan tietoturvallisuus on ”tavoitetila, jossa tiedot, tietojärjestelmät ja palvelut saavat asianmukaista suojaa niin, että niiden luottamuksellisuuteen, eheyteen ja saatavuuteen kohdistuvat uhat eivät aiheuta merkittävää vahinkoa yhteiskunnalle ja sen jäsenille”. Tietoturvallisuuden katsotaan kattavan myös kaikki ne toimenpiteet, lainsäädännöt ja normit, joilla edellä kuvattu tavoitetila pyritään saavuttamaan ja ylläpitämään. (Valtionhallinnon tietoturvakäsitteistö, 2003, 51)

Tiedon luottamuksellisuudella tarkoitetaan sitä, että tietoon pääsevät käsiksi vain ne, joilla on siihen syy ja oikeus sekä sitä, etteivät suojatut tiedot paljastu. Eheydellä viitataan tiedon oikeellisuuteen, tarkkuuteen ja oikeanmuotoisuuteen sekä siihen, että dataa voivat muokata ainoastaan siihen oikeutetut henkilöt ja järjestelmät. Saatavuus taas asettaa vaatimuksia sille, että tiedot ovat tarvittaessa käyttäjien saatavilla tietyn ajan kuluessa, oikeassa muodossa. (Pfleeger & Pfleeger 2003, 9-12)

Tietoturva ilmenee yrityksen toimintatapoina, teknisinä ratkaisuina sekä hallinnollisina toimina. Tietoturvainvestointeja tulisi tehdä nimenomaan hallinnolliselle puolelle, kuten koulutuksiin, koska ihmiset ovat loppujen lopuksi tietoturvan tärkein voimavara. He ovat niitä, jotka tietoa tuottavat ja käsittelevät. Tietoturvallisuus edellyttää teknisen kehityksen ohella siis myös sitä tukevia toiminnallisia muutoksia. Kaikkien työntekijöiden tulisi tuntea yrityksen tietoturvaperiaatteet ja syyt niiden noudattamiseen, jolloin niiden toteuttaminen ei tunnu pakolliselta. Parhaimmillaan tietoturvasta muodostuu organisaatiokulttuuri, jolloin kaikki työntekijät käsittävät sen merkityksen ja pyrkivät ylläpitämään sitä. Tämä voi muodostua jopa kilpailueduksi esimerkiksi organisaation parempana jatkuvuutena. (Laaksonen ym. 2006, 17-20; von Solms 1998a, 175)

Tietoturva ei ole samankaltaisesta ulkoasustaan huolimatta synonyymi tietosuojalle. Tietosuojalla tarkoitetaan yksityishenkilön henkilötietojen käsittelyä koskevaa yksityiselämän suojaa ja sitä turvaavia oikeuksia (Valtionhallinnon tietoturvakäsitteistö 2003, 50). Se varjelee luonnollisen henkilön oikeutta määrätä itseensä liittyvän, yksityisen tiedon tallentamisesta ja asettaa vaatimuksia näiden tietojen säilyttämiselle. Erityisesti terveydenhuoltoalan yritykset joutuvat usein pohtimaan tietosuojakysymyksiä ja siksi niillä onkin usein oma tietosuojavaltuutettunsa. Tietoturva taas keskittyy kaikentyyppis-

ten tietojen luottamuksellisuuden, eheyden ja käytettävyyden ylläpitämiseen kehittämällä toimintatapoja ja teknisiä ratkaisuja (Laaksonen ym. 2006, 17). Kuvio 4 havainnollistaa tietosuojan ja tietoturvallisuuden välistä suhdetta. Käsitteet ovat siis sikäli päällekkäisiä, että molemmat pyrkivät suojaamaan tiedon luottamuksellisuutta.



Kuvio 4 Tietosuoja ja tietoturvallisuus (Valtionhallinnon tietoturvakäsitteistö 2003)

Tietoturvallisuus on nykypäivän yrityksille jo lähes itsestäänselvyys, jota vaaditaan, jotta yhteistyö muiden yritysten kanssa olisi ylipäätään mahdollista. Von Solms (1998a, 175) toteaa, että mikäli muut katsovat yrityksen tietoturvan olevan kunnossa, se on tervetullut yhteiseen toimintaan. Jos näin ei kuitenkaan ole, se jätetään oman onnensa nojaan. Investointeja ja aikaa vaatinut, kattava ja tehokas tietoturva on käytännössä hyödytön, mikäli kumppaniorganisaation tietoturva on paljon huonommalla tasolla. Näin ollen tietoturva on merkittävä normaalin liiketoiminnan edellytys, jonka ongelmat heijastuvat koko yritykseen. Aiemmin, keskustietokoneiden aikakaudella, tietoturvaa pidettiin ainoastaan yrityksen sisäisenä asiana, mutta nykyään tietoturva-asioita pohdittaessa tulee huomioida myös yrityksen sidosryhmät ja esimerkiksi tarkastaa heidän tietoturvansa taso säännöllisesti. (von Solms 1998a, 175)

2.6.2 Tietoturvariskien hallinta

Jatkuvuudenhallinta pyrkii ehkäisemään häiriöitä ennalta ja mahdollistamaan yrityksen nopean toipumisen. Näiden tavoitteiden saavuttaminen edellyttää tietoturvariskien kartoittamista ja niiden ehkäisemistä. Tietoturvan osalta tulee perinteisten riskienhallinnan periaatteiden mukaisesti kartoittaa uhat, haavoittuvuudet ja suojatoimenpiteet.

Tietoturvan näkökulmasta uhka on mikä tahansa voima, joka voi vaikuttaa haitallisesti vähintään yhteen kolmesta tietoturvan tavoitteesta: eheyteen, saatavuuteen tai luottamuksellisuuteen. Tällaisia voivat olla esimerkiksi tietomurrot ja järjestelmien kaatumiset. Tietoturvan epäonnistuessa vaikutukset ulottuvat yleensä laajalle koko yrityksessä. Seurauksena voi olla esimerkiksi toimintakatkoksia tai imagokatastrofeja. (Rittinghouse & Ransom 2006, 59-61)

Whitman (2003) erottelee kattavassa tutkimuksessaan kaksitoista erilaista tietoturvauhkakategoriaa, joihin tavallisimmat tietoturvaongelmat voidaan jakaa. Uhkien jaottelu perustuu aikaisempiin julkaisuihin sekä kolmeen tietoturvapäällikön haastatteluun. Tutkimus selvittää Suomen mittakaavassa suurten ja keskisuurten yritysten mielipiteitä siitä, mitkä uhkatekijöistä ovat vaarallisimpia tietoturvan kannalta. Vastaajina toimivat pääasiassa tietojärjestelmä- ja tietohallintojohtajat.

Tietoturvauhat merkittävimpänä pidetystä vähiten merkittävään (Whitman 2003, 92):

- ohjelmistohyökkäys (esim. virus, mato tai makro)
- tekniset ohjelmistoviat (esim. koodivirhe)
- inhimilliset virheet tai laiminlyönnit
- vakoilu tai tunkeutuminen (esim. luvaton käyttö tai tiedonkeruu)
- sabotaasi tai vandalismi (esim. järjestelmien tai tiedon tuhoaminen)
- tekniset laitteistoviat
- varkaus (esim. laiton tiedon tai laitteiston hankkiminen)
- luonnonvoimat (esim. tulipalo, tulva tai maanjäristys)
- tekijänoikeuksien vaarantuminen (esim. piratismi)
- palveluntoimittajien poikkeaminen sovitusta (esim. sähkö- ja tietoliikenneasiat)
- teknologian vanhentuminen (esim. antiikkinen tai päivittämätön teknologia)
- tiedolla kiristäminen (esim. tiedon paljastamisella kiristäminen).

Tutkimustulosten mukaan selvästi merkittävimpänä tietoturvauhkana pidetään ohjelmistohyökkäystä, johon kuuluvat esimerkiksi virukset ja madot. Niitä pidettiin lähes kaksi kertaa niin merkittävänä vaarana kuin toiseksi tullutta teknisten ohjelmistovikojen uhkaa. Kolmanneksi pahimmaksi uhaksi koetaan inhimilliset virheet sekä laiminlyönnit. Neljännellä ja viidennellä sijalla ovat tietomurtoihin eli hakkerointiin liittyvät uhat, kuten tiedon luvaton käyttö tai tuhoaminen. Vähiten huolestusta yrityksissä aiheuttaa tiedolla kiristäminen, jonka aiheuttama uhka on vain kymmenesosa ohjelmistohyökkäyksien vastaavasta. (Whitman 2003, 92-93)

Waden (2004) mukaan tietoturvan suurin heikkous on ihminen. Samansuuntaiseen lopputulokseen päätyvät myös Kraemer, Carayon ja Clem (2009), jotka tutkivat inhimillisten ja organisationaalisten tekijöiden sekä tieturvaheikkouksien välistä suhdetta. Yrityksen tiedot päätyvät alttiiksi hyökkäyksille ja tietomurroille yleensä työntekijöiden

toiminnan seurauksena. Henkilökuntaan kuuluvat kykenevät luomaan helposti oivallisen kasvualustan tietoturvaongelmille esimerkiksi käyttämällä yksinkertaisia salasanoja tai availemalla epämääräisiä sähköpostien liitetiedostoja. Heidän tarkoituksensa ei useinkaan ole edesauttaa tietoturvauhkien toteutumista, mutta se tapahtuu tietämättömyyden, osaamattomuuden, välinpitämättömyyden tai hyväuskoisuuden seurauksena. Työntekijä voi esimerkiksi paljastaa tietoja tuntemattomalle kyselijälle, koska hän ei yksinkertaisesti tiedä kyseisten tietojen olevan salaisia. (Sumner 2009, 11; Wade 2004, 33)

Ihmisten tietämättömyys, osaamattomuus tai välinpitämättömyys johtuu usein yrityksen epäonnistuneista tai kokonaan puuttuvista tietoturvaperiaatteista. Tietoturvan tärkeydestä ja sen syistä ei ehkä viestitetä tarpeeksi tai oikealla tavalla. Muita tietoturvan haavoittuvuuksia ovat esimerkiksi ohjelmistovirheet, huono verkkoinfrastruktuuri, vanhentunut tai puutteellinen teknologia, toimittajariippuvuus ja olematon kulunvalvonta (Whitman 2003, 93). Myös jokaisella ohjelmistolla ja laitteistolla on omat heikkoutensa, joita hyväksikäyttämällä rikolliset ja vahingontekijät voivat aiheuttaa vakavia haittoja yritykselle (Keller, Powell, Horstmann, Predmore & Crawford 2005, 8).

Yrityksen tunnistettua omat tietoturvauhkansa ja heikot kohtansa sen tulee kehittää ratkaisut riskien ehkäisemiseksi ja vaikutusten minimoimiseksi. Tietoturvauhkien suuresta lukumäärästä johtuen myös niiden ehkäisykeinoja on lukemattomasti. Selvästi yleisimmät tavat suojata arkaa tietoa ovat Whitmanin (2003, 93) tutkimuksen mukaan salasanojen käyttö, varmuuskopiointi, virusohjelmistojen käyttö sekä henkilöstön koulutus. Salasanasuojaus löytyi kaikista kyseiseen tutkimukseen osallistuneista organisaatioista. Varmuuskopiointi ja virusohjelmisto olivat käytössä lähes 98 prosentissa yrityksistä. Muita yleisiä tiedon suojauskeinoja ovat palomuurit, Virtual Private Networkit (VPN), salaukset, yhtenäiset tietoturvaperiaatteet, paloturvallisuudesta huolehtiminen, kulunvalvonta, tarkastukset sekä valvonta. (Rittinghouse & Ransom 2006, 100-107; Keller ym. 2005, 13-14; Whitman 2003, 93)

Von Solms (1998a, 175) toteaa, että turvallinen IT-ympäristö tarvitsee teknisen puolen seuraksi tietoturvaperiaatteita ja -ohjeita sekä harkittua johtamista. Koko tietoturvaprosessin tulee olla kunnossa, jotta tieto pysyisi suojattuna. Hyvä esimerkki ihmisen ja teknologian toisiaan täydentävästä suhteesta on se, ettei paksuinkaan ovi suojaa murtautumiselta, ellei ihminen ole sitä ensin lukinnut. Turvallisinkaan tekniikka ei siis ole tehokas, ellei sitä käytetä oikein (von Solms 1998a, 177). Tietoturvalle asetettujen tavoitteiden saavuttamiseksi jatkuvuussuunnittelussa tulee pohtia keinoja, joilla ihmisten aiheuttamia tietoturvariskejä, kuten vääriä toimintatapoja, voidaan ehkäistä ja toisaalta myös sitä, kuinka tietoturvaa voidaan ihmisten toiminnan avulla parantaa. Vaihtoehtoja voivat olla esimerkiksi tietoturvaperiaatteet, koulutus, valvonta sekä kannustinjärjestelmät. Niiden ohella tarvitaan kuitenkin aina teknistä tietoturvaa, koska tietoturvarikko-

muksia – joko tahattomia tai tahallisia – tulee tapahtumaan joka tapauksessa. (Wade 2004, 36)

2.7 Strateginen jatkuvuudenhallinta

Strateginen johtaminen tarkoittaa yleisesti ottaen huolehtimista siitä, että yritys säilyttää arvonsa ja saavuttaa pitkän tähtäimen tavoitteensa. Se sisältää analysointia, suunnittelua ja suunnitelmien toimeenpanoa. Jatkuvuudenhallinta tulisi liittää osaksi pitkän tähtäimen suunnittelua, koska se auttaa organisaatiota ymmärtämään paremmin itseään ja nostaa esiin asioita, joiden avulla kilpailuetujen sekä pitkän aikavälin tavoitteiden saavuttaminen on mahdollista. (Wong 2009, 63)

Strategisen johtamisprosessin on havaittu sisältävän kolme perusosaa: suunnittelun, toteutuksen ja valvonnan (Preble 1997, 770-772). Strateginen jatkuvuudenhallinta sisältää kaikki nämä vaiheet ja kattaa organisaation kaikki toiminnot. Suunnittelu alkaa pitkän aikavälin tavoitteiden määrittelyllä ja jatkuu riski- ja vaikutusanalyyseillä sekä riskien ehkäisystrategioiden valitsemisella. Tehdyt havainnot ja päätökset dokumentoidaan jatkuvuussuunnitelmaan ja suunnitelma toteutetaan tekemällä tarvittavia muutoksia yrityksen prosesseihin ja organisaatiorakenteisiin. Oleellista on myös toiminnan säännöllinen arviointi ja valvonta sekä organisaation kehittäminen kerätyn informaation avulla. (Herbane ym. 2004, 438)

Wongin (2009, 63) mukaan koko yrityksen strategiset tavoitteet tulisi liittää jatkuvuudenhallinnan strategisiin tavoitteisiin, koska se parantaa yrityksen suorituskykyä ja pitkän aikavälin tehokkuutta. Richardson (1994, 63) tukee tätä näkemystä. Hän on todennut häiriöiden olevan tapahtumia, jotka uhkaavat yrityksen strategisten tavoitteiden saavuttamista, joten häiriöitä ehkäisevä jatkuvuudenhallinta vaikuttaa siten samalla myös strategisten tavoitteiden saavuttamiseen.

Strategisen johtamisprosessin vaiheet sisältyvät siis myös strategiseen jatkuvuudenhallintaan, mutta niiden olemassa olo ei kuitenkaan vielä takaa, että jatkuvuudenhallinnan merkitys olisi yritykselle strateginen. Herbanen ym. (2004, 439) mukaan strateginen jatkuvuudenhallinta perustuu liiketoiminnan tarpeisiin ja sen avulla pyritään tuottamaan lisäarvoa ja hyötyä yritykselle. Hyötyä ja lisäarvoa voidaan saavuttaa esimerkiksi kehittämällä ainutlaatuisia toimintatapoja, joiden avulla yritys välttää riskejä kilpailijoita tehokkaammin (Wong 2009, 63). Lisäksi strateginen jatkuvuudenhallinta on luonteeltaan sosioteknistä (*socio-technical*), eli se huomioi sekä suunnittelun että johtamisen – sekä asiat että ihmiset. Teknisten ratkaisujen ohella tulee pohtia esimerkiksi viestintää ja ihmisten kyvykkyyksiä (Herbane ym. 2004, 439).

Strategisen jatkuvuudenhallinnan tarkoitus ei ole ainoastaan luoda yritykselle dokumentoitua toimintaohjetta, joka kaivetaan esiin kriisin sattuessa. Sen tavoitteena on tur-

vata operaatioiden jatkuvuus aktiivisella toiminnalla ja antaa siten vakaa pohja yrityksen kilpailukyvylle. Sen lisäksi, että jatkuvuudenhallinta auttaa säilyttämään saavutettuja etuja, se voi muodostua myös itsessään kilpailueduksi. Kun esimerkiksi saman alan tai saman maantieteellisen alueen yritykset kärsivät samoista ongelmista, voivat jatkuvuudenhallintaa soveltavat yritykset saada toipumisetua, joka tehostaa liiketoiminnan normalisoitumista ja minimoi esimerkiksi yrityskuvalle aiheutunutta haittaa. Jatkuvuudenhallintaa ei tulekaan nähdä vain toiminnallisena, rajattuna prosessina, vaan kyvykkyytenä, joka tukee organisaation kehittymistä. (Herbane ym. 2004, 435, 437)

Strategisen jatkuvuudenhallinnan tulisi siis Herbanen ym. (2004, 439-440) mielestä olla luonteeltaan sosioteknistä, kattaa yhden toiminnon sijasta koko organisaatio ja tuottaa hyötyä ja arvoa pitkällä tähtäimellä. Näiden ominaisuuksien lisäksi Herbane ym. (2004, 439-440) erittelevät tutkimuksessaan neljä tekijää, joiden avulla yrityksen jatkuvuudenhallinnan roolia voidaan arvioida. Nämä tekijät ovat toipumisnopeus (*speed*), joustavuus (*configuration resilience*), pakollisuus (*obligation*) ja sulautuminen (*embeddedness*). Ne helpottavat jatkuvuudenhallinnan roolin tutkimista ja ovat oleellisia tutkimuksen empiriaosuuden kannalta. Tämän vuoksi tekijät käsitellään seuraavaksi yksityiskohtaisemmin.

2.7.1 Toipumisnopeus

Toipumisnopeus on kriittistä jatkuvuudenhallinnassa. Yleisestikin ottaen kyky saavuttaa tavoitteet kilpailijoita nopeammin on yrityselämässä merkittävä strateginen kilpailuetu. Herbane ym. (2004, 440) toteavat, että yritys, joka kykenee toipumaan ongelmista muita nopeammin, ei joudu käännyttämään yhtä paljon uusia asiakkaita, seisottamaan vanhojen asiakkaiden toimituksia tai laskemaan liikearvoaan. Niinpä jatkuvuudenhallinnan on mahdollistettava kilpailijoita tehokkaampi toipuminen kriisitilanteista.

Herbanen ym. (2004, 440) mukaan toipumisnopeus on oikeastaan kyvykkyys, joka on yrityksen valppauden (*alertness*) ja valmiuden (*preparedness*) tulos. Valppaudella tarkoitetaan kykyä havaita häiriöitä ja reagoida niihin nopeasti. Se sisältää esimerkiksi yrityksen raportointijärjestelmät ja kriisitilanteiden organisoinnin, kuten erilaiset kriisienhallintatiimit. Yrityksen valmiudella taas viitataan etukäteen tehtyihin valmisteluihin, joilla pyritään ehkäisemään häiriöiden esiintymistä ja haittavaikutuksia. Niillä tarkoitetaan esimerkiksi suunnitelmien harjoittelua, varatoimitilojen olemassa oloa sekä ylimääräisten resurssien hankkimista. Toipumisnopeus riippuu siis siitä, kuinka nopeasti ongelmat havaitaan, miten tehokkaasti niiden hoitaminen on organisoitu ja kuinka hyvin niihin on valmistauduttu ennalta.

Toipumisnopeudesta on hyötyä aina häiriöiden sattuessa, joten se edistää yrityksen kilpailukyvyn ja arvon säilymistä ja kehittymistä. Hyvään reagointikykyyn tähtäävät

toimintatavat, kuten tietojen varmuuskopiointi, eivät kuitenkaan ainoastaan nopeuta toipumista, vaan saattavat ehkäistä häiriöiden esiintymistä ylipäätään. Näin ollen ne parantavat myös yrityksen joustavuutta. (Herbane ym. 2004, 440)

2.7.2 Joustavuus

Joustavuudella viitataan yrityksen kykyyn mukautua ilmeneviin ongelmiin siten, etteivät ne vaikuta yrityksen toimintakykyyn haitallisesti. Toisin sanoen joustavuus kuvaa yrityksen toimintavarmuutta ja kykyä välttää kriisejä. Sisäinen joustavuus tarkoittaa organisaation kykyä käsitellä sen sisällä tapahtuvia häiriöitä, kuten tietoverkkojen kaatumisia tai avainhenkilöongelmia. Ulkoinen joustavuus taas tarkastelee organisaatiota sen toimintaympäristössä ja arvioi kuinka hyvin yritys selviää, mikäli esimerkiksi avaintoimittajat tai -asiakkaat joutuvat vaikeuksiin. Molemmat joustavuuden näkökulmat on otettava huomioon koko organisaation laajuudella, jotta yrityksen joustavuuden voitaisiin sanoa viittaavan strategiseen jatkuvuudenhallintaan. (Herbane ym. 2004, 441)

Organisaation joustavuutta voidaan parantaa esimerkiksi valitsemalla useita eri tavarantoimittajia samalle tuotteelle, käyttämällä peilaavia tiedonvarmennusjärjestelmiä tai vähentämällä riippuvuutta yksittäisistä asiakkaista. Kuten todettu, samat riskejä ehkäisevät toimenpiteet voivat edistää samanaikaisesti sekä yrityksen joustavuutta että toipumisnopeutta. Hyvänä esimerkkinä on jatkuvuussuunnitelmien koulutus ja harjoittelu: suunnitelman harjoittelun avulla henkilöstö oppii toimimaan nopeasti ongelmatilanteissa, mutta samalla he oppivat myös tunnistamaan häiriöiden aiheuttajat. Näin he ymmärtävät paremmin miten toimia, jotta ongelmilta vältyttäisiin kokonaan. Hyvän joustavuuden hedelmät ovat usein näkyviä vain häiriöiden sattuessa, mutta se turvaa jatkuvasti yrityksen arvoa paremman riskienehkäisyn ja toimintojen luotettavuuden kautta. (Herbane ym. 2004, 441)

2.7.3 Sulautuminen

Sulautuminen on jatkuvuudenhallinnan strategisuutta ilmentävä tekijä, joka kuvaa, missä määrin jatkuvuudenhallinnan prosessit ovat levittäytyneet osaksi koko yritystä, sen henkilöstöä ja toimintatapoja. Jatkuvuudenhallinnan sulautumista on havaittavissa, mikäli strateginen jatkuvuusajattelu on levinnyt myös ylimmän johdon ulkopuolelle saaden aikaan henkilöstön sitoutumista sen periaatteisiin ja tavoitteisiin. Jatkuvuudenhallinta ei tällöin ole yritykselle ainoastaan dokumentoitu suunnitelma, vaan osa päivittäistä toimintaa yksilötasolla asti. (Herbane ym. 2004, 442)

Herbane ym. (2004, 442) ovat sitä mieltä, että sulautuminen on ehdoton edellytys jatkuvuudenhallinnan strategiselle roolille, koska vain sulautuneet prosessit voivat tukea yrityksen pitkän tähtäimen strategisia tavoitteita. Muussa tapauksessa jatkuvuudenhallinta on vain ajoittain ilmenevä tukitoiminto, jonka rooli jää operatiiviseksi. Hyviä toimintatapoja kokoava BS25999-standardikin tukee sulautumista, sillä se kehottaa yritystä rakentamaan organisaatiokulttuurin, joka edistää jatkuvuudenhallintaa (Gallagher 2007, 34-35).

2.7.4 Pakollisuus

Organisaation jatkuvuudenhallintaprosessit voivat olla sulautuneita ja yrityksellä saattaa olla erinomainen kyky toipua häiriöistä ja joustaa niiden suhteen. Kipinä jatkuvuudenhallinnan toteuttamiselle ei kuitenkaan aina ole peräisin yrityksen omista tarpeista tai haluista, koska yksittäisen organisaation jatkuvuus saattaa olla myös jonkin ulkopuolisen tahon intressi ja tällä taholla saattaa olla määräysvaltaa kyseiseen yritykseen. Esimerkiksi valtion lait tai toimialan sisäiset standardit voivat asettaa erilaisia vaatimuksia. Siksi eri yritysten jatkuvuudenhallintaa ja sen strategista roolia tuleekin tarkastella hieman eri tavoin riippuen siitä, missä määrin yritys on pakotettu jatkuvuudenhallinnan toteuttamiseen. (Herbane ym. 2004, 441)

Pakollisuus on organisaation näkökulmasta ainut ulkoinen jatkuvuudenhallinnan strategisuutta ilmentävä tekijä. Se kertoo, miltä osin yrityksen jatkuvuudenhallinta on säädelty pakolliseksi ja kuinka yritys näitä säädöksiä noudattaa (Herbane ym. 2004, 441). Esimerkiksi Suomen rahoitusalan yritykset joutuvat noudattamaan Finanssivalvonnan standardia, joka määrittelee melko tarkasti riskeihin varautumisen periaatteet (Standardi 4.4b 2010). Pakollisuus kattaa myös sellaiset standardit ja toimintatavat, joiden noudattamista laki ei varsinaisesti vaadi, mutta joiden omaksuminen on käytännössä välttämätöntä kilpailukyvyn säilyttämiselle esimerkiksi tietyn toimialan sisällä (Herbane ym. 2004, 442).

Jatkuvuudenhallinnan roolia yrityksessä voidaan tarkastella pakollisuuden asteen avulla. Ensin tulee selvittää, mitä jatkuvuudenhallintaan kuuluvia asioita yritykseltä vaaditaan, jonka jälkeen vaatimuksia voidaan verrata yrityksen toimintaan. Organisaatio voi valita, noudattaako se määräyksiä kirjaimellisesti vai kehittääkö se jatkuvuudenhallintaansa pidemmälle. Minimivaatimusten ylittäminen viittaa siihen, että yritys tiedostaa jatkuvuudenhallinnan arvon ja käyttää sitä hyödyksi tavoitteidensa saavuttamisessa. Se on samalla osoitus jatkuvuudenhallinnan strategisemmasta roolista. Eri toimialoilla ja eri yrityksillä saattaa kuitenkin olla erilaisia jatkuvuudenhallintavaatimuksia, joten määräysten ylittämisen merkitystä tulee aina pohtia tapauskohtaisesti. (Herbane ym. 2004, 441-442)

3 TUTKIMUSASETELMA

3.1 Lähestymistapa

Ghaurin ja Grönhaugin (2002, 85-86) mukaan ei voida sanoa, onko kvalitatiivinen tutkimustapa kvantitatiivista parempi tai toisin päin. Tutkimustavat eivät eroa toisistaan tutkimustulosten laadun, vaan tutkimuksen muodon ja toimintatapojen suhteen. Kvantitatiivisen tutkimuksen pääpaino on testauksessa sekä teorioiden ja hypoteesien todistamisessa kun taas kvalitatiivinen tutkimus korostaa tulkintaa ja ilmiöiden ymmärtämistä. Tutkimustavan soveltuvuus tiettyyn tutkimukseen riippuu tutkimusongelmasta (Ghauri & Grönhaug 2002, 86).

Tämän tutkimuksen keskeisenä tavoitteena on luoda kuva siitä, millainen on jatkuvuudenhallinnan rooli suurissa suomalaisissa yrityksissä. Jatkuvuudenhallinnan roolin tutkiminen kvantitatiivisin metodein edellyttäisi tarkkojen tutkimuspisteiden määrittelyä ennen havaintoaineiston keräämistä. Se olisi kuitenkin erittäin hankalaa ja työlästä ja saattaisi rajata merkittävästi tutkimuksen antamaa kuvaa todellisuudesta. Tässä tapauksessa tutkimustulosten kannalta parempi vaihtoehto onkin antaa tutkimuskohteille tilaa tuoda näkemyksiään esiin vapaammin ja tutkia ilmiötä joustavammin ja suunnittelemattomammin (Ghauri & Grönhaug 2002, 87-88). Kvalitatiiviset menetelmät tarjoavat juuri näitä ominaisuuksia ja siksi tämä tutkimus toteutetaan käyttäen kvalitatiivisia metodeja.

Tutkimusstrategiaksi valittiin laaja tapaustutkimus. Se soveltuu erityisesti tutkimuksiin, joiden tarkoituksena on tarkastella jonkin ilmiön olemassa oloa tai luonnetta ja sillä voidaan tutkia ilmiötä syvällisesti sen todellisessa ympäristössä (Hirsjärvi, Remes & Sajavaara 2009, 138-139; Yin 2009, 18). Tässä tapauksessa tutkittava ilmiö on jatkuvuudenhallinta suurissa suomalaisissa yrityksissä vuonna 2010. Laajalla tapaustutkimuksella tarkoitetaan sitä, että havaintoaineisto koostui useista samantyyppisistä havaintoyksiköistä. Laajan tapaustutkimuksen kohteena eivät kuitenkaan ole yksittäiset organisaatiot, vaan niiden kaikkien yhdessä muodostama kokonaiskuva (Eriksson & Kovalainen 2008, 122, 124). Tavoitteena oli löytää riittävästi yhtäläisyyksiä tai eroavaisuuksia havaintoyksiköiden välillä, jotta päätelmät jatkuvuudenhallinnan roolista suomalaisissa yrityksissä olisivat mahdollisia.

Herbane ym. (2004) ovat aikaisemmin toteuttaneet tutkimuksen, jossa he selvittivät jatkuvuudenhallinnan roolia isobritannialaisissa ja yhdysvaltalaisissa rahoitussektorin yrityksissä. Aikaisemman teorian olemassa olo helpottaa tutkimusrakenteen muodostamista sekä haastattelukysymysten kohdistamista oleelliseen informaatioon. (Yin 2009, 18, 130). Siksi Herbanen ym. (2004) tutkimusta käytetäänkin tämän tutkimuksen pääasiallisena teoreettisena viitekehyksenä.

3.2 Tutkimuskohteiden valinta

Tutkimuksen tarkoituksena on tutkia suurten suomalaisten yritysten jatkuvuudenhallintaa. Tässä tutkimuksessa suurena yrityksenä pidettiin organisaatiota, jolla on vähintään 250 työntekijää, joten valinta kohdistui sellaisiin. Rajauksen pohjana käytettiin Tilastokeskuksen määritelmää, jonka mukaan pk-yrityksessä on alle 250 työntekijää (Tilastokeskus 2011). Koska kaikki tutkimukseen osallistuneet yritykset ovat suuria, viitataan pienellä yrityksellä jatkossa noin 250-2000 henkeä ja suurella yli 2000 henkeä työllistävään yritykseen. Tämä helpottaa havaintojen esittämistä.

Toisena valintakriteerinä pidettiin toimialaa, sillä tutkittavien yritysten toimialojen välillä haluttiin olevan riittävää hajontaa. Näin voitaisiin havaita mahdollisia eroja myös toimialojen välillä. Tavoitteeksi asetettiin, että tutkittavia tapauksia olisi vähintään kymmenen kappaletta.

Tietohallinnon ja erityisesti tietoturvan rooli on yrityksen jatkuvuudelle nykyisin merkittävä, joten tutkimuksessa haluttiin saada näkemystä yrityksen tietohallinnon puolelta. Aineistoa pyrittiin keräämään henkilöitä, joilla oli käsitys sekä jatkuvuudenhallinnasta että tietoturvasta. Samalla tiedostettiin, että tutkimusaineisto saattaisi olla rajoittunutta tai puolueellista IT-osaston suuntaan, mikäli aineisto olisi peräisin tietohallintoon suuntautuneilta henkilöiltä.

Potentiaalisia tutkimuskohteita lähestyttiin sähköpostitse ja viesti lähetettiin yhteensä 26 yritykselle. Saatekirjeessä (Liite 1) kerrottiin, mistä tutkimuksessa on kyse ja painotettiin sen luottamuksellisuutta. Samalla kerrottiin, että tutkimus toteutetaan haastattelututkimuksena ja että sen arvioitu kesto on 45 minuuttia. Viestiin liitettiin myös haastattelukysymykset, jotta yritys voisi ohjata haastattelupyynnön parhaiten sopivalle työntekijälle. Kaikille organisaatioille annettiin kolme arkipäivää aikaa perehtyä alustavaan haastattelupyyntöön, jonka jälkeen lähetettiin uusi viesti, jossa tiedusteltiin mahdollisuutta osallistua tutkimukseen. Mikäli toiseen viestiin ei saatu vastausta, ei yritykseen otettu enää yhteyttä.

Loppujen lopuksi tutkimukseen osallistui yksitoista organisaatiota. Niiden henkilöstömäärät vaihtelevat noin 250:stä yli sataan tuhanteen, joten ero pienimmän ja suurimman välillä on merkittävä. Siitä kertoo myös se, että yritysten henkilöstölukumäärien keskiarvo on noin 14900, mutta mediaani sijoittuu kuitenkin vain 1100 henkeen. Taulukko 1 antaa kokonaiskuvan tutkimukseen osallistuneista yrityksistä.

Taulukko 1 Tutkimuksen havaintoyksiköt

Yrityksen toimiala	**Henkilöstömäärä**	**Haastateltavan titteli**
Pankki- ja vakuutusala	390	Tietohallintopäällikkö
Pankki- ja vakuutusala	1000	IT-palvelupäällikkö
Pankki- ja vakuutusala	8000	Tietoturvajohtaja
Pankki- ja vakuutusala	36500	Turvallisuusjohtaja Riskienhallintajohtaja
Palveluala	510	Tietohallintojohtaja
Palveluala	700	ICT Manager
Palveluala	1100	Tietoturvapäällikkö
Palveluala	2300	Talousjohtaja
Tuotantoteollisuus	3000	Tietoturvajohtaja
Tuotantoteollisuus	110000	Senior Manager, IT assurance
Tuotantoteollisuus	252	Järjestelmäpäällikkö

Havaintoyksiköiden taustoja tutkittiin tarkemmin, koska ne pyrittiin jakamaan toimialoittain siten, että yhteen toimialaan kuuluisi vähintään kaksi yritystä. Tämä estäisi mahdollisuuden liittää tutkimuksen tuloksia yksittäiseen yritykseen. Organisaatiot jaettiin kolmeen eri toimialaan siten, että jokainen ala sisältää vähintään kolme tapausta. Muutamalla yrityksellä voidaan sanoa olevan liiketoimintaa useammallakin toimialalla, mutta jaottelu tehtiin päätoimisen alan perusteella. Tutkimuksessa käytetyt toimialat ovat pankki- ja vakuutusala, palveluala sekä tuotantoala.

Tutkimukseen osallistuneiden henkilöiden tittelit ja asiantuntemuksen alueet vaihtelevat hieman, mutta pääosin heidän roolinsa yrityksessä liittyvät tietoturvaan ja -hallintoon. He osasivat siten kertoa erityisesti tietoturvan merkityksestä yrityksessä ja sen jatkuvuudenhallinnassa. Joukossa oli myös muutama riskienhallinnasta tai yleisestä turvallisuudesta vastaava henkilö, joiden näkökulma jatkuvuudenhallintaan oli liiketoiminnallisempi ja kokonaisvaltaisempi.

3.3 Aineiston keruu

Jatkuvuudenhallinnan tutkiminen toissijaisen datan, kuten raporttien, tilastojen tai asiakastutkimusten avulla on hankalaa, koska ilmiöstä ei ole olemassa juurikaan käyttökelpoista toissijaista dataa. Tähän vaikuttaa varmasti se, että jatkuvuudenhallinta voi olla hyvin sulautunutta ja sidoksissa ympäristöönsä, jolloin sen tutkiminen edellyttää syvällistä perehtymistä yksittäiseen tutkimuskohteeseen. Jatkuvuudenhallinnan rooli yrityksessä ei muodostu ainoastaan teoista, vaan myös ihmisten asenteista, joiden selvittämiseen toissijainen data ei edes sovellu. Ensisijaisen datan kerääminen ja käyttö onkin

perusteltua, vaikka se vaatii enemmän aikaa ja vaivaa. (Ghauri & Grönhaug 2002, 81-82)

Tutkimusaineisto päätettiin kerätä käyttäen semistrukturoitua teemahaastattelua, jossa kysymykset olivat ennalta laadittuja, mutta avoimia. Kysymyksiin ei näin ollen ole olemassa tiettyjä valmiita vastausvaihtoehtoja, koska sellaisten keksiminen vain rajoittaisi tutkimuksen tuloksia. Tutkittavaan ilmiöön voidaan perehtyä syvällisesti, kun haastateltava saa vastata kysymyksiin omin sanoin. Tämä mahdollistaa sellaistenkin asioiden ilmenemisen, joita kysymysten muodostamisvaiheessa ei olisi osattu edes ajatella tai jotka eivät ole nousseet esiin aikaisemmissa teorioissa. (Ghauri & Grönhaug 2002, 101-102)

Haastattelututkimusta tukee myös kerättävän tiedon arkaluontoisuus. Yritysten tietoturvaan liittyviin kysymyksiin on Kotulicin ja Clarkin (2004, 604-605) tutkimuksen mukaan lähes mahdotonta saada vastausta sähköpostitse tai kirjeitse, ellei tutkimuksella ole erittäin vaikutusvaltaista tai luotettua tukijaa. Lisäksi tiedon suoja tulisi kyetä takaamaan sataprosenttisesti ja tutkimuksen pitäisi olla selvästi yritykselle hyödyksi. Tutkijat eivät suosittelekaan kyselymenetelmien käyttöä, mikäli tutkimuksen kohteena on arkaluontoinen tieto. (Kotulic & Clark 2004, 604-605)

Haastattelua pyrittiin selkeyttämään teemojen avulla, jotta tutkimuskysymyksiin vastaaminen onnistuisi helpommin. Ne käsittelivät jatkuvuudenhallinnan eri osa-alueita ja niiden avulla on mahdollista muodostaa kokonaiskuva jatkuvuudenhallinnan roolista yrityksessä. Teemat perustuivat pitkälti Herbanen ym. (2004) tutkimukseen, mutta niitä sovellettiin ja jaoteltiin tarkoitukseen soveltuvasti. Haastattelut toteutettiin yhdessä toisen, toipumissuunnittelua tutkineen opiskelijan kanssa, mikä vaikutti luonnollisesti myös teemoihin ja kysymyksiin (Liite 2).

Haastattelun runko koostui kahdeksasta teemasta, jotka olivat

- häiriöt
- henkilöstö ja vastuut
- viestintä ja sitoutuminen
- jatkuvuussuunnittelu ja prosessit
- asenteet ja omistajuus
- koostumus ja mittarit
- lainsäädäntö ja standardit
- strategia.

Yhteistyö toisen tutkielmantekijän kanssa vaikutti myös siihen, että haastattelujen kielenä pyrittiin käyttämään englantia. Tämä tuotiin esille myös yrityksille lähetetyissä haastattelupyynnöissä. Haastattelukysymykset tehtiin sekä suomeksi, että englanniksi ja ne käännettiin mahdollisimman suoraan kieleltä toiselle, jotta haastattelujen tulokset

olisivat vertailukelpoisia. Yhdestätoista yrityksestä neljä halusi tehdä haastattelun suomeksi ja lopuissa keskustelu käytiin englanniksi.

Kaikki haastattelut tehtiin henkilökohtaisesti yritysten toimitiloissa. Haastatelluilta saatujen signaalien perusteella yritykset keskustelevat tietoturva- ja jatkuvuudenhallinta-asioistaan mieluiten kasvotusten. Haastattelut myös nauhoitettiin yhtä lukuun ottamatta. Poikkeus jouduttiin tekemään, koska yrityksen edustaja kielsi nauhoittamisen. Tästä haastattelusta teimme tutkimusparini kanssa kirjalliset muistiinpanot, joita jälkeenpäin vertailimme ja yhdistelimme. Nauhoitetut haastattelut litteroitiin siten, ettei yksittäisiä yrityksiä tai henkilöitä kyetä tunnistamaan. Tämän jälkeen haastatelluilta varmistettiin litterointien oikeellisuus ja heille annettiin mahdollisuus korjata virheitä ja lisätä heidän mielestään puuttuvia asioita.

3.4 Aineiston analyysi

Yhdentoista haastattelun jälkeen kasassa oli suuri määrä tietoa, jonka hyödyntäminen edellytti analyysiä. Yinin (2009, 127) mukaan aineiston analysointi on yksi kehittymättömimmistä ja vaikeimmista vaiheista tapaustutkimuksessa. Toisin kuin kvantitatiivisen aineiston analyysissa, kvalitatiivisen aineiston analysoijalle ei juuri ole olemassa etukäteen määriteltyjä toimintaohjeita, vaan paljon on kiinni itse tutkijasta. Oleellista analyysissä on oikeastaan vain se, että tutkija ymmärtää ja oppii tuntemaan ilmiötä (Ghauri & Grönhaug 2002, 137).

Kuten aineiston keruussa, myös analyysissä tukeuduttiin aikaisempaan teoriaan, jolla tässäkin tapauksessa tarkoitetaan Herbanen ym. (2004) tutkimusta jatkuvuudenhallinnan roolista. Se auttoi luokittelemaan aineistoa ja keskittymään tutkimuksen kannalta oleellisiin tiedonmurusiin (Yin 2009, 130).

Herbane ym. (2004, 444) käyttivät tutkimuksessaan neljää teemaa, jotka olivat: 1. henkilöstö ja vastuut (*human resources and responsibilities)* 2. jatkuvuussuunnittelu ja prosessit (*business continuity planning and processes)* 3. viestintä ja rakenne (*communications and structure*) sekä 4. asenteet jatkuvuutta kohtaan ja prosessin omistajuus (*attitudes toward business continuity and ownership of the process*). Niistä jokainen on oma näkökulmansa jatkuvuudenhallintaan ja niiden kautta voidaan tehdä erilaisia päätelmiä. Eri teemat voivat siis antaa erilaisia tuloksia jatkuvuudenhallinnan roolista.

Edellä mainittuja Herbanen ym. (2004) teemoja käytettiin pienin muutoksin aineiston analyysissä. Mielestäni tietohallinnon rooli yrityksen häiriöttömyyden turvaamisessa ei kuitenkaan tule kyllin selvästi esille edellä mainituista teemoista ja lisäksi fyysiset resurssit, kuten toimitilat ja raaka-aineet jäävät pitkälti huomiotta. Niiden suunnitelmallinen hyödyntäminen yrityksen jatkuvuudenhallinnassa voi silti parantaa yrityksen toipumisnopeutta ja joustavuutta merkittävästi. Siksi Herbanen ym. (2004) teemojen rin-

nalle luotiin viides teema: tietovarat ja fyysiset resurssit. Kaikkien teemojen sisällöt käsitellään tarkemmin analyysikappaleessa.

Näin ollen analyysissä käytetyt teemat olivat:

- henkilöstö ja vastuut
- tietovarat ja fyysiset resurssit
- jatkuvuussuunnittelu ja prosessit
- viestintä ja rakenne
- asenteet ja sitoutuminen

Aineiston analyysitekniikkana käytettiin ristikkäisanalyysiä (*cross-case analysis*), joka soveltuu erityisesti usean tapauksen tapaustutkimukseen. Jokaisesta havaintoyksiköstä muodostetaan ensin oma kuvauksensa, jonka jälkeen tuloksia etsitään tutkimalla kaikkia tapauksia kokonaisuutena. Apuna voidaan käyttää esimerkiksi sana- tai asialistoja, jotka helpottavat tapausten vertailua (Yin 2009, 156, 160; Eriksson & Kovalainen 2008, 130).

Tässä tutkimuksessa käytettiin hyväksi itse luotua 65 kohdan listaa (Liite 3), joka sisälsi sekä tulkinnanvaraisia, että melko yksiselitteisiä asioita. Nämä kohdat valittiin aikaisempaan teoriaan perustuen ja ne ilmentävät kukin omalla tavallaan jatkuvuudenhallinnan roolia. Aineistosta pyrittiin löytämään vastaus jokaiseen kohtaan, erikseen jokaisen yrityksen kohdalla. Sitten kohtia vertailtiin yritysten ja toimialojen kesken ja niistä pyrittiin löytämään yhtenevyyksiä sekä eroavaisuuksia johtopäätösten tekemiseksi. Kaikkiin kohtiin ei jokaisen yrityksen kohdalla saatu selviä vastauksia, mikä rajoitti myös päätelmien tekemistä.

3.5 Tutkimuksen arviointi

Erityisesti kvalitatiivisessa tutkimuksessa on haasteena, miten lukijat vakuutetaan tutkimuksen laadusta ja luotettavuudesta. Lähtökohtana on, että tutkija on kvalitatiivisen tutkimuksen tärkein tutkimusväline ja tutkimukset ovat aina jossain määrin subjektiivisia (Eskola & Suoranta 1996, 165). Tutkimuksen tulee olla läpinäkyvää ja sitä tulee voida arvioida, jotta sen vahvuudet ja rajoitukset kyetään määrittelemään. Klassinen tutkimuksen arvioinnin viitekehys sisältää reliabiliteetin, validiteetin ja yleistettävyyden, mutta niiden soveltumattomuus laadulliseen tutkimukseen on johtanut erilaisen käsitteen, luotettavuuden (*trustworthyness*) käyttöön. Se arvioi tutkimusta uskottavuuden (*credibility*), siirrettävyyden (*transferability*), varmuuden (*dependability*) ja vahvistettavuuden (*confirmability*) näkökulmista. (Eriksson & Kovalainen 2008, 291-294)

Uskottavuudella tarkoitetaan sitä, kuinka hyvin tutkimuksen tulokset peilaavat todellisuutta. Hyvä uskottavuus edellyttää tutkijan riittävää asiantuntemusta ja perehtymistä. Muidenkin tutkijoiden tulee pystyä pääsemään riittävän lähelle tutkimuksen tuloksia annetun aineiston pohjalta tai hyväksymään tulokset. (Eriksson & Kovalainen 2008, 294; Eskola & Suoranta 1996, 167)

Tässä tutkimuksessa tutkijalla ei ollut aikaisempaa tietämystä jatkuvuudenhallinnasta, vaan se kertyi tutkimuksen edetessä. Tutustuin aiheeseen huolellisesti lukemalla siihen liittyvää kirjallisuutta. Pitkäaikaisen kokemuksen puuttuminen on kuitenkin voinut vaikuttaa sekä havaintoaineiston keräämiseen, että sen tulkintaan. Joidenkin haastattelukysymysten vääränlainen muotoilu on saattanut vääristää joitakin tuloksia ja tutkijan rajalliset tiedot ovat mahdollistaneet sen, ettei kaikkia virheitä ole havaittu. Toisaalta jatkuvuudenhallinnan teoriat muodostavat niin sekavan ja kiistellyn kokonaisuuden, että erot eri tutkijoiden tulkintojen välillä voivat johtua myös siitä.

Haastatteluja tehtiin yhteensä yksitoista, joka on kohtuullisen paljon kvalitatiivisessa tapaustutkimuksessa ja parantaa tutkimuksen luotettavuutta. Osa haastatteluista tehtiin englanniksi ja osa suomeksi. Niiden nauhoittaminen parantaa luotettavuutta, mutta siitä huolimatta on olemassa väärinymmärryksen riski, koska haastateltava tai haastateltavat eivät puhu englantia äidinkielenään. Asioita ei välttämättä osata pukea sanoiksi niin kuin ne on tarkoitettu tai kuulija ei ymmärrä kuulemaansa oikealla tavalla. Tutkimusaineistosta löytyi kaiken kaikkiaan vain muutama pieni kohta, jota en ymmärtänyt lainkaan, mutta väärinymmärrysten lukumäärän arviointi on mahdotonta.

Haastatteluun osallistuneiden henkilöiden taustat ovat saattaneet vaikuttaa heidän vastaustensa painopisteisiin. Pohdittaessa esimerkiksi jatkuvuudenhallinnan laajuutta yrityksessä, on pyritty ottamaan huomioon haastateltavan tausta. Tietoturva-asiantuntijan kuva jatkuvuudenhallinnasta voi olla IT-keskeisempi kuin talousjohtajan.

Haastatelluilla oli hyvin aikaa vastata esitettyihin kysymyksiin eikä kukaan kieltäytynyt vastaamasta yhteenkään kysymykseen. Tarpeen vaatiessa esitettiin lisäkysymyksiä ja lisäksi kaikki haastateltavat suostuivat vastaamaan täydentäviin kysymyksiin tarvittaessa sähköpostitse. Haastattelija ei johdatellut kysymyksiä suuntaan eikä toiseen, eikä vastauksiin pyritty muutenkaan vaikuttamaan.

Siirrettävyydellä viitataan siihen, että tutkijan tulee todeta tutkimuksen yhtenevyys aikaisempien tutkimusten kanssa, jotta tulosten välille voidaan luoda jonkinlainen yhteys. Tarkoitus ei ole havaita plagiointia, vaan tarjota lukijoille mahdollisuus vertailla samansuuntaisten tutkimusten tuloksia. (Eriksson & Kovalainen 2008, 294)

Hyvin samantyyppisenä tutkimuksena on esitelty vain Herbanen ym. (2004) tutkimus, koska se on ainoana pohtinut varsinaisesti jatkuvuudenhallinnan roolia. Sitä on käytetty hyväksi koko empiirisen tutkimuksen rakenteen suunnittelussa ja analysoinnissa. Olen verrannut havaintojani jossain määrin myös suoraan Herbanen ym. (2004) tuloksiin.

Tutkimuksen varmuudella tarkoitetaan, että tutkijan tulee kuvata riittävän tarkasti tutkimuksen looginen eteneminen ja käytetyt menetelmät. Riittävä dokumentointi varmistaa, että tutkimus on toistettavissa ja parantaa tutkimuksen luotettavuutta. (Eriksson & Kovalainen 2008, 294) Tämän tutkimuksen eteneminen on kuvailtu tarkasti varmuuden parantamiseksi. Se kattaa tutkimuskohteiden valinnan, aineiston keruun sekä analyysin vaiheet ja perustelut niiden tekemiselle.

Neljäntenä luotettavuuden näkökulmana on vahvistettavuus. Sillä varmistutaan, etteivät tutkijan tulkinnat ole vain tuulesta temmattuja mielikuvituksen tuotteita. Tulkinnat tulee johtaa havaintoaineistosta siten, että muutkin voivat ymmärtää tutkijan ajatusten kulun (Eriksson & Kovalainen 2008, 294). Analyysissä olen aina pyrkinyt esittelemään ensin datan, josta päätelmiä teen. Tulkintojen perustelut on siis kerrottu tai ne ovat näkyvillä ja lukija voi itse arvioida, tulkitseeko aineiston tutkijan tavoin.

4 HAVAINNOT

4.1 Henkilöstö ja vastuut

Ensimmäinen teema kokoaa yhteen jatkuvuudenhallintaan liittyvät vastuuasiat ja kartoittaa yritysten inhimillisiä resursseja. Nimensä mukaisesti teema porautuu esimerkiksi jatkuvuus- ja kriisienhallintavastuiden jakautumiseen sekä henkilöstöresursseihin. Jatkuvuudenhallinnan vastuiden jakautuminen kertoo paljon yrityksen jatkuvuusajattelusta. Turner (1994, 215-216) toteaa onnettomuuksien olevan ilmiöitä, jotka johtuvat teknisten syiden ohella lähes aina myös johtamiseen ja hallintoon liittyvistä tekijöistä. Hyvällä hallinnolla on siis erittäin tärkeä rooli kriisien ehkäisemisessä. Herbanen ym. (2004, 439) mukaan aito, mahdollisesti strateginen jatkuvuudenhallinta on sosioteknistä ja poikkitoiminnallista. Poikkitoiminnallisuutta ja parempaa sulautumista edustaa vastuiden jakaminen myös ylimmän johdon ulkopuolelle. Kun vastuu jatkuvuudesta kulkee läpi organisaation, synnyttää se todennäköisesti myös sitoutumista jatkuvuuden edistämiseksi ja sulattaa jatkuvuusideologiaa yhä luontaisemmaksi osaksi organisaation päivittäistä toimintaa. (Herbane ym. 2004, 444-445)

4.1.1 Jatkuvuussuunnitteluvastuut

Vastuuhenkilöt sekä jatkuvuus- ja kriisienhallintatiimit ovat hyviä tutkimuskohteita, koska ne ilmentävät, nähdäänkö jatkuvuudenhallinta koko yrityksen laajuisena prosessina. Niistä voidaan tehdä tulkintoja jatkuvuusajattelun sulautumisesta ja painopisteistä (Herbane ym. 2004, 444). Mikäli päävastuu jatkuvuudesta on annettu esimerkiksi IT-osastolle, jää näkökulma jatkuvuuteen melko suppeaksi. Seurauksena voi olla, että oleellisia liiketoiminnan ongelmia tai parannuskohtia jää huomaamatta, mikä taas on haitaksi yrityksen joustavuudelle. Lisäksi jatkuvuusajattelun juurruttaminen koko yrityksen ajattelutapaan voi olla hankalaa (Herbane ym. 2004, 445).

Jatkuvuudenhallinnan vastuukysymykset ovat kiinnostavia myös yrityksen toipumisnopeutta ajatellen. Mikäli jatkuvuussuunnitelman laadinta on hajautettu siten, että jokaisen yksittäisen osan laatijana on kyseisen alueen asiantuntija, on toipumissuunnitelmakin todennäköisesti kattavampi ja soveltuvampi, kuin jos ratkaisua haettaisiin yksittäisellä ylimmän johdon kokonaisratkaisulla. Mikäli kriisitilanteen vastuut ovat hyvin määriteltyjä ja johtovastuun ottaa ensisijaisen ongelma-alueen johtaja, voidaan saavuttaa hyvä toipumiskyky, koska suunnitelma on hänen laatimansa ja siksi todennäköisesti myös hyvin sisäistetty. Tämä on osoitus organisaation valppaudesta, mikä on Herbanen ym. (2004, 440) mukaan kyvykkyys, joka johtaa nopeampaan toipumiseen.

Haastatteluista havaittiin, että pitkän tähtäimen suunnittelun levinneisyys ylimmän johdon ulkopuolelle riippuu jossain määrin yrityksen koosta. Suuremmissa, vähintään tuhannen työntekijän yrityksissä jatkuvuussuunnittelu on siirretty pääosin divisiooniin tai yksiköihin. Pienemmissä taas suunnittelusta vastaa usein johtoryhmä tai mahdollisesti pelkkä IT-osasto. Tämä on sinänsä loogista, koska suurempien yritysten liiketoiminta on monimutkaisempaa ja ylimmän johdon käsitys liiketoiminnoista tai yksiköistä ei ole usein kovinkaan tarkka. Pienemmissä organisaatioissa myös ylin johto voi olla kyvykäs luomaan toimivia jatkuvuussuunnitelmia, koska he työskentelevät itsekin lähellä liiketoimintoja ja asiakasrajapintaa.

Organisaation alatasojen sitouttaminen suunnitteluun viittaa siihen, että pitkän tähtäimen suunnittelu on pyritty levittämään koko yritykseen, jolloin jatkuvuudenhallintaideologian sulautumisen aste on korkeampi. Vastuun jakautumisen kautta ilmenevä sulautuminen on kuitenkin hankala havaita pienemmissä yrityksissä, koska organisaation pienuuden vuoksi jatkuvuudenhallintavastuita ei ole kenties edes syytä hajauttaa. Näin ollen vastuun hajauttamista tuleekin tarkastella suhteessa yrityksen kokoon. Pienemmässä yrityksessä, jonka jatkuvuussuunnittelusta vastaa vain viisi ihmistä, voi sulautumisen aste olla korkeampi kuin suuremmassa yrityksessä, jossa vastuussa on kymmenen henkilöä.

Erityisen selvästi vastuun hajauttaminen ilmenee pankki- ja vakuutusalan yrityksissä, joista kolme on siirtänyt vastuun yksiköille. Osasyynä on varmasti Finanssivalvonnan standardi, joka vaatii yrityksiä laatimaan kaikille keskeisille liiketoiminnoilleen ajantasaiset ja riittävät jatkuvuussuunnitelmat (Standardi 4.4b 2010, 22).

> *Jokaisella yksiköllä ja divisioonalla tulisi olla jatkuvuussuunnitelma. […] Divisioonan johtajan vastuulla on, että kaikilla niillä yksiköillä, jotka sitä tarvitsevat, on jatkuvuussuunnitelma olemassa ja päivitettynä.*
> (Turvallisuusjohtaja, pankki- ja vakuutusala)

Tuotantoalan yrityksiä eivät koske tämänkaltaiset säädökset, mutta niistäkin kaksi suurinta on antanut suunnitteluvastuun yksiköille. Ne ovat siis tehneet näin vapaaehtoisesti, mikä viittaa strategisempaan lähestymistapaan, kuin pankki- ja vakuutusalan yrityksissä. Palvelualalla hajauttaminen vaikuttaisi olevan harvinaisinta, sillä yksikään yritys ei ole antanut vastuuta liiketoimintayksiköille tai alemmille organisaatiotasoille IT-osastoa lukuun ottamatta.

4.1.2 Vastuu IT:n jatkuvuudesta

Nykyajan liiketoiminnassa tieto ja erityisesti digitaalinen tieto on elintärkeää lähes yritykselle kuin yritykselle. Siksi odotin IT:n olevan erityisen suuressa roolissa myös organisaatioiden jatkuvuudenhallinnassa. Tämä ei kuitenkaan tule yksiselitteisesti esille vastuiden kautta, sillä minkään yrityksen jatkuvuussuunnittelu ei ole rajoittunut yksinomaan IT-osastolle. Osassa yrityksistä painopiste tosin on IT:ssä. Myöskään kriisitilanteiden johtaminen ei ole IT-osaston vastuulla, vaan yleensä mukana on osaajia eri osa-alueilta. Kaikilta yrityksiltä ei löydy varsinaista kirjallista jatkuvuus- tai toipumissuunnitelmaa, mutta kriiseihin on varauduttu enemmän tai vähemmän myös IT:n ulkopuolella. Tämä viittaa siihen, ettei yrityksen kaikkien ongelmien katsota olevan lähtöisin IT:stä, minkä ymmärtäminen on yksi edellytys strategisesti hyödynnettävälle jatkuvuudenhallinnalle.

> *Ehkä se on meillä se, että se on niin kriittinen tämä jatkuvuusasia ja ylipäätään se, että millaisia ne ovat ne yllättävät poikkeamatilanteet meidän liiketoiminnalle ja asiakaspalvelulle. Että se pitää olla niin hyvin vahvistettu ja mahdollisimman laajasti asiantuntemusta siinä ryhmässä pitää olla, jotta me pystymme nopeasti reagoimaan ja nopeasti sitten palauttamaan tilanne ennalleen.*
> (Tietohallintopäällikkö, pankki- ja vakuutusala)

Yrityksen IT-infrastruktuurin hallinnointi ja vastuu sen ylläpidosta voivat vaikuttaa organisaation toipumisnopeuteen ja joustokykyyn. Mikäli yritys luottaa omaan IT-osaamiseensa ja -resursseihinsa enemmän kuin olisi perusteltua, voi pieni häiriö muuttua nopeasti laajavahinkoiseksi kriisiksi. Mikäli taas IT on päätetty ulkoistaa, voivat toipumista hankaloittaa esimerkiksi informaatiokatkokset tai toimittajan kiireet muiden asiakkaiden kanssa. Toisaalta ulkoisen toimittajan erikoisasiantuntemus ja resurssit auttavat suunnitelmien laatimisessa sekä kriiseissä.

> *Kaikki (IT-laitteet) ovat meidän omissa tiloissa, omassa hallussa, omassa omistuksessa ja omassa ylläpidossa. Se on ihan sellainen strateginen valinta, että olemme lähteneet siihen, koska koemme sen niin tärkeäksi. Ulkoistamisella on tietysti jotakin hyviä puolia, mutta yksi huono puoli on se, että se hidastaa reaktioaikaa. [...] Nyt kun meillä on kaikki täällä omassa tilassa ja meillä on oma henkilökunta, joka sen tekee, niin se reaktioaika lyhenee siihen, että kun se ehtii sen tekemään, niin se tekee sen alusta loppuun. Että ei olla ulkoistettu.*
> (ICT Manager, palveluala)

IT:n ulkoistaminen on hankala kysymys jatkuvuudenhallinnan strategisen roolin kannalta, koska sekä ulkoistaminen, että ulkoistamatta jättäminen voidaan perustella pyrkimyksellä parempaan toipumisnopeuteen ja joustavuuteen. Infrastruktuurin pitäminen yrityksen sisällä edellyttää suuria panostuksia, koska esimerkiksi henkilöstön osaamistaso, tietojärjestelmät ja tiedonvarmennus tulee itse pitää riittävällä tasolla. Hyvä puoli on esimerkiksi se, että omat asiantuntijat tuntevat organisaation järjestelmät läpikotaisin ja työskentelevät vain ja ainoastaan työnantajayritykselleen ollen siten välittömästi käytettävissä häiriön sattuessa. Lisäksi omassa hallinnassa olevat tietojärjestelmät ovat helposti muokattavissa, mikäli tarve niin vaatii. Erään ulkoistamatta jättäneen palvelualan yrityksen tietohallintojohtaja kuvaili oman henkilöstönsä osaamistasoa seuraavasti:

> *Järjestelmäasiantuntijat toteuttavat koko infran, eli he valvovat, asentavat palvelimet ja työasemat, hoitavat kirjoittimet, kaikki. Eli sitä kautta heillä on kokemusta käyttöjärjestelmistä, raudasta, ohjelmistoista […] Heillä on 5-15 vuoden kokemus vastaavista tehtävistä. Pääsääntöisesti meillä on huono puolikin se, että meillä on kierto niin vähäistä, että vaihtuvuus on jopa liiankin pientä. Viimeinen on tullut työharjoittelun kautta 2005. He tuntevat organisaation ja talon ja ovat olleet koko kehityskaaren mukana.*
> (Tietohallintojohtaja, palveluala)

Toisaalta ulkoistaminenkin voidaan nähdä positiivisena yrityksen reagointikyvyn ja joustavuuden kannalta. Kun infrastruktuuri annetaan sellaisen tahon haltuun, jolle IT on ydinosaamista, voidaan olettaa, että palvelu on tietyn tasoista ja että resursseja ja taitoa on riittävästi häiriötilanteiden selvittämiseksi.

> *Että nykykäytäntö on, että pyritään löytämään jokaiselle osa-alueelle kustannustehokas ja paras ammattitaito. Että kaikkea ei pysty näin laajassa kokonaisuudessa itse tekemään. Mutta he kuitenkin tekevät nämä asiat meidän ohjeistuksemme kautta ja raportoivat ja samoin siellä seurataan palveluvasteaikoja ja sitten toiminnan häiriöttömyyttä ja sille on sitten sanktioita ja niin edelleen.*
> (Talousjohtaja, palveluala)

Sekä IT:n ulkoistaminen tai ulkoistamatta jättäminen voidaan siis perustella joko toipumisnopeuden tai joustavuuden paranemisella. Ratkaisevaa ulkoistamisratkaisun strategisuudessa on kuitenkin sen luonne – onko päätös tehty liiketoiminnan tarpeiden ja

organisationaalisen edun perusteella sekä yrityksen pitkän aikavälin arvoa ajatellen vai onko ratkaisu vain tarkemmin harkitsematonta jatkoa aiemmalle toiminnalle (Herbane 2004, 439).

Havaintoaineiston perusteella noin puolet yrityksistä on perustellut itselleen, miksi tiettyyn ulkoistamisratkaisuun on päädytty. Syitä olivat esimerkiksi jo aikaisemminkin mainittu reaktioaika ja parhaan osaamisen hankkiminen. Eräs yritys totesi ulkoistaneensa tiettyjä IT-toimintoja, koska on katsottu, ettei oma osaaminen riitä niihin tai osaamisen ylläpito ei ole kannattavaa. Harkittujen ratkaisujen määrä voi olla tätä suurempikin, sillä kaikissa tapauksissa ei noussut esiin erityisiä perusteluja. Kaikista yrityksistä vain yksi kertoi, että päätös säilyttää IT-infrastruktuuri omalla vastuulla johtuu pitkälti ”historian havinasta”. Havainnot viittaavat siis siihen, että ratkaisut tehdään useimmin perustellusti, yrityksen liiketoiminnan pitkän aikavälin etuja ajatellen, eli ne ovat luonteeltaan strategisia.

IT:n ulkoistaminen näyttäisi olevan melko voimakkaasti riippuvaista yrityksen koosta. Kuudesta alle 1500 henkeä työllistävästä organisaatiosta vain kaksi pankki- ja vakuutusalan yritystä on ulkoistanut IT:n. Neljä viidestä näitä suuremmasta yrityksestä on ulkoistanut suurimman osan. Suurilla yrityksillä olisi kenties resursseja toteuttaa itse IT-infrastruktuurinsa, mutta ne ovat pääsääntöisesti päättäneet keskittyä ydinliiketoimintaansa ja ulkoistaneet IT:n. Pienet yritykset taas hoitavat rajallisista resursseistaan huolimatta IT:n useimmin itse.

Merkittäväksi IT:n ulkoistamista selittäväksi tekijäksi muodostui haastattelujen perusteella myös toimiala, mutta vaihtelua esiintyi toimialojen sisälläkin. Pankki- ja vakuutusalalla IT:n ulkoistaminen oli selvästi yleisintä. Kaikki haastatellut alan yritykset kertoivat ulkoistaneensa vähintään kriittiset järjestelmänsä. Alan yrityksille tietojärjestelmien toimivuus ja tiedon saatavuus ovat niin kriittisiä asiakaspalvelun toimivuuden ja lainsäädännön tiukkojen vaatimusten täyttämisen kannalta, että ne ovat ilmeisesti katsoneet parhaaksi ostaa huippuosaamista ulkoa ja keskittyneet itse omaan ydinliiketoimintaansa.

> *Pankkitoimintahan ei ole mitään muuta kuin tietojen hallintaa. Mitään ei pysty tekemään ilman tietotekniikkaa. Et voi tehdä sopimuksia tai nostaa rahaa.*
> (Tietohallintopäällikkö, pankki- ja vakuutusala)

Ne yritykset, jotka ovat päättäneet pitää suurimman osan IT-infrastruktuuristaan talon sisällä, ovat hyvin luottavaisia oman IT:nsä suhteen. Se on sikäli myös perusteltua, että niillä on päätöksen seurauksena selvästi paremmat valmiudet ratkoa itse IT-ongelmia, kuin ulkoistaneilla yrityksillä. Ulkoistamatta jättäneet yritykset uskovat kykenevänsä toipumaan IT-häiriöistä riittävän nopeasti, mutta ne kaikki ovat jättäneet

avoimeksi myös mahdollisuuden ostaa ulkopuolista apua, mikäli oma osaaminen tai resurssit eivät sattuisikaan riittämään. Käytännön osaamista arvostetaan erityisen paljon ja se heijastuu erään tietohallintojohtajan mukaan myös dokumentointiin eli jatkuvuus- ja toipumissuunnitelmien tekemiseen:

> *Olen ehkä vähän vanhan kansan kasvatti siinä mielessä, että tekemisen kautta oppinut näitä asioita, niin näen hirvittävän tärkeänä sen, että ne ihmiset oikeasti osaavat sen. Olen aina suhtautunut kriittisesti kaikissa tietojärjestelmissä sen dokumentoinnin tärkeyteen. Myönnän, että olen osittain väärässä, mutta tärkeämpää on se, että ne ihmiset oikeasti tietävät, mitä ne tekevät ja ymmärtävät.*
> (Tietohallintojohtaja, palveluala)

4.1.3 Kriisienhallintavastuut

Herbanen ym. (2004, 442-443) mukaan organisaatio, joka pyrkii hoitamaan kriisejään organisaation alatasoilla, osoittaa strategisempaa lähestymistapaa jatkuvuudenhallintaan, koska tämä luottamus kannustaa pitkän tähtäimen jatkuvuusajatteluun kaikilla organisaatiotasoilla. Aineiston perusteella organisaatioilla on selvästi erilaisia tapoja jakaa kriisiajan johtovastuuta. Osa yrityksistä haluaa ylimmän johdon olevan mukana lähes kaikkien häiriöiden käsittelemisessä kun taas toiset pyrkivät pitämään vastuun mahdollisimman alhaisella tasolla mahdollisimman pitkään. Parhaassa tapauksessa liiketoimintayksikkö kykenee hoitamaan häiriön itsenäisesti, eikä ylin johto saa ongelmasta välttämättä edes tietoa.

Vaikka riskien proaktiivinen tunnistaminen ja ennaltaehkäisy eivät haastattelujen perusteella olekaan suuressa roolissa kaikissa yrityksissä, ovat ne kaikki pohtineet ainakin jossain määrin kriisitilanteita ja niissä toimimista. Aina kyettiin nimeämään joku taho, joka ottaa ohjat käsiinsä silloin, kun asiat eivät sujukaan suunnitellun mukaisesti ja tarvitaan nopeaa reagointia. Kriisitilanteiden vastuut onkin määritelty vähintään kohtuullisen hyvin kaikissa haastatelluista yrityksistä.

Aineiston perusteella yritysten kriisienhallintavastuut voivat jakautua kolmentyyppisesti. Ensimmäinen tapa on, että häiriöitä hoitamaan on määritetty etukäteen tiimi tai tiimit, jotka ottavat häiriön ilmetessä johtovastuun ja hoitavat asiat itsenäisesti järjestykseen. Toinen vaihtoehto on, että näiden etukäteen määriteltyjen kriisienhallintatiimien lisäksi toipumisen johtamiseen osallistuu tilanteesta riippuen asiantuntijoita, kuten häiriölle altistuneiden liiketoimintayksiköiden tai divisioonien johtajia. Kolmas malli kriisivastuiden jakamiselle on jättää tiimit etukäteen määrittelemättä ja muodostaa sellainen aina häiriöstä riippuen niistä asiantuntijoista, joita toipuminen edellyttää.

Haastattelujen perusteella yritykset jakautuvat melko tasaisesti sekä toimialojen, että kokojensa osalta edellä mainittuihin kolmeen tyyppiin. Ne organisaatiot, jotka ovat määritelleet kriisienhallintatiimit melko tarkasti etukäteen, ovat sisällyttäneet niihin sekä liiketoiminnan, että IT:n asiantuntijoita.

> *Meillä taustalla pyörii tuollainen Crisis Management Team, jossa on sitten jaettuna vastuut erilaisille liiketoiminnan häiriötekijöille – oli se sitten varkaus, tulipalo, tietoturva- tai imagohaitta. Kaikki nämä kuitenkin vaikuttavat meidän liiketoimintaamme. [...]Meillä on koko johtoryhmä siellä, eli on toimialajohtajat, henkilöstöjohtaja ja toimitusjohtaja, joista tulee jo viisi. Sitten on meidän asiakkuuspäällikkö, joka vastaa käytännön viestinnästä. Sitten on kiinteistöpäällikkö ja turvallisuusvastaava siinä mukana. Lisäksi tiedotetaan myös sisäiselle tarkastukselle ja eräälle johtajalle.*
> (Talousjohtaja, palveluala)

Muutamassa yrityksessä liiketoiminnalle ja IT:lle on määritelty erikseen omat kriisienhallintatiiminsä, kun taas eräässä sama tiimi reagoi kaikkiin häiriöihin. Etukäteen määritellyt tiimit voivat parantaa yrityksen toipumisnopeutta erityisten organisointi- ja viestintäkykyjensä avulla. Mikäli tiimeillä ei ole kuitenkaan ole tarkkaa tuntemusta häiriöalueen liiketoiminnasta, voivat päätökset olla yrityksen kannalta epäsuotuisia, eikä toipumisnopeus merkittävästi parane.

Neljän tapausyrityksen kriisienhallinta lähtee liikkeelle ydintiimistä, jonka ympärille kootaan tilanteesta riippuen erityistaitoisia ihmisiä. Kriisienhallinnalle on haluttu jättää kiinteän yksittäisen tiimin sijasta hieman joustovaraa, koska kaikki häiriöt ovat loppujen lopuksi yksilöllisiä.

> *On vaikea muodostaa etukäteen mitään laajempaa organisaatiota, koska häiriö voi olla mikä tahansa. […] Eli sitä ei ole tehty valmiiksi ja syy on yksinkertaisesti etukäteen muodostamisen vaikeus. Mutta operationaalinen riskienhallinta on se, joka aloittaa prosessin… ja sitten IT.*
> (Tietoturvajohtaja, pankki- ja vakuutusala)

Ydintiimiin kuuluu aineiston perusteella tavallisimmin liiketoiminnan ylintä johtoa ja tukitoimintojen edustajia, kuten riskien ja kiinteistöturvan asiantuntijoita, henkilöstön ja yhteistyökumppaneiden turvallisuudesta vastaavia ihmisiä sekä viestintään tai tietohallintoon erikoistuneita henkilöitä. Tarkoituksena on ilmeisesti ottaa mukaan ne henkilöt ja toiminnot, joiden läsnäolo on katsottu olevan tarpeellista kaikissa häiriöissä. He hal-

litsevat tietyt häiriöiden poistamisen edellyttämät asiat paremmin kuin liiketoimintayksiköiden johtajat.

> *He ovat enemmänkin turvallisuusihmisiä. Ne erikoistilanteet – sanotaan vaikka, että meillä on jonkinlainen suuri onnettomuus – vaativat hieman enemmän, kuin mitä ehkä pystymme liiketoimintajohtajalta odottamaan. Heidän fokuksensa on jossain muualla kuin turvallisuudessa koko ajan ja nämä riskienhallinnan ihmiset on koulutettu esimerkiksi kriiseihin, joten heillä on vähän enemmän tietämystä viestinnästä, henkilöstöhallinnosta ja sellaisesta.*
> (Tietoturvajohtaja, pankki- ja vakuutusala)

Kun ydintiimi hoitaa kriisissä esimerkiksi henkilöturvallisuuteen tai viestintään liittyviä asioita, voi liiketoiminta-alueensa toiminnan parhaiten tunteva yksikön tai divisioonan johtaja keskittyä liiketoiminnallisiin asioihin. Tämä vaikuttaa todennäköisesti yrityksen toipumisnopeuteen positiivisesti.

Kriisienhallintaorganisaatio voidaan jättää myös kokonaan tilannekohtaisesti muodostuvaksi. Häiriöitä ryhtyvät käsittelemään ne, joita häiriö koskettaa tai jotka voivat osaamisellaan edesauttaa nopeaa toipumista. Erityistä ryhmää ei ole siis määritelty, mutta jokaisella toiminnolla ja prosessilla on oma vastuuhenkilönsä, joka reagoi tarvittaessa. Tällainen rakenne on havaittavissa neljässä yrityksessä. Niille luonteenomaista on, että reagoiminen lähtee kriisialueelta ja ensisijainen johtovastuu on alueen vastaavalla tai sillä, joka tuntee alueen parhaiten. Asiantuntemusta ja suurempaa päätäntävaltaa otetaan mukaan tarpeen vaatiessa.

> *Jos tulee häiriöitä, se riippuu siitä, missä kohtaa häiriö on. Sen asian vastuulliset henkilöt. Ja sitten tavallaan koottaisiin jonkinnäköistä tiimiä sen ympärille tapauskohtaisesti. Mutta ei ole sellaisia kriisinhallintajoukkoja.*
> (ICT Manager, palveluala)

4.1.4 Koordinaattorit

Eräässä pankki- ja vakuutusalan yrityksessä riskienhallinta ja jatkuvuuden turvaaminen näkyvät selvästi myös henkilöstön tehtävissä. Jokaisella divisioonalla ja osalla yksiköistäkin on oma riskienhallintahenkilönsä, jonka tehtävänä on tukea linjajohtoa riskien tunnistamisessa ja ennaltaehkäisemisessä sekä parantaa henkilöstön tietoisuutta erilaisten riskien olemassa olosta. Lisäksi he valvovat, että yksikön toiminta vastaa organisaa-

tion tai lainsäädännön asettamia vaatimuksia ja auttavat sekä jatkuvuussuunnitelmien laatimisessa että niiden testaamisessa ja päivittämisessä. He siis tukevat yksikön toimintaa, mutta heillä on kuitenkin aina mahdollisuus raportoida ylemmille johtoportaille, mikäli he katsovat, että riskienhallintaa laiminlyödään.

Herbane ym. (2004, 447) kutsuvat tämänkaltaisia henkilöitä koordinaattoreiksi ja heillä on suuri merkitys jatkuvuudenhallinnan viestinnälle ja pohjainformaation laadulle. Näistä organisaatiossa virallisesti määritellyistä koordinaattoreista on todettu olevan hyötyä, koska he ovat linkki yritysjohdon, toimintojen ja prosessien välillä. Viralliset koordinaattorit myös viittaavat siihen, että jatkuvuudenhallintaa pidetään yrityksessä strategisena voimavarana. (Herbane ym. 2004, 447)

Muissa tutkituista yrityksistä ei esiintynyt vastaavanlaisia koordinaattoreita. Kuitenkin yhdessä palvelualan ja yhdessä tuotantoalan yrityksessä tietoturvajohtaja toimii eräänlaisena IT:n koordinaattorina. Myös näistä tapauksista voidaan todeta, että organisaatio on selvästi tunnistanut koordinaattorista saatavan viestintähyödyn ja pyrkii saavuttamaan sen avulla parempaa IT-palvelujen jatkuvuutta.

> *Autan IT-henkilöstöä luomaan ja arvioimaan jatkuvuussuunnitelmia. Tämä arviointi on jatkuvaa, eikä se voi valmistua, sillä vaatimukset muuttuvat. Liiketoiminnan vaatimukset muuttuvat nopeasti eivätkä uudet tarpeet ole IT:lle automaattisesti selkeitä, joten minä toimin välikätenä IT:n ja liiketoiminnan välillä.*
> (Tietoturvajohtaja, palveluala)

Kyseisessä palvelualan yrityksen tapauksessa toipumissuunnitelman soveltuminen liiketoiminnan tarpeisiin on jatkuvan tarkastelun alla, joten toipumissuunnittelu on selvästi liiketoimintalähtöistä. Sen ylläpitämiseksi uhrataan resursseja, mikä viittaa siihen, että toipumissuunnitelmaa pidetään organisaation tavoitteiden kannalta oleellisena. Tämä on merkki IT:n jatkuvuudenhallinnan strategisesta suuntautumisesta yrityksessä. Koordinaattorin keskittyminen vain IT-toimintojen jatkuvuuteen viittaa kuitenkin tekniseen lähestymistapaan, eikä palvele koko yritystä. Näin ollen IT-koordinaattorin olemassa olo ei ole luonteeltaan strategista.

Tapauksista tulee selvästi esiin, että pankki- ja vakuutussektorin yritykset ovat panostaneet muita enemmän riskienhallintaan. Finanssivalvonnan vaatimuksilla on jälleen varmasti tekemistä asian kanssa, koska ne määrittelevät melko tarkasti riskienhallinnan periaatteet (Standardi 4.4b 2010, 13-15). Riskienhallinnan laajuus näyttäisi olevan voimakkaasti riippuvaista sekä yrityksen toimialasta, että koosta työntekijöiden määrässä mitattuna. Pankki- ja vakuutussektorin yritysten lisäksi organisoitua riskienhallintaa oli selkeästi nähtävissä ainoastaan eräässä tuotantoalan yrityksessä, jossa työntekijöitä on huomattavasti muita enemmän.

Kysyttäessä jatkuvuudenhallinnan vastuutahoja, kertoi kolme pankki- ja vakuutusalan yritystä neljästä, että heidän jatkuvuudenhallintansa on suurelta osin erillisen riskienhallintaorganisaation tai riskiasiantuntijoiden käsissä. Tämä viittaa häiriöiden ennaltaehkäisyyn, mikä parantaa yrityksen joustavuutta myös IT:n ulkopuolisten häiriöiden suhteen. Suunnitteluvastuu on yksiköillä, mutta nämä erilliset tahot kartoittavat riskejä aktiivisesti koko organisaation laajuudella. Herbanen ym. (2004, 447) mukaan koordinaattorin tehtävänä on tukea oleellisen tiedon havaitsemista, ja levittää informaatiota läpi organisaation. Riskienhallintaorganisaatio ja -asiantuntijat tekevät juuri tätä työtä ja ne voidaankin mieltää virallisiksi koordinaattoreiksi ja siten osoitukseksi jatkuvuuden strategisesta tärkeydestä yrityksessä.

4.1.5 Henkilöstöresurssit

Kriisienhallintatiimien luoman valppauden ohella organisaation toipumisnopeuteen vaikuttaa valmius, joka kuvaa, missä määrin yritys on nähnyt vaivaa valmistautuakseen kriiseihin etukäteen esimerkiksi resurssisuunnittelulla. Se kattaa fyysisten resurssien, kuten toimitilojen ja materiaalien lisäksi myös henkilöstöresurssit (Herbane ym. 2004, 440). Tutkimusyrityksistä analysoitiinkin, miten ylimääräiset henkilöstöresurssit on niissä otettu huomioon. Onko yritys panostanut esimerkiksi ristikkäiseen osaamiseen vai luotetaanko siihen, että ulkopuolisilta toimittajilta saadaan tarvittaessa apua? Etukäteen suunnitelluilla henkilöstöresursseilla voidaan parantaa organisaation toipumisnopeutta sekä kykyä vastustaa kriisejä, koska työntekijöitä voidaan esimerkiksi siirtää tarvittaessa kriittisempiin tehtäviin ja puuttuvaa osaamista voidaan täydentää toimittajan palveluilla.

IT:n osalta todettiin jo aikaisemmin, että IT-infrastruktuurin ulkoistaneet yritykset ovat pääosin hyvin riippuvaisia toimittajan osaamisesta ja resursseista kun taas ne, jotka eivät ole ulkoistaneet infrastruktuuriaan, ovat siltä osin melko omavaraisia. Nekin kuitenkin luottavat osin toimittajilta saatavaan apuun hädän hetkellä. Nämä toimittajat ovat havaintoaineiston perusteella aina ennalta määritettyjä yhteistyökumppaneita, joten osaamisen ja henkilöstöresurssien riittävyys sekä nopea reagointikyky on pyritty turvaamaan tiedostamalla oman osaamisen mahdollinen riittämättömyys.

> *Eli meillä on tiettyjä kriittisiä osia sillä tavalla, että meillä on yhteistyö- ja asiantuntijakumppaneita, joiden kanssa niitä on rakennettu ja niiltä on saatavissa myöskin tarvittaessa sitä apua ja korvaamaan sitä omaakin resurssia. Ja näin on tehtykin välillä ihan kapasiteetinkin kannalta teetetty. Vaikka olisi itselläkin ollut osaamista, mutta resurssit eivät ole olleet riittäviä – että ei ole keritty tekemään – niin silloin se on otettu sieltä ul-*

> *kopuolelta sitten. Mutta näitä on vain tiettyihin, hyvin kriittisiin kohteisiin, eli lähinnä dataan liittyvät, palomuurit, toimistojen liittämiseen toisiinsa ja siihen on olemassa resursseja ulkopuolisia, jotka pystyvät kyllä auttamaan sitten.*
> (ICT Manager, palveluala)

Muiden kuin IT:tä koskevien ylimääräisten henkilöstöresurssien osalta ei juuri kyetty tekemään erityishavaintoja. Kaksi pankki- ja vakuutusalan yritystä tosin totesivat, että kriisitilanteessa toiminnan jatkuvuutta parantaa laaja konttoriverkosto. Yhden konttorin ollessa poissa pelistä, voidaan sen työtaakkaa jakaa toimivien konttoreiden kesken. Samoin yhden henkilön poissa ollessa voidaan hänen tehtäviään siirtää muiden konttorien työntekijöille. Konttoriverkostostakaan ei tosin ole hyötyä, mikäli ongelma on esimerkiksi koko organisaation laajuisessa tietojärjestelmässä. Yleisesti ottaen voidaan olettaa, että yritykset, joilla on useita samantyylisiä toimipaikkoja ja paljon henkilöstöä kykenevät paikkaamaan henkilöstövajetta paremmin. Tämä vaikuttaa yrityksen joustavuuteen ja toipumiskykyyn.

4.1.6 Yhteenveto

Jatkuvuussuunnitelmat tulisi räätälöidä liiketoimintojen tarpeisiin ja eri yksiköiden pitäisi osallistua suunnitteluun. Näin varmistetaan yrityksen optimaalinen joustavuus ja toipumisnopeus sekä henkilöstön sitoutuminen (Herbane ym. 2004, 442-443, 446, 450). Havaintojen perusteella pitkän tähtäimen jatkuvuussuunnittelun hajauttaminen yrityksen ylimmän johdon ulkopuolelle riippuu yrityksen koosta. Mitä suurempi yritys on kyseessä, sitä todennäköisemmin vastuuta on jaettu yksiköihin ja divisiooniin. Hajauttaminen vaikuttaa olevan pankki- ja vakuutusalalla yleinen ja palvelualalla harvinainen käytäntö. Herbanen ym. (2004, 447) kuvailemia koordinaattoreita yritykset hyödyntävät erittäin harvoin, mutta niihin verrattavissa olevaa riskienhallintatoimintaa havaittiin erityisesti pankki- ja vakuutusalan yrityksistä.

Jatkuvuudenhallintaan liittyvien vastuiden keskittyminen tai rajoittuminen IT-osastoon viittaa rajoittuneeseen lähestymistapaan, joka ei ole luonteeltaan strategista (Herbane ym. 2004, 446). Yksikään tapausyrityksistä ei rajoita jatkuvuudenhallintaansa ainoastaan informaatioteknologiaan, mutta osassa on havaittavissa selvää painottumista. Kriisienhallinnassa on kuitenkin aina mukana sekä IT:n että liiketoiminnan edustajia.

IT-infrastruktuurin ulkoistaminen voi vaikuttaa yrityksen toipumisnopeuteen ja joustavuuteen. Havainnot viittaavat siihen, että yrityksen koon kasvaessa IT todennäköisemmin ulkoistetaan. Nekin yritykset, jotka ovat jättäneet IT:n omalle vastuulleen, luottavat ulkoista apua olevan tarvittaessa saatavilla. Ulkoistamispäätösten lopputuloksia

tärkeämpiä ovat kuitenkin niiden perustelut, sillä ne kertovat enemmän jatkuvuudenhallinnan roolista. Useimmat yritykset ovat perustelleet ratkaisunsa ja syinä ovat esimerkiksi osaamistason varmistaminen ja riittävä reaktiokyky. Tämä on merkki strategisesta ajattelusta.

4.2 Tietovarat ja fyysiset resurssit

Työntekijöiden osaamisen ja saatavuuden varmistaminen on tärkeää, mutta se ei missään nimessä ole ainut liiketoiminnalle kriittinen resurssi. Monien, erityisesti suomalaisten organisaatioiden työ on nykyisin ns. tietotyötä, johon liittyy tiedon luomista, käsittelyä ja hallintaa. Tämä tieto tulee aina myös tallentaa jossakin muodossa johonkin paikkaan, jotta sitä voitaisiin käyttää hyväksi ja tarkastella myöhemminkin. Tallennus ei vielä kuitenkaan itsessään riitä takeeksi tiedon saatavuudelle, koska tieto on aina haavoittuvaista ja alttiina uhille. Tarvitaan suoja- ja varajärjestelmiä. Erään palveluyrityksen ICT Manager kiteytti tiedon saatavuuden merkityksen seuraavasti:

> *Kun ajattelee, että meidän arvokkain omaisuutemme mitä on, on se tehty työ. Että me tehdään sitä työtä, joka tallentuu meidän palvelimillemme ja menee sieltä turvakopioihin. Ja sitten jos tapahtuu jotakin, että se häviää jostakin syystä, niin viikkojen… tai sanotaan, että jotakin häviää, niin se saattaa olla, että useammat ihmiset ovat tehneet viikkoja töitä ja sitten se häviää, niin se on aikamoinen kustannuserä. Niin silloin me ollaan koettu se turvakopiointi ja siitä palauttaminen, että se on todella tärkeä, että pystymme palauttamaan sen tilanteen, joka on ollutkin.*
> (ICT Manager, palveluala)

4.2.1 Tiedon saatavuus

Tallennetun tiedon merkitys yrityksen toiminnalle voi siis olla valtava – ja usein onkin. Monesti yrityksen kilpailukyky on peräisin tehdystä työstä ja siten luodusta tiedosta. Sen saatavuuden hallinta on yksi suurimmista tekijöistä yrityksen kriisivalmiudelle, toipumisnopeudelle ja joustavuudelle, minkä vuoksi tutkimuksessa kiinnitettiin huomiota juuri tiedon saatavuuden varmistamiseen (Herbane ym. 2004, 440).

Tutkitut yritykset ovat huomioineet tiedonvarmennuksen pääosin erittäin hyvin. Suurin osa varmentaa ainakin kriittisimmät tietonsa ja järjestelmänsä peilaamalla. Pankki- ja vakuutusalan yrityksistä näin tekevät kaikki. Vaikka päätietokannalle tai -

järjestelmälle tapahtuisi jotakin, voidaan toimintaa jatkaa lähes normaalisti ja parhaassa tapauksessa keskeytyksettä. Varmennusjärjestelmän toimiessa oikein, ei tietoa ja siten henkilöstön työpanosta heitetä hukkaan. Tämä vaikuttaa merkittävästi organisaation kykyyn vastustaa kriisejä ja toipua niistä.

> *Se on suunniteltu toimimaan sillä tavalla. Kapasiteetti ei ehkä ole 100% ja se voi olla hieman hitaampi, mutta se toimii.*
> (Tietoturvajohtaja, pankki- ja vakuutusala)

Ne yritykset, jotka eivät jatkuvasti peilaa tietoaan varmuuskopioihin, luottavat päivittäin tehtäviin nauha- tai levyvarmistuksiin. Nekin ovat siis tiedostaneet tiedon saatavuuden merkityksen, mutta eivät ole katsoneet tarpeelliseksi pitää yllä täysin ajantasaista varatietokantaa. Tiedot varmennetaan öisin, joten tarvittaessa saatavilla on aina edellisen päivän dataa. Tämä mahdollistaa yhden päivän tietojen katoamisen, mutta se on silti tärkeä tekijä yrityksen hyvälle joustavuudelle ja toipumisnopeudelle. Kaikilta tutkituilta yrityksiltä löytyy siis vähintään edellisen päivän varmuuskopiot, joten varmennusten ajantasaisuus on kaiken kaikkiaan hyvällä mallilla.

Tietoliikenneyhteyksien nopeutuminen on vaikuttanut siihen, että varmuuskopioita ei useinkaan säilytetä lähellä alkuperäisiä tallenteita. Tämä on havaittavissa myös haastatelluissa yrityksissä, joista yhdeksän kertoi säilyttävänsä ainakin kriittisten tietojen varmuuskopioita fyysisesti eri sijainnissa kuin alkuperäisiä. Säilytyspaikan etäisyys vaihtelee jonkin verran. Joillakin yrityksillä varmennukset ovat naapurirakennuksessa, toisilla taas satojen kilometrien päässä ja jopa useissa eri sijainneissa. Tärkeintä kuitenkin on, etteivät ne voi tuhoutua samanaikaisesti esimerkiksi vesivahingon tai tulipalon sattuessa.

Ne yritykset, joiden varmuuskopiot sijaitsevat samassa rakennuksessa kuin alkuperäinen data, ovat kuitenkin sijoittaneet varmennuksensa eri paloalueelle. Sen on nähty alentavan riskit riittävät alhaiselle tasolle ja on siis tietoista riskinottoa.

> *Että jos tämä talo tuhoutuu täydellisesti ja kokonaan, niin kyllä meillä sitten on sillä tavalla munat samassa korissa, että meillä on sekä palvelimet että turvakopiot samassa rakennuksessa. Sehän on jonkunmoinen riski, mutta toistaiseksi se riski on arvioitu sellaiseksi, että toivottavasti tällaista ei tapahdu ja pyritty varautumaan siihen riskiin.*
> (ICT Manager, palveluala)

Kuten Wade (2004) artikkelissaan toteaa, suurin uhka tietoturvalle on ihminen. Siksi tekninen varmennus ei riitä suojaamaan tietoa täydellisesti. Tietoturvan tärkeydestä ja sen ylläpitämisen edellyttämistä toimenpiteistä tulee viestiä tehokkaasti, jotta dataa

käyttävät ja muokkaavat ihmiset eivät vaarantaisi tietoturvan tavoitteiden saavuttamista. Heidät tulisi kyetä sitouttamaan tietoturvaperiaatteisiin, jotta tietoturva – yhtenä osana jatkuvuudenhallintaa – muodostuisi saumattomaksi osaksi ajattelua ja toimintaa. Viestintää ja sitoutumista käsitellään myöhemmin kappaleissa 4.4 ja 4.5.

4.2.2 Toimitilat

Luonnonmullistuksen tai vaikkapa sähkökatkon sattuessa on datan hajauttaminen tärkeää toipumisen ja jatkuvuuden kannalta. Mikäli tiedon hyväksikäyttö ei kuitenkaan ole mahdollista ilman alkuperäisiä toimitiloja ja laitteita, voi edessä olla ongelmia. Tiedon saatavuuden varmistamisen ohella yrityksen tulisikin kartoittaa myös vaihtoehtoisia paikkoja, joissa toimintaa voidaan tarvittaessa jatkaa. Tämä pätee myös tuotantokeskeisiin, laiteriippuvaisempiin yrityksiin, joiden tulisi pohtia tuotantolaitteisiin liittyviä riskejä sekä mahdollisuuksia laitteiden korvaamiseksi.

Tutkimuksessa löytyi viitteitä sille, että pankki- ja vakuutusalalle ominainen laaja konttoriverkosto auttaa myös tässä tapauksessa. Toimialan tietokeskeisyys mahdollistaa joustavuuden sijainnin suhteen. Asiakkaan tietoihin päästään käsiksi mistä konttorista tahansa, joten palvelu ei keskeydy, vaikka yksittäinen konttori joutuisikin sulkemaan ovensa.

Palvelu- ja tuotantoalojen laiteriippuvaisemmissa organisaatioissa sijainnillinen joustavuus riippuu jossain määrin liiketoiminnan luonteesta ja yrityksen koosta. Eräällä haastatellulla tuotantoalan suuryrityksellä on esimerkiksi niin monta tuotantopaikkaa, että edes yhden poisjääminen ei olisi kohtalokasta. Pienemmissä yrityksissä on pohdittu ainakin joidenkin organisaationlaajuisten tukitoimintojen, kuten tietohallinnon korvaamista tarvittaessa. Tuotantopaikan häiriö tuottaisi niissä kuitenkin jo nopeasti suuria ongelmia. Kaikille yrityksille toimipaikan vaihto ei olisi edes mahdollista.

> *Mutta toki tuohon voi sanoa, että jos meidän toimitiloja ei olisi käytössä, niin ei meidän yritystäkään olisi sitten. Sanotaan vähän kärjistetysti, että minulta on joskus kysytty, että miten me varmistaisimme tietojärjestelmien toimivuuden jos meidän toimitilamme tuhoutuisivat, niin ei meillä ole mitään ongelmaa. Pistetään vain työnhakuilmoituksia, koska ei meidän yritystäkään ole sen jälkeen. Ei meillä ole mitään mahdollisuutta käynnistää meidän toimintaa. Me olemme konkurssissa ennen kuin me saamme toiminnan pystyyn jossakin muualla. Tästä kaupungista ei löydy tiloja.*
> (Tietohallintojohtaja, palveluala)

4.2.3 Yhteenveto

Tiedon merkitys yrityksen liiketoiminnalle on suuri, joten toimet, jotka parantavat tiedon saatavuutta vaikuttavat yrityksen jatkuvuuteen (Herbane ym. 2004, 440). Havaintojen perusteella tämä on tiedostettu erittäin hyvin. Tiedonvarmennukseen on kiinnitetty huomiota myös niissä yrityksissä, joissa jatkuvuudenhallinta ei muilta osin ole suuressa roolissa. Organisaatiot käyttävät peilaavaa varmuuskopiointia tai vähintään öisin tehtävää nauhavarmistusta. Muutamassa yrityksessä varmuuskopiot sijaitsevat fyysisesti samassa rakennuksessa, mutta yleisempää on siirtää tieto kaukaisempaan paikkaan.

Toimintaan vaadittavien laitteiden ja toimitilojen saatavuus on paremmalla tolalla niissä yrityksissä, joilla on käytettävissään useita samanlaisia konttoreita tai tuotantopaikkoja. Yhden toimipaikan jouduttua ongelmiin voivat muut auttaa tilanteen hallitsemisessa. Kaikkien yritysten ei ole liiketoimintansa luonteen vuoksi edes mahdollista siirtyä vaihtoehtoiseen toimipaikkaan.

4.3 Jatkuvuussuunnittelu ja prosessit

Jatkuvuudenhallinnan roolia yrityksessä voidaan tarkastella jatkuvuussuunnittelun ja sen luomisprosessin kautta. Kolmannessa teemassa tutkitaankin yrityksen jatkuvuussuunnitteluun liittyviä asioita. Tarkastelun kohteena ovat suunnitteluprosessien vaiheet, niiden laajuus ja suuntautuminen.

4.3.1 Suunnitelman luominen

Kirjallinen jatkuvuussuunnitelma on jo itsessään osoitus pyrkimyksestä häiriöttömyyteen ja kertoo, että yritys on nähnyt ainakin jossain määrin vaivaa kartoittaakseen toimintaansa uhkaavia riskejä ja omia haavoittuvuuksiaan. Suunnitelmien sisällöt sekä voivat kuitenkin erota toisistaan todella paljon. Siksi myös jatkuvuudenhallinnan rooli organisaatiossa voidaan nähdä hyvin erilaisena suunnitelmasta riippuen.

Liiketoiminnalle tehty kirjallinen jatkuvuussuunnitelma löytyy yhdeksästä yrityksestä, joten sen olemassa olo on melko yleistä. Pankki- ja vakuutusalan kaikilla haastatelluilla yrityksillä on jatkuvuussuunnitelma – tiukasta lainsäädännöstä johtuen. Muiltakin aloilta suunnitelmia löytyy. Niiden sisällöllinen kattavuus ja merkitys liiketoiminnan tavoitteiden saavuttamiselle vaihtelevat kuitenkin suuresti.

Jotkut organisaatiot eivät ole luoneet järjestelmälliseen analysointiin perustuvia, koko liiketoiminnan kattavia kirjallisia jatkuvuussuunnitelmia, mutta nekin ovat uhranneet aikaa turvatakseen tärkeimmän voimavaransa, eli ihmiset. Näiltä yrityksiltä löytyy pe-

lastussuunnitelmat, joiden avulla henkilöstöä pyritään suojelemaan hätätilanteessa. Tämä on lakien mukaista ja noudattaa Devargasin (1999, 36) priorisointia, jonka mukaan työntekijät ovat yrityksen tärkein turvattava resurssi häiriön sattuessa. Liiketoiminnan joustavuutta tai toipumiskykyä ei ole ryhdytty harkitusti kehittämään, mutta esimerkiksi riskienhallintaa on saatettu kuitenkin tehdä.

Kaikki organisaatiot eivät käytä yrityksen jatkuvuutta ylläpitävistä suunnitelmista nimitystä ”jatkuvuussuunnitelma”. Esimerkiksi erään palveluyrityksen jatkuvuussuunnittelu on käytännössä johdon tekemää strategiatyötä. Ylin johto tekee suunnitelmat viideksi vuodeksi eteenpäin ja määrittelee, millä tavalla liiketoiminta voi kehittyä suotuisasti. Suunnitelmat sisältävät tarvittavia toimenpiteitä ja painotusalueita ja häiriötilanteisiin varautuminen on luonnollinen osa niitä. Jatkuvuudenhallinta on vain teoreettinen käsite, joka kattaa häiriöitä ja niiden vaikutuksia ehkäisevän toiminnan. Organisaatio saattaa hyvinkin mukailla jatkuvuudenhallinnan teoreettista viitekehystä ja tavoitella sen hyötyjä, mutta käyttää toiminnastaan täysin eri termejä.

> *Ei, emme sellaista (jatkuvuudenhallinta)termiä käytä. Meille paremmin sopisi liiketoiminnan häiriöttömyys. Mutta me tietysti katsomme sitä laajemminkin kuin riskien kautta. Se on kuitenkin kokonaispaketti, johon liittyy henkilöstö, talous ja sitten myös nämä turvallisuusasiat, jotka liittyvät oikeastaan jokapäiväiseen toimintaan. Että on se sitten henkilöturvallisuutta ja siellä tulee sitten nämä vastuullisuustekijät, työkykyasiat.*
> (Talousjohtaja, palveluala)

Kirjallinen IT:n toipumissuunnitelma löytyy seitsemästä yrityksestä. Niistä peräti viidessä IT-infrastruktuuri on hyvin suurelta osin ulkoistettu. Kaikista yrityksistä kolmella ei ole toipumissuunnitelmaa lainkaan ja niissä kaikissa IT on jätetty omalle vastuulle. Huomion arvoista on siis se, että yritykset, joissa IT-infrastruktuurin ulkoistamisaste on hyvin alhainen, eivät pääsääntöisesti ole tehneet toipumissuunnitelmaa. Pankki- ja vakuutusala erottuu muista, sillä alan kaikista tapausyrityksistä löytyy joko itse laadittu tai toimittajalta vaadittava toipumissuunnitelma. Niissä myös IT-infrastruktuurin ulkoistamisaste on korkea. Tämä on seurausta Finanssivalvonnan standardista, joka edellyttää alan toimijoilta korkeatasoista jatkuvuudenhallintaa ja jatkuvuus- ja toipumissuunnitelmia (Standardi 4.4b 2010).

Toipumissuunnitelman olemassa olo on siis tapausten mukaan usein jollakin tavalla sidoksissa ulkoiseen IT-palvelujen toimittajaan. Haastattelujen perusteella voidaan karkeasti sanoa, että toimittajan osallisuus toipumissuunnitelmien laatimisessa kasvaa sitä mukaa, kun IT-palvelujen ulkoistamisaste nousee. Pankki- ja vakuutusalan yrityksissä toipumissuunnitelma on joko kokonaan toimittajan vastuulla, tai sitten suunnitelmat

luodaan yhteistyössä. Niissä yrityksissä, joista toipumissuunnitelma löytyy ja joissa IT-infrastruktuurin ulkoistamisaste on alhainen, on suunnitelma laadittu itse.

On mielenkiintoista, että yritykset, jotka pitävät IT:nsä talon sisällä ja joiden IT-häiriöiden hoitaminen on omissa käsissä, eivät useinkaan laadi toipumissuunnitelmaa. Tämä voi johtua yritysjohdon suhteesta tietohallinnon henkilöstöön sekä luottamuksesta heidän osaamiseensa. Kun työntekijät ovat oman yrityksen palkkalistoilla ja heidän taitonsa tunnetaan, voi erillisen toipumissuunnitelman laatiminen tuntua sekä työntekijöiden että johdon mielestä turhalta ajan ja resurssien haaskaukselta. IT-henkilöstö tuntee toimialueensa läpikotaisin ja toimii häiriöiden sattuessa samalla tavalla oli toipumissuunnitelmaa tai ei.

IT-infrastruktuurinsa ulkoistaneet yritykset eivät puolestaan tunne – ainakaan yhteistyön alkuvaiheessa – toimittajan kaikkia kyvykkyyksiä ja ilmassa saattaa olla joitakin kysymysmerkkejä. Toipumissuunnitelma on osoitus siitä, että toimittaja on pohtinut erilaisia riskejä ja kriisitilanteissa toimimista etukäteen ja suunnitelmaa arvioimalla asiakasyritys voi varmistua riittävästä IT-palvelujensa suojasta. Se on siis väline toimittajan osaamisen arvioimiseksi, jota ei-ulkoistaneissa yrityksissä ei samalla tavoin tarvita.

4.3.2 Tietopohja

Jatkuvuudenhallinnan käytännön onnistumisen kannalta on ensiarvoisen tärkeää, että se perustuu riittävään ja oikeaan tietoon. Mikäli yritys ei esimerkiksi tunne riskejään tai ne on analysoitu väärin, häiriöiltä on vaikea suojautua. Loppujen lopuksihan yrityksen jatkuvuus on seurausta hyvästä ennakoinnista ja varautumisesta, joka taas pohjautuu historiallisen ja spekulatiivisen tiedon perusteella tehtyihin suunnitelmiin ja harkittuihin toimenpiteisiin. Spekulatiivinen tieto ei kuitenkaan ole silkkaa arvailua, vaan tarkkaa uhkien, haavoittuvuuksien ja suojakeinojen analysointia.

Riskeihin varautuminen sekä toimintojen priorisointi heijastavat omalla tavallaan jatkuvuudenhallinnan roolia organisaatiossa. Mikäli päätösten pohjana käytetään ainoastaan omia summittaisia arvioita, voivat häiriötilanteet yllättää ikävästi. Kaikki haastatellut organisaatiot käyttävät hyväksi omia mielikuviaan siitä, mikä on liiketoiminnan kannalta oleellisinta. Suurin osa kuitenkin hakee tukea mielikuvilleen erilaisilla analyyseillä. Pankki- ja vakuutusalan yrityksille se on välttämätöntä, sillä Finanssivalvonnan standardi vaatii, että suunnitelmat pohjautuvat liiketoimintojen uhka- ja haavoittuvuusanalyyseihin (Standardi 4.4b 2010, 22).

Jatkuvuussuunnitelman painopistealueet ja eri toimintojen tärkeydet liiketoiminnalle tulisi kyetä selvästi perustelemaan. Perusteltavuus ei ole oleellista niinkään ulkoisten sidosryhmien kannalta, vaan suurimman hyödyn faktaan perustuvista päätöksistä saa

yritys itse. Analysoimalla omaa liiketoimintaansa yritys varmistuu siitä, että se kohdistaa resurssejaan oikeisiin paikkoihin oikeassa suhteessa. Tämä parantaa yrityksen joustavuutta ja toipumisnopeutta. Erään palveluyrityksen tietoturvapäällikkö korosti itsetuntemuksen tärkeyttä jatkuvuussuunnittelussa seuraavasti:

> *Jos olemme luomassa jatkuvuussuunnitelmaa IT-järjestelmälle, meidän tulee ensin tunnistaa järjestelmän eri osat ja niiden tärkeys sekä ymmärtää, mitä järjestelmän jatkuvuus edellyttää. […] Se on erittäin tärkeää tehtäessä liiketoiminnallista vaikutusanalyysiä (BIA), joka yhdistää liiketoiminnan tarpeet, IT:n toipumisen ja tietoturvan. Muutoin on hyvin hankalaa saada johtoa investoimaan jatkuvuudenhallintaan.*
> (Tietoturvapäällikkö, palveluala)

Tietoturvapäällikön kommentti rajoittuu IT-näkökulmaan, mutta kertoo ajattelun syvyydestä. Tärkeää on ensin tuntea nimenomaan oma liiketoiminta – sen vahvuudet, heikkoudet, uhat ja vaatimukset. Tälle tietämykselle perustuva suunnittelu tukee yrityksen jatkuvuudenhallintaa huomattavasti paremmin, kuin olettamusten varaan luotu. Resurssien oikeanlainen kohdistaminen parantaa toipumisnopeutta ja joustavuutta.

Haastattelujen perusteella näyttäisi siltä, että mitä liiketoimintalähtöisempää jatkuvuudenhallinta on, sitä parempaan tietoon suunnitelmat perustuvat. Yritykset, joille asiakkaiden vaatimukset ovat suunnittelun päämotivaattori, ovat nähneet selvästi vähemmän vaivaa suunnitelmien luomiseen.

Toimintaympäristön tuntemuksen tärkeys korostuu myös Snedakerin (2007) kuvailemassa jatkuvuussuunnitteluprosessissa, jonka yhtenä osana on riskianalyysi. Jotta yritys voisi tehdä valintoja esimerkiksi nopean, mutta epävakaan sekä hitaan, mutta varman kasvun välillä, tulee sen ensin kartoittaa riskit ja suhteuttaa ne mahdollisiin hyötyihin (Devargas 1999, 37). Analyysin liittäminen suunnitteluun lisääkin todennäköisesti suunnitelman luotettavuutta ja edelleen yrityksen joustavuutta, koska se kyseenalaistaa vakiintuneet ja mahdollisesti virheelliset olettamukset.

Suurimmalla osalla tutkituista yrityksistä on ainakin jonkinasteista riskien tunnistamis- ja ehkäisytoimintaa. Se ei kuitenkaan välttämättä kata koko yritystä saati ulkoisia toimitusketjuja, vaan saattaa rajoittua esimerkiksi tietoturvaan ja teknisiin ongelmiin. Se voi myös käsitellä vain vahinkoriskejä, kuten tulipaloja ja vesivahinkoja ja jättää liikeriskit, kuten materiaalien saatavuuden, tuotteiden kysynnän tai korkojen vaihtelun huomiotta.

Parhaimmillaan riskienhallinta on laajamittaista ja järjestelmällistä. Se tukee liiketoimintayksiköiden jatkuvuussuunnittelua, mutta hallitsee myös yritystasoisia riskejä. Erityisesti pankki- ja vakuutusala nousee esiin, sillä kolmella alan yrityksistä on erillinen riskienhallintaorganisaatio.

> *Meillä on riskienhallinnan johtoryhmä, jota johtaa toimitusjohtaja. Hänellä on siellä useita eri riskien asiantuntijoita. Tämä riskienhallinnan johtoryhmä käsittelee sekä liikeriskit että ns. katastrofiriskit. […] Teemme esimerkiksi paljon sijoituksia ja he hoitavat kaikki sijoitusriskit ja muutkin liikeriskit. Mutta riskienhallinnan johtoryhmä on siis se, joka huolehtii riskeistämme.*
> (IT-palvelupäällikkö, pankki- ja vakuutusala)

Muilla aloilla riskienhallinta on selvästi vaihtelevampaa. Jotkut ovat huomioineet pelkkiä vahinkoriskejä, toiset osittain myös liikeriskejä. Joillakin riskienhallinta tuntuu keskittyvän tietojärjestelmiin tai tietoturvaan, kun taas toisilla näkemys on laajempi. Yhdestä palvelualan yrityksestä ei tunnistettu lainkaan riskien analysointiin viittaavia toimia. Havainnot tukevat jälleen Herbanen ym. (2004, 442) toteamusta siitä, että pankki- ja vakuutusala on muita kehittyneempi jatkuvuudenhallintaan liittyvissä asioissa.

Kaikentyyppinen riskien ja haavoittuvuuksien analysointi parantaa yrityksen tietoisuutta itsestään ja toimintaympäristöstään ja tämän tiedon hyödyntäminen riskien ehkäisyssä parantaa liiketoiminnan joustavuutta häiriöiden suhteen. Mikäli analyysit kuitenkin rajoittuvat vaikkapa IT:hen, ei jatkuvuudenhallinta tue koko organisaation jatkuvuutta ja sen strategisten tavoitteiden saavuttamista. Syntynyt vaikutelma yritysten IT-keskeisestä riskienhallinnasta saattaa tässä tutkimuksessa osittain johtua haastateltavien henkilöiden taustoista, jotka olivat monessa yrityksessä tietoturvapainotteisia. Kiistatonta kuitenkin lienee se, että haastattelujen perusteella pankki- ja vakuutusala poikkeaa muista aloista paremmalla riskienhallinnallaan.

Riskianalyysien ohella jatkuvuussuunnittelun apuna voidaan käyttää erilaisia strategisia suunnittelutyökaluja. Niitä sovelletaan tavallisessakin strategisessa suunnittelussa, koska ne parantavat yrityksen ymmärrystä omasta liiketoiminnastaan. Herbane ym. (2004, 446) toteavat, että näiden työkalujen käyttö jatkuvuuden edistämiseksi osoittaa yrityksen ymmärtäneen strategisen suunnittelun ja jatkuvuudenhallinnan välisen yhteyden yrityksen pitkäaikaisen arvon muodostamisessa sekä sen säilyttämisessä. Se viestii siis siitä, että organisaatio näkee jatkuvuudenhallinnan tärkeänä strategisten tavoitteiden saavuttamisen kannalta.

Esimerkiksi arvoketjuanalyysin (*value chain analysis*) tai liiketoiminnallisen vaikutusanalyysin pohjalta rakennettu jatkuvuussuunnitelma pakottaa tarkastelemaan myös eri toimintojen välisiä yhteyksiä sekä ulkoisia toimitusketjuja (Herbane ym. 2004, 446). Messer (2009, 9) jopa mainitsee liiketoiminnallisen vaikutusanalyysin tehokkaimmaksi yrityksen saatavana olevaksi työkaluksi. Snedaker (2007) on nimennyt juuri liiketoiminnallisen vaikutusanalyysin tärkeäksi osaksi jatkuvuussuunnitteluprosessia, mutta Herbane ym. (2004, 441) toteavat yleisemmin, että yrityksen sisäisten ja ulkoisten vai-

kutus- ja riippuvuussuhteiden tunnistaminen on merkki strategisesta ajattelutavasta. Näin ollen myös muita työkaluja ja toimintamalleja voidaan mieltää strategisiksi.

Haastattelujen perusteella strategisia työkaluja käytetään vain suuremmissa, vähintään tuhannen työntekijän yrityksissä. Seitsemästä kyseisen kokoisesta yrityksestä kuudessa on käytetty jotakin strategiseksi miellettävää suunnittelumetodia. Selvästi yleisin on liiketoiminnallinen vaikutusanalyysi, mutta myös arvoketjuanalyysiä sovelletaan. Haastatelluista alle tuhannen työntekijän yrityksistä yksikään ei ollut omaksunut suunnittelutyökaluja toimintaansa. Joissakin suuremmista yrityksistä suunnittelutyökalujen käyttö on välttämätöntä vaaditunlaisen jatkuvuussuunnitelman luomiseksi:

> *…arvoketjuun kuuluvien yksiköiden arviointi on itse asiassa pakollista. Mitkä ovat organisaation tärkeimmät yksiköt, joille toimitamme palveluja? Ja toisaalta meidän tulee ymmärtää, mitkä ovat tärkeimpiä palvelun-tarjoajiamme, jotta tiedämme tarkasti, mitkä ne yksiköt arvoketjussamme ovat.*
> (Riskienhallintajohtaja, pankki- ja vakuutusala)

Erilaiset analyysit ja strategiset työkalut antavat yritykselle kuvan esimerkiksi siitä, mitkä toiminnot ovat haavoittuvaisimpia uhille, millaiset riskit toteutuvat todennäköisimmin ja minkä prosessin toimimattomuus on haitallisinta liiketoiminnalle. Tälle teoreettisen viitekehyksen mukaiselle pohjalle on melko hyvä alkaa rakentaa yrityksen jatkuvuussuunnitelmaa (Snedaker 2007, 31-35).

Kaikki tutkimuksen organisaatiot eivät kuitenkaan sovella näitä itsetutkiskelua edellyttäviä apuvälineitä lainkaan tai hyödyntävät niitä korkeintaan rajoittuneesti. Ne priorisoivat prosessejaan enemmän tai vähemmän maalaisjärkeen, kokemukseen ja omiin arvioihinsa perustuen.

> *Enemmänkin me simuloimme, että miten me ajattelemme, että miten meidän liiketoiminta kehittyy ilman näitä riskejä, mutta emme me sellaista ole laskeneet, että jos tulee vaikkapa joku epidemia tai tällainen tai sitten liiketoiminta lamaantuu jonkin tietojärjestelmäjutun takia. Kun sen tietää ilman analyysiäkin, että huonosti siinä menee ja sille ei oikein sitten voi mitään. […] Että vähän niin kuin vakuuttamisessa, että mikä sinun riskinsietokyky on. […] Että jos sinä sataprosenttisesti kaiken vakuutat, niin se tulee niin kalliiksi, että ei siinä ole mitään järkeä. Sinun pitää löytää se kultainen keskitie. Oikeastaan käytäntö on sitten siihen opettanut, että mikä on oikea taso.*
> (Talousjohtaja, palveluala)

Haastateltava on yhtä mieltä Snedakerin (2007, 254) kanssa siitä, että tietyn prosessin toimintakatkoksen ja halutun toipumiskyvyn ylläpitämisen aiheuttamien kustannusten välillä tulee löytää optimitila. Jos yritys tarvitsee avainprosessin sataprosenttista saatavuutta, tulee sen sijoittaa prosessin ylläpitämiseen huomattavasti enemmän rahaa, kuin jos sille sallittaisiin ajoittaisia katkoksia. Snedaker (2007, 254) puhuu teoksessaan kuitenkin nimenomaan avainprosesseista, joiden määrittämiseksi on ensin tehty liiketoiminnallinen vaikutusanalyysi. Haastatellussa yrityksessä sellaista ei ilmeisesti ole toteutettu, vaan tärkeysluokittelut perustuvat omiin arvioihin. Voikin siis olla mahdollista, että parhaiten suojellut prosessit eivät olekaan liiketoiminnan kannalta tärkeimpiä.

Myös lainsäädäntö luo omat paineensa tiettyjen prosessien toimivuudelle. Varsinkin pankki- ja vakuutusalan kireät vaatimukset vaikuttavat prosessien priorisointiin ja sitä kautta jatkuvuudenhallinnan painopisteisiin. Kolme alan neljästä yrityksestä mainitsi, että laki asettaa omat vaatimuksensa toiminnalle ja sen edellyttämät prosessit tulee kyetä suorittamaan tilanteesta riippumatta. Samat lait vaikuttavat todennäköisesti myös neljännen yrityksen jatkuvuutta koskeviin ratkaisuihin, vaikka se ei haastattelussa esiin tullutkaan.

> *Olemme priorisoineet siten, että meillä on tietyt kriittiset liiketoiminnot, joiden tulee toimia kaikissa tilanteissa. Niitä ovat esimerkiksi eläkkeet, koska laki vaatii niin. Vaikka tämä rakennus räjähtäisi, meidän pitää maksaa eläkkeet. Olemme priorisoineet ne liiketoiminnan tarpeiden sekä lainsäädännön perusteella.*
> (IT-palvelupäällikkö, pankki- ja vakuutusala)

4.3.3 Laajuus

Aiemmin käsiteltyjen vastuukysymysten ohella myös itse suunnitelma ilmentää, missä määrin jatkuvuus nähdään vain teknisin keinoin ratkaistavana ongelmana. Laaja, sosioteknninen suunnitelma huomioi myös IT:stä riippumattomat häiriöt, kuten työntekijöiden lakot, koska yritys ei koostu ainoastaan tietojärjestelmistä. Avarakatseisempi suhtautuminen suunnitteluun on merkki jatkuvuudenhallinnan suuremmasta roolista yrityksen kokonaisarvon säilyttämisessä. Se on signaali siitä, että jatkuvuudenhallintaa pidetään strategisesti tärkeänä.

Herbane ym. (2004, 445-446) havaitsivat tutkimuksessaan, että yritykset voivat lähestyä jatkuvuussuunnittelua eri tavoin ja nämä tavat heijastuvat koko jatkuvuudenhallinnan laajuuteen. Yksi tapa on jakaa liiketoiminnan ja IT:n prosessit selvästi erilleen painottaen nimenomaan liiketoiminnallista puolta. Jaottelu pyrkii ohjaamaan siihen, että liiketoimintaa tarkastellaan integroituna, sisäisiä ja ulkoisia arvoketjuja sisältävänä ko-

konaisuutena. Laaja näkemys parantaa joustavuutta monenlaisten häiriöiden suhteen ja turvaa asiakkaiden intressejä. Jatkuvuudenhallinta ei näin rajoitu ainoastaan IT-osastoon ja sen merkitys kilpailutekijänä ja arvon säilyttäjänä kasvaa.

Tutkimukseni kaikissa pankki- ja vakuutusalan sekä kahdessa tuotantoteollisuuden yrityksessä on tunnistettavissa edellä mainitun kaltainen jaottelu liiketoiminnan ja IT:n välillä. Ne ovat kaikki kooltaan vertailujoukon yläpäästä. Yritykset kertoivat, että liiketoiminnalle on olemassa IT:stä erillinen suunnitelmansa, mikä on selvä osoitus siitä, että teknisen puolen ohella jatkuvuuden liiketoiminnallinenkin komponentti on huomioitu.

> *Teoriassa meillä on toipumissuunnitelma, mutta vain IT:lle. Heillä on toipumissuunnitelma. Mutta liiketoiminnassa meillä on vain jatkuvuussuunnitelma.*
> (Turvallisuusjohtaja, pankki- ja vakuutusala)

Neljässä yrityksessä jatkuvuussuunnittelu painottuu IT:hen tai vahinkoriskeihin, kuten tulipaloihin ja varkauksiin. Liikeriskejään ne pohtivat jossain määrin, mutta tämä vaikuttaisi olevan satunnaista ja epäorganisoitua. Edellisiin suunnittelutapoihin verrattuna näiden yritysten suunnittelu näyttää reaktiiviselta, lyhytkatseiselta ja tekniseltä. Esimerkiksi erään palveluyrityksen jatkuvuussuunnittelu toteutetaan käytännössä IT-osastolla, mutta lisäksi ”joillakin osastoilla on tämäntyyppisiä dokumentteja”. Käytännön toimenpiteet rajoittuvat lähinnä onnettomuusvalmiuden parantamiseen, kuten tiedonvarmennukseen, kulunvalvontaan ja pelastusharjoituksiin. Näistä neljästä yrityksestä kaksi on luonut jatkuvuussuunnitelmasta fyysisen dokumentin, mutta kahdella sellaista ei ole lainkaan. Riskejä on saatettu analysoida, mutta se ei ole johtanut Snedakerin (2007, 31-35) suunnitteluprosessin mukaiseen riskien ehkäisystrategioiden muodostamiseen. Erään jatkuvuussuunnitelman luoneen palveluyrityksen ICT manager luonnehti tietoturvan asemaa suunnitelmassa seuraavasti:

> *Kyllä tietoturvan rooli siinä (jatkuvuussuunnitelmassa) on hyvin keskeinen. Ihan teknisen tietoturvan.*
> (ICT Manager, palveluala)

Haastatteluaineiston perusteella yritykset, joissa suunnittelun painopiste on IT:ssä tai vahinkoriskeissä, ovat niitä, joissa IT-infrastruktuuria ei ole ulkoistettu. Ne ovat myös kooltaan joukon pienimmästä päästä. Voi olla, että suuremmissa yrityksissä IT-infrastruktuurin ulkoistaminen sekä yhteistyö toimittajan kanssa jättää yritykselle resursseja ja mielenkiintoa suunnitella myös jatkuvuuden liiketoiminnallisia puolia. Lisäksi liiketoiminnan suuren koon mukanaan tuoma monimutkaisuus saattaa edellyttää

etukäteissuunnittelua. Häiriöiden hallinta ilman suunnitelmaa tai ennalta määritettyjä vastuita on yksinkertaisesti hidasta ja hankalaa monimutkaisessa organisaatiossa.

Pienissä yrityksissä syy heikompaan jatkuvuudenhallintaan voi olla nimenomaan yrityksen koko ja käytettävissä olevat resurssit: jos on mahdollista ehkäistä vain hyvin rajallinen osa riskeistä, kohteeksi on helppo valita todennäköisin häiriöiden aiheuttaja. IT ja tietojärjestelmät ovat kaikille nykyorganisaatioille niin kriittisiä toimintaedellytyksiä, että niiden saatavuuden turvaamista pidetään ymmärrettävästi tärkeänä.

4.3.4 Suuntautuminen

Arvo- ja toimitusketjujen tunnistaminen jatkuvuussuunnittelussa voi vaikuttaa yrityksen joustavuuteen. Se, miten yritys huomioi jatkuvuussuunnitelmassaan nimenomaan ulkoiset toimitusketjut, kertoo ajattelutavan suuntautumisesta ja vaikuttaa joustavuuden lisäksi myös toipumisnopeuteen. Esimerkiksi yhteistyökumppaneiden kanssa solmitut sopimukset palvelutasosta ja toipumissuunnitelmista sekä vaihtoehtoisten toimittajien määrittäminen parantavat kykyä vastustaa kriisejä ja kehittävät palautumiskykyä. Yritys tiedostaa siis jatkuvuutensa olevan riippuvainen myös ulkoisista toimitusketjuista. (Herbane 2004, 441)

Haastattelujen perusteella ulkoisia toimitusketjuja voidaan ottaa mukaan yrityksen jatkuvuudenhallintaan monin eri tavoin. Toimittajille saatetaan antaa esimerkiksi palvelutaso- tai tietoturvavaatimuksia tai heiltä saatetaan edellyttää omaa jatkuvuus- tai toipumissuunnitelmaa, jota mahdollisesti myös auditoidaan. Saman hyödykkeen tai palvelun toimittamiseen voidaan käyttää tarkoituksellisesti useampia toimittajia jopa eri maista, jolloin estetään liiallinen riippuvuus yksittäisestä yrityksestä ja vältetään esimerkiksi kansallisten lakkojen haitalliset vaikutukset. Myös asiakkaita voidaan etsiä eri toimialoilta ja kotimaan ulkopuolelta, jotta esimerkiksi kansallinen lama ei pääse vaikuttamaan yhtä voimakkaasti.

Jokainen haastateltu yritys on huomioinut ainakin jossain määrin ulkoisten toimitusketjujen aiheuttamat riskit ja asettanut vaatimuksia niiden ehkäisemiseksi. Niillä pyritään ylläpitämään suunnitelmien mukaista toimintaa. Selkeää yksittäistä tapaa, jota kaikki yritykset olisivat ulkoisiin toimitusketjuihinsa soveltaneet, ei kuitenkaan ole. Yleisimpiä ilmenemismuotoja ovat toimittajille annetut tietoturvakriteerit, palveluvasteajat sekä jatkuvuus- tai toipumissuunnitelmavaatimukset. Kaikki pankki- ja vakuutusalan sekä tuotantoteollisuuden yritykset yhtä lukuun ottamatta vaativat yhteistyökumppaneiltaan jatkuvuus- tai toipumissuunnitelmaa. Vastaavasti palvelualalla näin ei tee yksikään haastateltu yritys.

> *Edellytämme yhteistyökumppaneilta omaa jatkuvuussuunnitelmaa. Että me haluamme todentaa, että jos meillä on rahahuollon yhteistyökumppanilla jotakin ongelmia, niin miten he ovat suunnitelleet oman jatkuvuussuunnitelmansa. Miten toiminta silti pyörii? Miten fyysinen raha liikkuu, vaikka siellä tulisikin heille joku häiriötilanne?*
> (Tietohallintopäällikkö, pankki- ja vakuutusala)

Arvoketjun ulkoisten osien huomioiminen on siis poikkeuksellisen tarkkaa pankki- ja vakuutusalalla. Suuri syy tähän on jälleen Finanssivalvonnan standardi, jossa todetaan yksiselitteisesti, että ”valvottavan on varauduttava ulkoisten sidosryhmiensä toiminnan häiriöihin”. Se kattaa niin alihankkijat, palveluntarjoajat kuin merkittävimmät asiakkaatkin (Standardi 4.4b 2010, 23).

Vaatimusten antamisen lisäksi niiden noudattamista saatetaan myös valvoa. Toimittajaan ei siis luoteta sokeasti, mikä viittaa siihen, että ulkoisista toimitusketjuista johtuvia häiriöitä pyritään aidosti ehkäisemään. Kaksi yritystä vaikutti kuitenkin luottavan pitkälti yhteistyökumppaneiden kanssa solmittuihin sopimuksiin, eivätkä ne maininneet valvovansa tietoturvan toteutumista. Mielenkiintoista on, että eräs tuotantoyritys, jonka toiminnasta ei ole juuri tunnistettavissa Snedakerin (2007, 31-35) jatkuvuussuunnitteluprosessin vaiheita, kertoi auditoivansa toimittajiaan myös jatkuvuusmielessä – kuinka ne pystyvät toimittamaan tavaraa kohdatessaan häiriöitä. Yritys tuntuu siis pohtivan toimittajiensa jatkuvuutta enemmän kuin omaansa. Erään pankki- ja vakuutusalan yrityksen turvallisuusjohtaja kiteytti valvonnan motiiveja seuraavasti:

> *Se on niin, että olemme ulkoistaneet sen, mutta emme voi ulkoistaa riskiä, joten olemme silti vastuussa siitä alueesta ja siksi edellytämme jatkuvuussuunnitelmaa. Eli heillä tulee olla jatkuvuussuunnitelma, jotta tiedämme miten asiat siellä ovat. Ja näin tehdään kaikissa tapauksissa, eli ulkoistamiskumppanilla tulee olla jatkuvuussuunnitelma ja meidän tulee voida tarkastella sitä, jotta voimme arvioida, onko se riittävä meille ja jotta voisimme kehittää sitä yhdessä kumppanin kanssa. Eli loppujen lopuksi meidän täytyy kantaa riski.*
> (Turvallisuusjohtaja, pankki- ja vakuutusala)

Toisaalta, vaikka osassa yrityksistä valvonta on ilmeisesti määritelty virallisesti sopimuksiin ja organisaation toimintamalleihin, voi sen toteutuslaatu vaihdella. Se saattaa luoda harhakuvan, että yritys on turvassa ulkoisten toimitusketjujen riskeiltä. Tämä on yrityksen kannalta erityisen vaarallinen käsitys ja on omiaan johtamaan vakaviin häiriöihin (Turner 1994, 217).

> *Kun joillakin alueilla on pienempiä toimittajia, toivomme, että ne toteuttavat tietoturvatoimenpiteitä. Eräässä tapauksessa kuitenkin tajusimme, ettei sovellustoimittaja käyttänyt minkäänlaista virustorjuntaohjelmaa, joten sanoimme heille, että yhteistyömme tulisi päättymään. He sanoivat, että korjaavat asian saman tien, mutta parannuksia ei koskaan auditoitu kokonaisuudessaan.*
> (Tietoturvapäällikkö, palveluala)

Haastattelujen perusteella havaittiin, että kriisitilanteessa yhdelläkään IT:n ulkoistaneella organisaatiolla ei ole varavaihtoehtoa IT-palvelujen toimittajaksi. Mikäli toimittaja joutuisi ongelmiin, saattaisi se heijastua merkittävinä vaikeuksina myös haastatellulle asiakkaalle. Luottamus yhteistyökumppanin toimintakykyyn on siis vahva. Se on sikäli ymmärrettävää, että yrityskohtaisten tietojärjestelmien suunnittelu, toteutus ja ylläpito ovat erityisasiantuntemusta vaativia tehtäviä, jotka ainoastaan valittu yhteistyökumppani tuntee. Vaihtoehtoisen toimittajan hyödyntäminen kriisitilanteessa edellyttäisi syvällistä ja jatkuvaa yhteistyötä myös ennen kriisiä, mikä kuluttaisi paljon resursseja. Lisäksi sopimukset päätoimittajan kanssa saattavat estää yhteistyön muiden saman alan toimittajien kanssa.

Kaksi yritystä mainitsi miettineensä vaihtoehtoja erilaisten materiaalitoimittajien osalta. Toisessa varatoimittajaa lähdetään ilmeisesti etsimään vasta siinä tapauksessa, että päätoimittajalla ilmenee ongelmia. Puutteita pystytään tällä tavalla reagoiden jonkin verran paikkaamaan, mutta tarvittavat volyymit ovat niin isoja, ettei normaalikapasiteettia kuitenkaan saavuteta. Materiaalipulaa todennäköisesti siis syntyy ja täydellinen ehtyminenkin on mahdollista, mikäli uutta toimittajaa ei nopeasti löydetä.

Toinen organisaatio on omaksunut huomattavasti strategisemman ja proaktiivisemman lähestymistavan ja käyttää saman materiaalin hankkimiseen aina vähintään kahta eri toimittajaa. Lisäksi on huomioitu toimittajien maantieteellinen sijainti. Tämä parantaa yrityksen joustavuutta merkittävästi.

> *Varsinkin tietyissä materiaaleissa on pyritty menemään tietoisesti ulkomaille. Että jos maan sisällä tulee esim. lakkoja, niin se ei vaikuta siihen.*
> (Järjestelmäpäällikkö, tuotantoala)

4.3.5 Ylläpito

Jatkuvuudenhallinta on jatkuva prosessi, joten siihen tulisi sisältyä toistuvaa uudelleenarviointia, tarkastuksia ja testaamista, eli toisin sanoen ylläpitoa. Tehokkaan toipumisen ja joustavuuden säilyttämisen edellytys on, että jatkuvuussuunnitelma on ajantasainen ja

perustuu todellisiin uhkakuviin, haavoittuvuuksiin ja yrityksen nykyiseen toimintaan. Organisaatio, jolle jatkuvuuden turvaaminen on pitkän aikavälin tavoite ja joka pyrkii säilyttämään saavuttamaansa arvoa ja kilpailuetua, tunnistaa myös suunnitelmien toimivuuden tärkeyden ja siten ylläpidon oleellisuuden. Jatkuvuudenhallinnan strategisuudesta on havaittavissa merkkejä, mikäli esimerkiksi yrityksen toimintaohjeet edellyttävät suunnitelmien säännöllistä päivitystä tai niiden ajantasaisuuden valvonta on annettu nimettyjen henkilöiden tehtäväksi. Tällaiset toimintatavat edistävät myös jatkuvuusajattelun sulautumista yritykseen, koska ne sitouttavat henkilöstöä ja viestivät siitä, ettei jatkuvuudenhallinta ole ainoastaan kertaluontoinen asia (Herbane ym. 2004, 447).

Finanssivalvonnan standardi edellyttää pankki- ja vakuutusalan yrityksiä määrittämään suunnitelmien ylläpidolle vastuuhenkilöt sekä päivittämään, testaamaan ja harjoittelemaan suunnitelmia (Standardi 4.4b 2010, 23). Se näkyy myös käytännössä, sillä aineiston perusteella pankki- ja vakuutusalan yritysten ylläpitokäytännöt ovat selvästi organisoiduimmat ja säännöllisimmät. Niiden kaikkien sisäisistä ohjesäännöistä löytyy mainintoja sekä suunnitelman päivittämisestä että testaamisesta, minkä vuoksi ne kykenivät antamaan tarkimmat vastaukset esimerkiksi päivitysten säännöllisyydestä. Kun suunnitelmien ylläpito on sidottu virallisesti organisaation toimintatapoihin ja sitä vaaditaan työntekijöiltä, edistää se tietoisuutta jatkuvuudenhallinnan olemassa olosta sekä sitoutumista sen periaatteisiin.

> *Vaatimuksena on testata kerran vuodessa ja se sisältyy valvontaan. Kuten mainitsin, me tuemme yksiköitä testaamalla jatkuvuussuunnitelmia ja valvomalla niiden tilaa. Seuraamalla suunnitelman tilaa, tiedämme, onko sitä testattu vai ei. Ja se sisältyy johdon raportteihin.*
> (Riskienhallintajohtaja, pankki- ja vakuutusala)

Pankki- ja vakuutusalalla suunnitelmien päivitystiheys vaihtelee vuodesta kahteen. Alalla on yleistä, että suunnitelmat laaditaan yksiköittäin tai divisioonittain ja siksi niitä voidaan myös päivittää tai testata osissa. Tarvittaessa päivityksiä tehdään useamminkin. Esimerkiksi eräässä yrityksessä PR- ja avainhenkilösuunnitelmat käydään läpi ”silloin tällöin”. Palvelu- ja tuotantoaloilla suunnitelmien päivittäminen ei vaikuttaisi olevan yhtä selkeästi sisäisillä säädöksillä määrätty. Toisaalta kaikista yrityksistä ei saatu selvää kuvaa päivityskäytäntöjen osalta. Ylläpitovastuita on saatettu määritellä, mutta esimerkiksi päivitysten säännöllisyys jäi hämäräksi.

Kaikki pankki- ja vakuutusalan yritykset kertoivat testaavansa suunnitelmiaan ainakin osittain. Koko suunnitelmaa ei siis välttämättä testata, mutta liiketoiminnallisia osia on kuitenkin mukana. Testausta tehdään alalla yleisesti kerran vuodessa. Muillakin aloilla suunnitelmia testataan, mutta se keskittyy yhtä yritystä lukuun ottamatta selvästi enemmän IT-puoleen, kuten tiedonvarmennuksen toimivuuteen ja toipumissuunnitel-

maan. Tiedonvarmennusta testaa toisaalta säännöllisesti myös eräs tuotantoalan yritys, jolla ei ole jatkuvuussuunnitelmaa ja jonka jatkuvuudenhallinta on muiltakin osin hyvin rajoittunutta. Tiedonvarmennus ja sen toimivuus ovat ilmeisesti yritysten ensimmäisiä askelia kohti yrityksen turvatumpaa jatkuvuutta. Tiedon saatavuus on niin keskeistä, että sitä suojellaan, vaikka liiketoiminnallisia riskejä ei olisikaan suuremmin pohdittu.

4.3.6 Yhteenveto

Jatkuvuussuunnitelman olemassa olo voi vaikuttaa yrityksen toipumisnopeuteen ja kilpailukykyyn (Herbane ym. 2004 440). Suunnitelma löytyykin useimmista yrityksistä, mutta sen sisältö vaihtelee merkittävästi yrityksittäin. Parhaimmillaan se on liiketoimintalähtöinen ja poikkitoiminnallinen, mutta heikoimmillaan ulkoisten ajureiden ehdoilla luotu, IT-keskeinen tuotos, joka ei aidosti vaikuta yrityksen pitkän tähtäimen tavoitteiden saavuttamiseen. Havaintojen perusteella liiketoimintalähtöisyys johtaa usein suunnitelmien parempaan tietoperustaan, eli ne luodaan tarkemman ja realistisemman informaation pohjalta, esimerkiksi riskianalyyseihin perustuen ja strategisia työkaluja käyttäen. Työkalujen käyttö on sitä yleisempää, mitä suurempi yritys on kyseessä.

Tapausyritysten jatkuvuussuunnitelmat jakautuvat yleisesti liiketoiminnalliseen osaan ja IT-osaan, mikä on Herbanen ym. (2004, 445) mukaan positiivinen merkki jatkuvuudenhallinnan poikkitoiminnallisesta roolista. IT-infrastruktuurinsa itse hoitavat yritykset painottavat kuitenkin selvästi enemmän IT-ulottuvuutta tai vahinkoriskejä, mikä taas ei edusta strategista ajattelua (Herbane 2004, 446).

Yritykset eivät toimi eristyksissä ympäröivästä maailmasta, joten toimitusketjun kriisit voivat vaikuttaa yrityksen toimintakykyyn (Herbane ym. 2004, 441). Toimitusketjujen merkitys jatkuvuudelle on tunnistettu hyvin, sillä kaikki yritykset huomioivat enemmän tai vähemmän myös jatkuvuuteensa vaikuttavia ulkoisia tekijöitä. Ulkoisten riskien hallinnassa käytetään esimerkiksi palvelutaso-, tietoturva- ja jatkuvuussuunnitelmavaatimuksia. Yritykset eivät kuitenkaan ole määrittäneet IT-palvelujensa toimittajille varavaihtoehtoja, joten toimittajan ongelmat heijastuvat heti myös asiakasyrityksen toimintaan.

Suunnitelmien käyttökelpoisuus edellyttää säännöllistä ylläpitoa, minkä pankki- ja vakuutusalan yritykset ovat tiedostaneet selvästi parhaiten. Niiden päivityskäytännöt ovat muita aloja säännöllisemmät ja organisoidummat. Muilla aloilla ylläpito saattaa olla olematonta tai keskittyä IT-tekijöihin, kuten tiedonvarmennukseen. Ylläpitovaatimukset ja -käytännöt ovat viestintäkeino ja samalla osoitus jatkuvuudenhallinnan virallisesta roolista. Ne edistävät jatkuvuudenhallinnan sulautumista sekä henkilöstön sitoutumista (Herbane 2004, 442, 447).

4.4 Viestintä ja rakenne

Turnerin (1994, 217) mukaan viestintäjärjestelmien ongelmat ovat osasyynä käytännössä kaikkiin liiketoiminnan häiriöihin. Neljäs teema käsitteleekin jatkuvuudenhallinnan viestintään liittyviä kysymyksiä ja ottaa mukaan myös organisaatiorakenteellisia asioita, koska ne ovat yksi tapa ilmentää jatkuvuudenhallinnan roolia. Jatkuvuudenhallinnan juurtuminen organisaatiokulttuuriin ja sulautuminen ajattelu- ja toimintatapoihin vaatii, että ihmiset ovat tietoisia sen olemassa olosta. Sulautuminen taas edistää yrityksen häiriöttömyyttä ja kykyä toimia kriiseissä (Devargas 1999, 44).

Mikäli johto näkee jatkuvuudenhallinnan strategisena voimavarana, tulee sen pyrkiä tuomaan sitä esiin myös yrityksen viestinnässä. Viestintä pyrkii vahvistamaan käsitystä, jonka mukaan vakaa ja turvallinen toimintaympäristö on kaikkien etu ja tukee yrityksen arvon säilymistä pitkällä aikavälillä (Devargas 1999, 44). Kommunikoinnin tulisi olla jatkuvaa, monimuotoista ja vastaanottajien mukaan räätälöityä, jotta omaksuminen olisi mahdollisimman tehokasta. Se edistää henkilöstön tietoisuutta ja osaamista ja parhaimmillaan sitouttaa heitä yrityksen tavoitteisiin. Viestintä on siis merkittävä osoitus siitä, missä määrin johto pitää jatkuvuudenhallintaa jatkuvana prosessina (Herbane ym. 2004, 447).

4.4.1 Mistä viestitään ja kenelle?

Haastatteluaineiston perusteella organisaatiot, jotka ovat luoneet kirjallisen jatkuvuussuunnitelman, myös viestivät siitä sisäisesti. Viestinnän kohderyhmät ja säännöllisyys kuitenkin vaihtelevat merkittävästi eri yrityksissä. Erityisesti palvelualan yritykset mainitsivat puutteista viestinnässään. Se ei välttämättä ole jatkuvaa tai ulotu edes kaikkiin suunnitelmaan liittyviin henkilöihin. Eräässä yrityksessä jatkuvuussuunnitelmasta viestitään vain asiakasrajapinnan työntekijöille, mikä ei anna kuvaa pyrkimyksestä yrityksen kokonaisarvon säilyttämiseen. Tämä mielikuva hankaloittaa jatkuvuusajattelutavan laajempaa omaksumista.

> *Niistä (jatkuvuus- ja toipumissuunnitelmista) ei ole viestitty kovinkaan hyvin, mutta ne ovat olemassa osastoilla ja me pyrimme viestimään niistä liiketoimintahenkilöstön ja prosessien vastuuhenkilöiden avulla.*
> (Tietoturvapäällikkö, palveluala)

Viestinnän kohderyhmät siis vaihtelevat, mutta yleisintä vaikuttaisi haastattelujen perusteella olevan, että ainakin tärkeimmät, eli jatkuvuudenhallinnan suunnittelusta ja kriisitilanteista vastaavat henkilöt tuntevat suunnitelman. Parhaassa tapauksessa kriisi-

vastuulliset ovat myös suunnitelman laatijoita eli tämä tapahtuu melko luonnollisesti. Devargasin (1999, 44) mukaan vastuu vakaasta ja turvallisesta ympäristöstä sekä kriiseissä toimimisesta on loppujen lopuksi kaikilla, joten kaikkien tulisi olla siitä myös tietoisia. Suunnitelma saattaa olla kaikkien halukkaiden saatavilla esimerkiksi intranetissä, mutta pakon saneleman kiinnostuksen puuttuessa siihen ei vapaaehtoisesti tutustuta. Vaikuttaisi siltä, että haastatelluissa yrityksissä jatkuvuudenhallinnasta viestitään melko passiivisesti lukuun ottamatta avainhenkilöille tapahtuvaa viestintää. Jatkuvuudenhallinta ei sulaudu automaattisesti koko yrityksen toimintatapoihin ja ajatteluun, joten sen viestintään tulisi kiinnittää erityistä huomiota.

> *…kuten sanottu, liiketoimintapuolen ihmiset eivät ole kiinnostuneita toipumissuunnitelmista, mutta heitä kyllä kiinnostaa häiriöttömät liiketoiminnot. Jotta tämä toteutuisi, tarvittaisiin yhteistyötä ja liiketoiminnan tarpeiden selkeyttä IT-tasolla. Näin ei kuitenkaan kokonaisuudessaan ole tapahtunut.*
> (Tietoturvapäällikkö, palveluala)

Jatkuvuussuunnitelmasta viestiminen koko organisaatiolle vaikuttaa olevan harvinaista, mutta tietoturva-asioista tiedotetaan sitäkin enemmän. Nekin organisaatiot, jotka eivät ole laatineet erityistä jatkuvuussuunnitelmaa, ovat luoneet tietoturvaohjeistuksia, joiden sisältö pyritään tekemään henkilöstölle tutuksi. Kaikki yritykset kertoivat viestivänsä henkilöstölleen jollakin tavoin esimerkiksi siitä, mitkä ovat turvallisen Internetin käytön periaatteet ja miten tiedonvarmennus on toteutettu.

> *Niin siellä on kerrottu ihan tällaisia IT-puolen asioita, että meillä otetaan turvakopioita niin ja näin ja niitä pyöritellään sillä ja tällä lailla ja niitä voidaan palauttaa ja tätä saa tehdä ja tuota ei saa tehdä.*
> (Palveluyritys 2:n ICT Manager)

Kokonaisuudessaan yritysten viestintää näyttää yhdistävän tietoturva ja se vaikuttaa olevan oleellisin osa yritysten jatkuvuudenhallintaa viestinnän näkökulmasta. Haastateltujen henkilöiden taustoilla saattaa olla asiaan vaikutusta, koska ne ovat tässä tutkimuksessa pääasiassa liitoksissa tietoturvaan. Vaikuttaisi kuitenkin siltä, että tuotanto- sekä pankki- ja vakuutusalan yritykset, joilla on jatkuvuussuunnitelma, pyrkivät viestimään muita yrityksiä enemmän myös muista jatkuvuutta edistävistä asioista. Esimerkiksi eräässä pankki- ja vakuutusalan yrityksessä jatkuvuudenhallinta-asioista viestitään eri tavalla eri osastoille, koska niiltä odotetaan erilaisia jatkuvuutta parantavia toimenpiteitä. Se on samalla merkki siitä, että yritys on tunnistanut IT:n ulkopuolisten toimintojen

merkityksen jatkuvuuden turvaamisessa ja käyttää tietoa hyväkseen koko organisaation edun saavuttamiseksi.

4.4.2 Viestintätavat

Organisaatiot, jotka haluavat sulattaa jatkuvuudenhallinnan osaksi jokapäiväistä toimintaansa, voivat hyödyntää monia erilaisia keinoja sen viestimisessä (Herbane ym. 2004, 447). Valitulla viestintätavalla on suuri merkitys siihen, kuinka henkilöstö saadaan motivoitua ja kuinka hyvin periaatteet omaksutaan. Mikäli henkilöstö kokee esimerkiksi tietoturvan edellyttämät toimintatavat ainoastaan taakkana, he todennäköisemmin jättävät ne toteuttamatta (Devargas 1999, 44). Tämä taas vaarantaa yrityksen joustavuuden. Siksi jatkuvuudenhallinta tulisikin perustella sen hyötyjen kautta, vaikka ne aina eivät olekaan kovin selviä tai konkreettisia.

> *Jotkut voi katsoa sen niin, että se on haitta. Tai sitten, että on erilaisia varmistustoimenpiteitä tai kulunvalvontaa ja tilanvalvonta-asioita, niin onhan se käytännön tekemisen kannalta pientä haittaa ja viivettä tulee, mutta kyllä se tehostaa sitä kokonaisuutena hyvinkin paljon. […] Kyllä se tehostaa sitä organisaation kehitystä, mutta se, että miten sen perustelisi, että näin tosiaan on, on ehkä vaikeaa.*
> (Tietohallintopäällikkö, pankki- ja vakuutusala)

Tapoja, joilla yritykset viestivät sisäisesti jatkuvuudenhallinnastaan, on haastattelujenkin perusteella hyvin monia. Selvästi yleisin viestintäkanava on yrityksen intranet, jonka kautta tietoa on saatavilla jatkuvasti. Se on helppo ja nopea, mutta toisaalta hyvin passiivinen ja yksipuolinen kommunikointitapa, jonka välityksellä tiedon perillemenosta ei voida varmistua ilman erillistä valvontaa. Yritykset luottavat voimakkaasti ihmisten omaan haluun ja kykyyn etsiä tietoa intranetistä. Mikäli sellaisia ei ole, työntekijät eivät tunne suunnitelmaa, jolloin yrityksen joustavuus ja toipumisnopeus voivat jäädä yritysjohdon olettamaa heikommaksi. Intranetin käyttö ainoana tiedotusvälineenä ei siis viesti aktiivisesta ja strategisesta jatkuvuudenhallinnasta.

> *Heidän pitäisi (tuntea jatkuvuussuunnitelma), jos he lukevat intranetiä. Mutta sitä ei tarkisteta, lukevatko he sitä vai eivät. […] Valvontaa ei ole, mutta uskon, että ne henkilöt, joiden pitäisi tietää näistä asioista, ovat lukeneet ne, koska yleensä heillä on kiinnostusta huolehtia siitä…*
> (Tietoturvajohtaja, tuotantoala)

Tarkkaa palettia haastateltujen yritysten viestintäkanavista ei aineiston rajallisuuden vuoksi pystytä muodostamaan, mutta pelkästään intranetille perustuvaa viestintäpolitiikkaa ei ole havaittavissa missään yrityksessä. Muita tavattuja viestintätapoja ovat esimerkiksi luennot, palaverit, henkilökohtaiset perehdytykset ja sähköposti. Myös jatkuvuuteen ja sen edistämiseen sidotut kannustinjärjestelmät ohjaavat ajattelua haluttuun suuntaan. Lisäksi kappaleessa 4.3.5 käsitellyt suunnitelman ylläpitometodit, kuten testaus, päivitys ja tarkastaminen, ovat keinoja viestiä jatkuvuudenhallinnan olemassa olosta ja merkityksestä. Kun huomioidaan tämä suunnitelman ylläpidon viestinnällinen vaikutus, on pankki- ja vakuutusyritysten viestintä verrattain hyvää. Muutama yritys mainitsi työsopimuksen sisältävän tietoturvavaatimuksia ja eräässä tuotantoyrityksessä esimieheksi pääseminen edellyttää johtamiskurssin tietoturvakoulutusta. Myös ne voidaan laskea viestintäkanaviksi.

Jokaista edellä mainittua viestintätapaa havaittiin useammassakin yrityksessä, mutta eräs tuotantoalan yritys on omaksunut lisäksi aivan omanlaisensa tavan kommunikoida. Sillä on käytössään eräänlainen jatkuvuudenhallintafoorumi, joka kokoaa kuukausittain ihmisiä keskustelemaan aiheesta ja kehittämään jatkuvuutta edistävää toimintaa. Foorumeihin osallistuvat kaikki, jotka liittyvät yrityksen jatkuvuudenhallintaan. Tämä on säännöllisyydeltään ja muodollisuudeltaan hyvin poikkeuksellinen viestintätapa ja huomattava osoitus jatkuvuudenhallinnan tärkeästä roolista kyseisen yrityksen liiketoiminnalle.

Työntekijöiden tulisi siis olla tietoisia turvalliseen ja vakaaseen liiketoimintaan liittyvistä vastuistaan, mutta kaikkiin työtehtäviin kuuluvat vastuut eivät ole samanlaisia (Devargas 1999, 45). Varastomieltä edellytetään eri asioita kuin toimistotyöntekijältä. Herbanen ym. (2004, 447) tutkimuksesta käy ilmi, että viestinnän räätälöinti kohderyhmän mukaan saattaa parantaa viestinnän tehokkuutta. Esimerkiksi erilaisten prosessien, osastojen ja yrityksen alakulttuurien tarpeiden kartoittaminen ja niiden huomiointi kommunikoinnissa voi edistää välitetyn viestin omaksumista (Herbane ym. 2004, 447).

Haastatteluaineiston suppeuden vuoksi viestintäänsä räätälöivien ja räätälöimättömien yritysten lukumääriä ei voida määritellä tarkasti. Vaikuttaisi kuitenkin siltä, että viestinnän muokkaaminen kohderyhmille sopivaksi on melko harvinaista. Esimerkiksi intranetviestinnän helppous houkuttelee syöttämään kaikille käyttäjille saman viestin ja unohtamaan omaksumisen tehokkuuteen liittyvät kysymykset.

Oletettavasti lähiesimieheltä saatu viesti hyväksytään ja omaksutaan etäiseltä tuntuvan ylimmän johdon viestejä paremmin. Tämä on huomioitu useassa yrityksessä siten, että alemman tason esimiehet pitävät alaisilleen palavereja ja luentoja jatkuvuudenhallinta-asioista. Neljä yritystä mainitsi erikseen viestivänsä tällä tavoin, mutta on mahdollista, että se on myös yleisempää. Kuitenkin ainoastaan yksi haastatelluista yrityksistä osoitti selvästi muokkaavansa viestintää kohderyhmittäin.

> *Kuten tästä nähdään, suunnitelmat eivät ole samanlaisia. Jokainen yksikkö tekee oman suunnitelmansa ja niistä tulee myös viestiä eri tavoin. Esimerkiksi viestintäjohtajalla on täysin erilainen asenne, koska hän hoitaa julkisia suhteita ja vastaa toimittajien kysymyksiin. Mutta sitten esimerkiksi meillä IT:ssä on erilainen strategia.*
> (IT-palvelupäällikkö, pankki- ja vakuutusala)

Oli jatkuvuudenhallinnan viestintä minkä muotoista tahansa, sen tavoitteena on yleensä vaikuttaa ihmisten käyttäytymiseen ja toimintatapoihin riskejä ehkäisevästi. Ohjeistusten ja vaatimusten siirtäminen käytäntöön saattaa tehostua toiminnan valvonnalla, joka on samalla selvä viesti siitä, että yritys on tosissaan jatkuvuutta edistävien toimintatapojensa kanssa. Huolimatta sen mahdollisista positiivisista vaikutuksista, jatkuvuudenhallinnan käytännön toteutumista valvotaan kuitenkin haastattelujen perusteella vaihtelevasti tai epäorganisoidusti. Valvontavastuu on ehkä annettu esimiehelle, mutta tarkemmat toimenpiteet ja mittauskohteet on saatettu jättää määrittelemättä. Jatkuvuussuunnittelu ja tavoitteiden määrittely eivät siis automaattisesti johda toiminnan valvontaan ja tulosten seurantaan. Tämä vaikeuttaa jatkuvuudenhallinnalla saavutettujen hyötyjen havaitsemista.

Viidessä yrityksessä todettiin olevan jonkinlaista jatkuvuudenhallinnan toteutumisen valvontaa, mutta vain kolme niistä mainitsi valvovansa sitä säännöllisesti. Kyseisissä yrityksissä esimies tai sisäinen valvonta tekee havainnointia yksikössä ja raportoi kaksi kertaa vuodessa ylempiin johtoportaisiin. Raportoinnin pakollisuus viestii siitä, että jatkuvuudenhallinta on pysyvä osa yrityskulttuuria ja edistää sen sulautumista.

> *Jatkuvuussuunnitelmien tekemistä valvovalle riskienhallintahenkilölle tai johdolle on myös tarkistuslista. Sitten me rastitetaan ”tämä on tehty, tämä on tarkistettu”. Eli pidämme kirjaa näistä asioista ja annamme sitten sisäisiä raportteja riskienhallinnalle ja he antavat raportin ryhmän ylimmälle johdolle.*
> (Riskienhallintajohtaja, pankki- ja vakuutusala)

Valvonnan antamaa mitattavuutta voidaan hyödyntää jatkuvuudenhallinnan tavoitteiden asetannassa ja niiden saavuttamisessa. Normaalitilanteessahan työntekijällä ei ole erityistä intressiä muuttaa toimintatapojaan yrityksen riskejä vähentäviksi, ellei hän koe itse hyötyvänsä siitä jollakin tavoin. Siksi esimerkiksi työtä hankaloittavat tietoturvatoimenpiteet saattavat unohtua helposti. Valvonnan avulla kaikille työntekijöille voidaan luoda halu ylläpitää ja kehittää mahdollisimman vakaata työympäristöä. Tavoitteiden saavuttamiseen voidaan sitoa erilaisia kannustimia, mutta samalla myös rangaistuksia. Henkilöstön toiminnan motiivina ei näin ollen välttämättä ole toiminnan häiriöttö-

myys, mutta yrityksen jatkuvuuden kannalta on tärkeintä, että riskit pienenevät. Kannustinjärjestelmät viestivät vahvasti pyrkimyksestä häiriöttömyyteen, mutta rangaistukset saattavat aiheuttaa työntekijöille myös pakottamisen tunnetta, joka voi aiheuttaa negatiivisia vastareaktioita.

Henkilökohtaiset kannustimet pyrkivät sitouttamaan ihmisiä yrityksen tavoitteisiin, mutta niiden käyttö nimenomaan jatkuvuudenhallinta-asioissa on haastatteluaineiston perusteella hyvin harvinaista. Ainoastaan yksi organisaatio kertoi selvästi käyttävänsä niitä pyrkiessään liiketoiminnan jatkuvuuteen. Kyseinen tuotantoalan yritys kertoi toimintansa perustuvan muutenkin kannustimien käyttöön ja totesi niistä olevan hyötyä johtamisessa. Yksi pankki- ja vakuutusalan yritys mainitsi käyttävänsä riskienhallinnalle divisioonatasoisia kannustimia. Eräs toinen tuotantoalan yritys kertoi puolestaan vaikeuksista luoda oikeanlaisia mittareita ja kannustimia:

> *Emme käytä keppiä ja porkkanaa. Olen miettinyt sitä henkilökohtaisesti paljon, mutta sen implementoinnissa on ongelmia. Sen toteuttamiseksi ei ole helppoa tapaa. Mikä on hyvä porkkana ja mitä sinun tulee tehdä saadaksesi sen? Entä keppi? Hyvä keppi toimii, mutta se on hyvin vaikea kysymys ja haluaisin nähdä sen tietoturvajohtajan, joka on implementoinut sen. Sitä käytettäessä tulee ongelmia. Luulen, että keppi on loppujen lopuksi jossain määrin parempi kuin porkkana. Ei paljon. Sitä pitää käyttää varoen.*
> (Tietoturvajohtaja, tuotantoala)

Kannustinjärjestelmät itsessään eivät ole vieras asia yritysmaailmassa, mutta haastattelussa kysyttiin niiden käyttöä nimenomaan liiketoiminnan jatkuvuuteen liittyvissä asioissa. Laajemmin ajateltuna liiketoiminnan jatkuvuus riippuu toki esimerkiksi kilpailukyvyn ylläpitämisestä, jonka näkökulmasta tulospohjaiset kannustimet ovat myös jatkuvuudenhallinnallisia kannustimia. Tämän tutkimuksen kannustinkysymyksellä viitattiin kuitenkin pyrkimykseen ohjata yksittäisten ihmisten käyttäytymistä vahinkoriskejä ehkäisevään suuntaan, joten liiketoiminnalliseen tulokseen perustuvat kannustimet eivät nousseet tässä yhteydessä esille.

4.4.3 Virallinen asema

Herbane ym. (2004, 447) toteavat, että jatkuvuudenhallinnan näkyminen selvissä, virallisissa organisaatiorakenteisissa viestii strategisemmasta ja poikkitoiminnallisesta suhtautumisesta jatkuvuuden ylläpitoon. Virallisen aseman puuttuminen viittaa puolestaan jäykkään ja toimintopainotteiseen toipumissuunnitteluun (Herbane ym. 2004, 445). Sel-

vä rooli yrityksen hierarkiassa sekä ylemmän johdon asettamat raportointivaatimukset edistävät luonnollisesti jatkuvuudenhallintaa sulautumaan yritykseen ja henkilöstön toimintatapoihin.

Haastatelluista yrityksistä yhdeksällä on dokumentoitu jatkuvuussuunnitelma, mutta itse prosessilla ja ideologialla ei ole välttämättä niissäkään muodollista asemaa. Esimerkiksi erään palveluyrityksen tapauksessa jatkuvuussuunnitelma on kyllä laadittu, mutta tarkoituksena on ollut ilmeisesti enemmänkin tyydyttää asiakkaiden tarpeita kuin pyrkiä sisäistämään jatkuvuudenhallinnan periaatteita. Suurimmassa osassa suunnitelman laatineista organisaatioista on kuitenkin tunnistettavissa selkeitä merkkejä jatkuvuudenhallinnan virallisesta roolista. Tämä virallisuus ilmenee esimerkiksi jatkuvuudenhallintatiimien ja koordinaattoreiden olemassa olona, jatkuvuuteen tähtäävän toiminnan valvontana sekä ylimmältä johdolta annettuina raportointi-, suunnittelu- ja ylläpitovelvoitteina.

Kappaleessa 4.1.3 todettiin, että suurin osa yrityksistä on määritellyt erilaisia kriisienhallintatiimejä, mutta proaktiivisesti riskejä ehkäisevät jatkuvuus- tai riskienhallintatiimit ovat harvinaisempia. Seitsemän organisaatiota on määritellyt etukäteen erityisen ryhmän, joka osallistuu kriisienhallintaan joko itsenäisesti tai tarvittavien asiantuntijoiden ja johtajien avustamana. Riskien havaitsemiseen ja välttämiseen tähtääviä jatkuvuustiimejä ei löydetty kuitenkaan kuin pankki- ja vakuutusalan yrityksistä sekä yhdestä palvelualan yrityksestä. Niiden olemassa olo on virallinen osoitus yrityksen pyrkimyksestä kilpailukykyiseen joustavuuteen.

Jatkuvuussuunnitteluvastuun siirtäminen yrityksen alempiin osiin on tapa viestiä jatkuvuudenhallinnan virallisesta asemasta organisaatiossa. Kappaleessa 4.1.1 tuli esille, että vastuuta on siroteltu ylimmän johdon ulkopuolelle erityisesti suuremmissa, vähintään tuhannen työntekijän yrityksissä. Kun suunnittelua tehdään säännöllisesti eri yksiköissä, tulee jatkuvuudenhallinnasta automaattisesti viestittyä paljon useammille kuin jos sen toteuttaisi ainoastaan ylin johto tai erillinen jatkuvuustiimi. Tämä myötävaikuttaa jatkuvuudenhallinnan sulautumiseen.

Alemmille organisaatiotasoille siirrettyyn suunnitteluvastuuseen liitetään aineiston perusteella usein myös raportointivelvoitteita, jotka korostavat jatkuvuudenhallinnan prosessiluonnetta ja muodollista asemaa. Raportointi on liitoksissa myös valvontaan, jota harjoittavissa yrityksissä se on yleistä. Säännöllinen informointi on luonnollinen osa sekä suunnittelua että valvontaa, koska organisaation ylempien tasojen tulee olla tietoisia suunnittelun ja valvonnan edistymisestä ja niiden tuloksista. Ilman raportointia nämä toiminnot vaikuttaisivat turhilta.

> *…eli liiketoimintayksiköillä on tavallaan itsellään se jatkuvuudenhallintavastuu ja ylin johto johtaa sitä. Meillä on tavallaan kokonaisjatkuvuudenhallinta. Luulen, että yksiköt raportoivat jatkuvuudenhallinta-asioista jatkuvasti ylimmälle johdolle.*

(Tietoturvajohtaja, tuotantoala)

Kuten kappaleessa 4.3.5 todetaan, tulevat ylläpitovaatimukset esiin erityisesti pankki- ja vakuutusalalla, jonka kaikissa haastatelluissa yrityksissä suunnitelmat tarkistetaan ja päivitetään säännöllisesti. Päivityskäsky saattaa tulla erikseen ylimmästä johdosta tai se voi olla kirjattuna yrityksen virallisiin toimintaperiaatteisiin. Lisäksi suunnitelmien sisältöä ja ajantasaisuutta valvotaan säännöllisin väliajoin. Jatkuvuudenhallinta ei siis ole vain kertaluontoisesti tehty suunnitelma turvakaapissa tai esimiehille annettu suositus toimia riskejä ehkäisevästi, vaan se edellyttää myös säännöllisiä ja näkyviä toimia.

> *…päivitys tehdään säännöllisesti. Toimitusjohtaja viestii, että nyt on jälleen aika päivittää suunnitelma.*
> (IT-palvelupäällikkö, pankki- ja vakuutusala)

Eräs tuotantoalan yritys on vienyt jatkuvuudenhallinnan selvästi muita virallisemmalle tasolle. Se on kehittänyt itselleen jatkuvuudenhallinnan kypsyysmallin, jota sovelletaan koko yritykseen. Se on viisiportainen malli, jonka avulla kyetään näkemään kunkin prosessin jatkuvuudenhallinnan tila. Portaikko alkaa liiketoiminnallisesta vaikutusanalyysistä, jonka avulla määritellään, onko kyseinen prosessi kriittinen. Kriittiseksi määritellyille prosesseille seuraavat pakollisina suunnittelun, toteutuksen, viestinnän ja kriisienhallinnan askelmat. Mikäli prosessi määritellään kriittiseksi, vaatii se siis paljon jatkotoimenpiteitä. Ei-kriittisten prosessien ei tarvitse huolehtia jatkuvuudenhallinnastaan samalla tavoin. Tämän kaltainen jatkuvuudenhallinnan muodollinen asema oli haastattelujen perusteella poikkeuksellista. Se viittaa siihen, että jatkuvuudella on hyvin merkittävä rooli yrityksen strategiassa ja tavoitteiden saavuttamisessa.

4.4.4 Yhteenveto

Viestintä on tärkeä tekijä henkilöstön sitouttamisessa ja jatkuvuudenhallintaprosessien sulautumisessa (Herbane ym. 2004 447). Havaintojen perusteella jatkuvuussuunnitelmista viestitään, mutta viestinnän sisältö, säännöllisyys ja kohderyhmät voivat vaihdella merkittävästi yrityksittäin. Tietoturva-asiat on koettu tärkeäksi kaikissa yrityksissä, sillä niistä kommunikoidaan paljon myös niissä organisaatioissa, joissa ei ole luotu jatkuvuussuunnitelmaa.

Viestintäkeinoista yleisin on intranet, mutta muita havaittuja ovat esimerkiksi luennot, palaverit, sähköposti, henkilökohtaiset perehdytykset ja kannustinjärjestelmät. Myös johdon asettamat ylläpitovaatimukset voidaan mieltää viestinnäksi, sillä ne pakottavat pohtimaan jatkuvuudenhallintaa myös organisaation muissa osissa. Jatkuvuuden-

hallintafoorumin hyödyntäminen on poikkeuksellinen ja uudenlainen tapa viestiä, sillä sellainen todettiin olevan vain yhdessä organisaatiossa.

Virallisen aseman puuttuminen viittaa siihen, ettei jatkuvuudenhallintaa koeta organisaatiossa strategisena tekijänä (Herbane ym. 2004, 447). Jatkuvuussuunnitelman olemassa olo on kuitenkin usein merkki siitä, että jatkuvuudenhallinta sisältyy jollakin tavoin organisaation virallisiin rakenteisiin. Osoituksia jatkuvuudenhallinnan virallisuudesta ovat esimerkiksi erilaiset tiimit, koordinaattorit, valvonta sekä raportointi-, suunnittelu- ja ylläpitovelvoitteet. Kriisienhallintatiimien määrittäminen on yleistä, mutta riskejä ennaltaehkäiseviä tiimejä ei havaittu kuin neljässä yrityksessä, joista kolme pankki- ja vakuutusalalta. Poikkeuksellinen osoitus jatkuvuudenhallinnan virallisesta asemasta oli erään tuotantoalan yrityksen kypsyysmalli, jota sovelletaan organisaation kaikkiin yksiköihin.

Valvonnalla voidaan vaikuttaa henkilöstön sitoutumiseen ja asenteisiin sekä prosessin tuloksiin (Herbane ym. 2004, 447). Jatkuvuudenhallinnan valvonta vaikuttaa olevan melko harvinaista, mikä vaikeuttaa saavutettujen hyötyjen arviointia. Valvonnan vähäisyys on vaikuttanut todennäköisesti myös siihen, ettei jatkuvuudenhallintaan sidottuja kannustimia juuri käytetä. Jatkuvuudenhallinnan valvonta on liitoksissa raportointiin, joka taas vaikuttaa olevan jossain määrin riippuvaista vastuiden jakautumisesta. Suuremmissa yrityksissä vastuuta on jaettu alemmille organisaatiotasoille ja samalla on annettu myös raportointivelvoitteita.

4.5 Asenteet ja sitoutuminen

Työntekijöiden ja yritysjohdon asenne jatkuvuudenhallintaa kohtaan vaikuttaa merkittävästi heidän sitoutumiseensa ja siten ajattelutavan omaksumiseen sekä yrityksen joustavuuteen ja toipumisnopeuteen. Mikäli jatkuvuudenhallintaa pidetään yrityksen strategian kannalta merkityksettömänä tai työntekijät eivät näe sitä hyödyllisenä itselleen, ovat edellytykset sen menestyksekkäälle toteuttamiselle huonot. Tutkimuksen viides teema pyrkii kartoittamaan jatkuvuudenhallintaan liittyviä asenteita ja sitoutumista yritysten ja henkilöstön keskuudessa tutkimalla esimerkiksi toiminnan motiiveja ja havaittuja hyötyjä. Se on jatkuvuudenhallinnan strategisen roolin kannalta kenties teemoista tärkein, sillä ilman myönteistä suhtautumista ja avainhenkilöiden sitoutumista jatkuvuudenhallintaprosessi epäonnistuu lähes varmasti (Seow 2009, 201).

4.5.1 Motiivit ja lainsäädäntö

Syy siihen, että yrityksen jatkuvuutta ja sen edellytyksiä on ryhdytty alun perin organisoidusti johtamaan, on hyvin yrityskohtainen. Osalle tarve on noussut sisäisesti liiketoiminnan tarpeiden kautta, toisille taas ulkoisesti esimerkiksi asiakkaiden, valvontaviranomaisen tai lainsäädännön vaatimuksesta. Lainsäädännön eroavaisuudet alojen välillä vaikuttavatkin merkittävästi yritysten jatkuvuudenhallinnan laajuuteen. Haastattelujen perusteella pankki- ja vakuutusala on ehdottomasti tiukimman säännöstelyn kohteena, mutta myös yhtä palvelualan sekä yhtä tuotantoalan yritystä koskee erityislainsäädäntö, joka edellyttää huomattavasti normaalia parempaa tietoturvaa.

Tiukka lainsäädäntö ei kuitenkaan tarkoita sitä, että pakollisuus olisi välttämättä suurin syy yrityksen jatkuvuudenhallinnalle. Herbanen ym. (2004, 448) tutkimuksesta ilmenee, että vaikka alkuperäinen peruste olisikin ollut lainsäädäntö, voivat motiivit muuttua ajan myötä liiketoimintalähtöisemmiksi esimerkiksi strategian tai kriittisten prosessien vaatimusten vuoksi. Samansuuntainen näkemys nousi esiin erityisesti eräässä pankki- ja vakuutusalan yrityksessä:

> *Kun alamme puhua jatkuvuussuunnitelmasta ja jatkuvuudenhallinnasta, aloitamme aina liiketoiminnan näkökulmasta – perustuen liiketoiminnan, ei Finanssivalvonnan, vaatimuksiin. […] Jos emme tekisi sitä näin, emme pärjäisi liiketoiminnassa. Eli totta kai Finanssivalvonnan vaatimukset ovat tärkeitä, mutta tärkeintä on liiketoiminnan jatkuvuus.*
> (Turvallisuusjohtaja, pankki- ja vakuutusala)

Muissa pankki- ja vakuutusalan yrityksissä ei ollut havaittavissa samantyylistä lähestymistapaa ja erään yrityksen edustaja totesi, ettei määräyksiin perustuva jatkuvuudenhallinta vastaa täysin liiketoiminnan todellisia tarpeita:

> *…emme olisi tehneet joitakin asioita ellei meidän olisi ollut pakko. Säännösten noudattaminen maksaa valtavasti, joten ne yritykset, joiden ei ole pakko niitä noudattaa, pitävät toimenpiteitä järjettöminä.*
> (IT-palvelupäällikkö, pankki- ja vakuutusala)

Herbane ym. (2004, 442) toteavat, että yritykset, joille jatkuvuudenhallinta ei ole lain tai asetusten mukaan pakollista, voivat erottua edukseen omaksumalla käytäntöjä ja prosesseja muilta toimialoilta. Ne voivat siis ylittää lain asettamat minimivaatimukset ja pyrkiä parempaan arvon säilyttämiseen pitkällä tähtäimellä. Tämä vähimmäisvaatimusten ylittäminen viestii strategisemmasta toimintamallista, koska se on luonteeltaan vapaaehtoista ja viittaa jatkuvuudenhallinnan tiedostettuun merkitykseen yrityksen strate-

gisten tavoitteiden saavuttamisessa (Herbane ym. 2004, 441). Jatkuvuudenhallinnan hyödyntäminen nimenomaan yrityksen omien tarpeiden tyydyttämiseen on tärkeää, sillä strateginen jatkuvuudenhallinta ei ole olemassa ulkoisia toimijoita, vaan yritystä itseään varten.

Haastattelujen perusteella pankki- ja vakuutusala on toimialoista ainoa, jossa jatkuvuudenhallinnalle on asetettu suoria vaatimuksia. Muillakin aloilla velvoitteita saattaa satunnaisesti esiintyä, mikäli esimerkiksi Huoltovarmuuskeskus on määritellyt organisaation kriittiseksi valtion infrastruktuurin kannalta tai liiketoiminta edellyttää erityistä tietosuojaa. Haastatelluista pankki- ja vakuutusalan ulkopuolisista yrityksistä kaksi mainitsi joutuvansa kiinnittämään erityishuomiota tietosuojaan, mutta muilla yrityksillä erityisvaatimuksia ei ole. Niillä olisi siis halutessaan melko helppo työ kehittää jatkuvuudenhallintaansa minimiedellytyksiä paremmiksi, mikä olisi erinomainen osoitus sitoutumisesta liiketoiminnan jatkuvuuden parantamiseen.

Aineiston perusteella jatkuvuudenhallintaan liittyvät lain minimivaatimukset ylitetään sitä todennäköisemmin mitä suurempi yritys on. Pankki- ja vakuutusalan ulkopuolisista, alle tuhannen työntekijän yrityksistä yksikään ei mielestään panosta jatkuvuuteen lain vaatimuksia enempää. Yli tuhannen työntekijän yrityksissä määräyksiä noudatetaan – tai ainakin uskotaan noudatettavan – minimivaatimuksia paremmin vähintään osittain.

Selittävä tekijä sille, miksi pienemmät yritykset näyttävät toteuttavan jatkuvuudenhallintaa matalammalla tasolla, saattaa olla juuri yrityksen koko ja saatavilla olevat resurssit. Tämä näkemys tuli esille myös haastatteluissa, joissa erään suuremman palveluyrityksen talousjohtaja luonnehti oman yrityksensä tietoturvaa seuraavasti:

> *Emme me nyt minimitasolla mene. Että ehkä voisi sanoa, että varmasti toimialalla olemme keskitasossa vähintään ja se tietysti on sidoksissa siihen, että miten iso yritys on. Että silloin on resursseja myös tällaisiin asioihin paneutua ja sitten löytyy tällaisiin myös vastuuhenkilöt. Että mitä pienempi yritys, niin sitä huonommassa hantissa sitten on, koska tietoturva ei pääsääntöisesti ole yritysten päämielenkiinnon kohteena, vaan se liiketoiminta ja sen kannattavuus on se.*
> (Talousjohtaja, palveluala)

Edellä kuvattuun talousjohtajan mielipiteeseen yhtyy täydellisesti myös havaintojoukon pienimmän yrityksen järjestelmäpäällikkö:

> *Kyllä me hyvin matalalla menemme tässä. Että lainmukainen toimintatapa monessa asiassa. Se johtuu ehkä siitä, että meidän organisaatiomme on kuitenkin niin pieni, ettei resursseja ole siihen.*
> (Järjestelmäpäällikkö, tuotantoala)

Vaikuttaisi siis siltä, että jatkuvuudenhallinnan on vaikea nousta strategiseen rooliin pienemmissä yrityksissä vähäisistä resursseista johtuen. Seow (2009, 202) valottaa artikkelissaan tätä kustannus–hyöty -ongelmaa, joka jokaisella yritysjohdolla on pohdittavanaan. Yrityksen intressinä on ensisijaisesti ydinliiketoiminnan tehokas ja tuottava toiminta eikä häiriöihin varautuminen. Johto todennäköisesti ymmärtää riskien olemassa olon ja häiriöiden mahdolliset haittavaikutukset, mutta he joutuvat priorisoimaan vaihtoehtoja rajallisten resurssien kohdistamiseksi (Seow 2009, 202). Jokapäiväiset liiketoimintaoperaatiot ajavat jonossa usein jatkuvuudenhallinnan ohi, mikäli riskitaso säilyy johdon mielestä siedettävällä tasolla.

4.5.2 Standardit

Kappaleessa 2.5 esiteltiin erityisesti jatkuvuudenhallinnalle luotuja standardeja, joista tärkeimpänä BS25999. Lisäksi mainittiin myös muita standardeja, joita noudattamalla yritys voi parantaa häiriöttömyyttään. Sertifioidut standardit kertovat sekä ulkoisille että sisäisille sidosryhmille, että yrityksen toiminta täyttää tietyllä osa-alueella vaadittavat minimikriteerit. Ne ovat samalla voimakkaita viestejä yrityksen pitkän tähtäimen sitoutumisesta jatkuvuudenhallintaan, sillä sertifikaatin säilyttäminen edellyttää jatkuvaa työtä.

Haastattelut toivat esiin, että jatkuvuudenhallintastandardien noudattaminen ja sertifioiminen on erittäin harvinaista. Vain suuri tuotantoalan yritys kertoi noudattavansa sekä BS25999-, että BS25777-standardeja ja oli samalla ainut, joka ylipäätään mainitsi kyseiset jatkuvuudenhallintastandardit. Muut organisaatiot eivät ilmeisesti käytä kyseisiä standardeja hyödykseen millään tavoin. Haastatteluaineiston perusteella nimenomaan jatkuvuudenhallintastandardien soveltaminen on hyvin riippuvaista yrityksen koosta, koska niitä käytti hyväksi ainoastaan selvästi havaintojoukon suurin yritys.

Kaikista yrityksistä yhteensä seitsemän mainitsi käyttävänsä virallisia standardeja jollakin tavoin hyväkseen. Edellä mainitun tuotantoalan yrityksen hyödyntämiä lukuun ottamatta ne eivät kuitenkaan ole erityisesti jatkuvuudenhallinnallisia, vaan esimerkiksi tietoturva- tai laatustandardeja. Pankki- ja vakuutusalan yritysten tulee noudattaa Finanssivalvonnan omaa, velvoittavaa standardia, joka kattaa operationaalisten riskien hallinnan ja huomioi esimerkiksi jatkuvuussuunnittelun ja tietoturvariskit (Standardi 4.4b 2010, 22-23, 27-33). Se selittää pitkälti, miksi pankki- ja vakuutusalan yritykset eivät korkeasta jatkuvuudenhallinnan tasostaan huolimatta noudata yleisiä standardeja.

Haastateltujen yritysten ainoat mainitut sertifioidut standardit ovat laatujohtamisen ISO 9000 -sarjan standardeja, jotka eivät ole sisällöltään yrityksen häiriöttömyyttä tai häiriöiden hallintaa parantavia. Tietoturvastandardeja ei siis ole sertifioitu missään yri-

tyksessä, mutta niiden käyttäminen toimintaohjeena on yleistä pankki- ja vakuutusalan ulkopuolella. Haastatteluissa erikseen mainittuja tietoturvastandardeja olivat ISO 27001 ja ISO 27002, mutta kaikissa tapauksissa standardin nimi ei noussut esiin. Yritykset eivät näin ollen ole virallisesti sitoutuneet ylläpitämään lainsäädännön vaatimuksia korkeampaa tietoturvan tasoa. Yritys voi esimerkiksi ilmoittaa markkinointiviestinnässään toimivansa jonkin standardin mukaisesti, mutta ilman sertifikaattia tai omaa auditointia viestin vastaanottaja ei voi varmistua väitteestä.

Organisaatiosta riippuen jokin standardi on saatettu omaksua jopa kokonaan tai sitten toimintatapana on poimia ainoastaan yrityksen mielestä parhaat palat.

> *Me emme noudata mitään standardia, vaan ennemminkin poimimme parhaat palat ja hyödynnämme niitä. Emme esimerkiksi noudata ISO 27001:tä tai ISO 27002:ta, mutta poimimme niistä kirsikat päältä ja käytämme parhaita paloja pohjana tietoturvallemme.*
> (Tietoturvajohtaja, tuotantoala)

Kaksi yritystä mainitsi noudattavansa jotakin jatkuvuudenhallinta- tai tietoturvastandardia täydellisesti ja moni muukin ohjeellisesti, mutta yksikään niistä ei kuitenkaan jostakin syystä ole sertifioinut sitä. Tämä herättää kysymyksiä, sillä sertifikaatin voisi kuvitella olevan lisäarvo esimerkiksi uusasiakashankinnassa ja se saattaisi muodostua siten strategiseksi kilpailueduksi. Haastattelujen perusteella näin ei kuitenkaan ole. Pääsyy siihen, ettei standardeja sertifioida on juuri se, ettei niistä koeta saatavan tarpeeksi merkittävää hyötyä. Lisäksi ne aiheuttavat kustannuksia. Saavutetut edut tulisi siis pystyä osoittamaan hyvin suorasti, jotta sertifiointiin ryhdyttäisiin. Esimerkiksi erään palveluyrityksen ICT Manager totesi, etteivät asiakkaat aina edes huomioi sertifikaatteja:

> *…olemme huomanneet sen, että kun on tietyt asiakkaat, niin heillä on niin tiukat ne omat kriteeristöt, niin he eivät ole kyselleet, onko meillä jonkin standardin mukainen sertifiointi. Vaan niillä on ne omat kriteeristöt ja sitten käydään niiden kriteeristöjen mukaan se läpi ja sitten meidän pitää noudattaa heidän kriteeristöjä.*
> (ICT Manager, palveluala)

Kuten todettu, liiketoiminnan jatkuvuutta edistävien standardien sertifiointi on sidosryhmille virallinen todiste jatkuvuuden huomioimisen minimitasosta. Samalla ne ovat osoitus pitkäjänteisestä sitoutumisesta ja jatkuvuudenhallinnan strategisesta roolista. Sertifikaattien puuttumisesta ei kuitenkaan voida tehdä suoraa johtopäätöstä siitä, että jatkuvuudenhallintaan ei ole sitouduttu tai sen rooli ei ole strateginen. Esimerkiksi aikaisemminkin mainittu suuri tuotantoalan yritys noudattaa kahta jatkuvuudenhallinta-

standardia täysin ja vain sertifikaatti uupuu. Jatkuvuudenhallintaan on siis selvästi sitouduttu, mutta sertifikaatin tuomaa lisäarvoa ei yksinkertaisesti nähdä riittävänä. Standardien pelkkä mukaileminenkin viittaa toimintatapojen kehittämiseen ja paremman jatkuvuuden tavoittelemiseen, mutta ei vielä itsessään tee jatkuvuudenhallinnasta strategista.

4.5.3 Henkilöstön sitoutuminen

Kuten on tullut esille, johdon sitoutuminen jatkuvuudenhallintaan on erityisen tärkeää sen onnistumisen kannalta (Seow 2009, 201). Siksi tutkimuksessa pyrittiinkin selvittämään, missä määrin johto tukee yrityksen häiriöttömyyttä edistävää toimintaa. Niissäkin organisaatioissa, joissa jatkuvuussuunnittelua tehdään tai joissa jatkuvuudenhallinnalla on muodollinen rooli, on riskinä, että hyvin alkanut toiminta kutistuu koskemaan vain yrityksen tiettyjä osia tai unohtuu pahimmassa tapauksessa kokonaan. Strategisuuteen viittaava ulkomuoto ei siis takaa jatkuvuudenhallinnan strategista roolia. Haasteena on säilyttää johdon sitoutuminen myös jatkossa (Seow 2009, 202).

Kysyttäessä miten yrityksen johto tukee jatkuvuudenhallintaa tai riskejä ehkäiseviä toimia, olivat vastaukset melko vaihtelevia. Yleisimmin haastateltavat pitivät johdon sitoutumisen merkkinä jatkuvuudenhallinnan riittäviä taloudellisia resursseja. Resursseja tarvitaan esimerkiksi suunnitelman testaamiseen ja päivittämiseen sekä suunnitelmassa esitettyjen toimenpiteiden, kuten tiedonvarmennusjärjestelmien toteuttamiseen. Usean yrityksen kohdalla tuli erikseen ilmi, että resursseja saa, kunhan perustelut ovat hyvät.

> *Kyllä (hankkeet menevät läpi), mutta perusteltuja niiden pitää olla ja ne hyödyt pitää tuoda selvästi esille.*
> (Tietohallintopäällikkö, pankki- ja vakuutusala)

Muita asioita, joita haastateltavat tulkitsivat osoituksiksi johdon sitoutumisesta tai tuesta, olivat esimerkiksi viralliset vaatimukset jatkuvuudenhallinnalle sekä säännölliselle suunnitelman päivittämiselle, osallistuminen riskienhallintaan, harjoittelu kriisejä varten sekä kriisienhallintatiimin johtaminen. Lisäksi yleinen jatkuvuudenhallinnan tärkeäksi toteaminen oli erään haastateltavan mukaan merkki johdon tuesta.

Suorat kysymykset johdon sitoutumiseen liittyen saivat vastaukseksi hyvin subjektiivisia haastateltavien näkemyksiä. Ne eivät siis kerro johdon todellisista asenteista jatkuvuudenhallintaa kohtaan, mutta kuvaavat osaltaan sitä, millaisina henkilöstö johdon asenteet näkee. Nämä kokemukset vaikuttavat henkilöstön omaan sitoutumiseen ja jatkuvuudenhallinnan sulautumiseen yrityksessä, sillä johdon antama hyvä esimerkki edis-

tää minkä tahansa asian omaksumista. Yleisempiä päätelmiä johdon sitoutumisesta ei aineiston perusteella voida tehdä, mutta merkille pantavaa on, ettei yksikään haastateltavista kuitenkaan maininnut puutteista johdon sitoutumisessa tai tuessa liittyen häiriöiden ehkäisyyn.

Sitoutumista häiriöttömyystavoitteisiin voidaan koettaa parantaa niin johdon kuin henkilöstönkin osalta. Vaikutuskeinoina voivat olla esimerkiksi erilaiset kannustimet ja rangaistukset, vastuun hajauttaminen sekä valvonta. Periaatteena on, että omien tavoitteiden saavuttamista pyritään helpottamaan antamalla muillekin perusteltu syy ponnistella samojen tavoitteiden hyväksi. Viranomaistahot pyrkivät mahdollisesti vaikuttamaan johdon sitoutumiseen ja johto edelleen henkilöstöön. Esimerkiksi Finanssivalvonnan valtion edun nimissä asettamat vaatimukset jatkuvuudenhallinnasta velvoittavat pankki- ja vakuutusalan yritysjohtoa toimimaan häiriöiden ehkäisemiseksi ja säännösten rikkomisesta seuraa sanktioita. Vaatimusten täyttämistä myös valvotaan säännöllisesti. Johto taas pyrkii saavuttamaan Finanssivalvonnan asettamat tavoitteet jakamalla vastuuta organisaation eri osiin, luomalla toimintaperiaatteet ja valvomalla niiden toteutumista. Nämä toimet muokkaavat näkemyksiä jatkuvuudenhallinnan tärkeydestä, mikä taas vaikuttaa sitoutumiseen.

Kappaleessa 4.4.2 todettiin, että jatkuvuudenhallintaan liitetyt henkilökohtaiset kannustinjärjestelmät ovat haastattelujen perusteella hyvin harvinaisia, mutta valvontaa on useammassakin jatkuvuussuunnittelua tekevässä organisaatiossa. Keppiä sovelletaan siis porkkanaa useammin, mutta silläkin pyritään tuomaan esiin jatkuvuudenhallinnan virallinen asema, jotta henkilöstö sitoutuisi siihen. Pankki- ja vakuutusalalla jatkuvuussuunnittelun säännöllinen valvonta on toimintaedellytys (Standardi 4.4b 2010, 23). Tästä näkökulmasta katsottuna pankki- ja vakuutusala pyrkii selvästi muita aloja voimakkaammin sitouttamaan henkilöstöään jatkuvuudenhallinnan periaatteisiin.

Vastuun antaminen on tehokas tapa sitouttaa työntekijä yritykseen ja sen tavoitteisiin. Herbanen ym. (2004, 447-448) tutkimuksessa yritykset, joissa jatkuvuudenhallinta oli annettu linjajohdon vastuulle, käyttivät jatkuvuudenhallintaa strategisimmin hyväkseen. Nämä yritykset totesivat, että hajautettu vastuu auttoi luomaan jatkuvuudenhallinnasta paremman, organisaationlaajuisen kuvan. Haastattelujen perusteella vastuun hajauttaminen on yleisin tapa toteuttaa suunnittelu myös tämän tutkimuksen yrityksissä ja samalla se on yleisin keino vaikuttaa henkilöstön sitoutumiseen. Kuten kappaleessa 4.1.1 mainittiin, riippuu suunnitteluvastuiden jakautuminen jossain määrin yrityksen koosta, joten pienemmissä yrityksissä henkilöstö sitoutetaan ilmeisesti pääosin muilla tavoin, jos lainkaan.

4.5.4 Havaitut hyödyt

Haastateltavien asenteita jatkuvuudenhallintaa kohtaan pyrittiin määrittämään myös kartoittamalla heidän kokemuksiaan ja näkemyksiään sen hyödyllisyydestä. Tuntemukset riskejä ehkäisevän toiminnan hyödyllisyydestä kuvaavat osaltaan sitoutumista ja ainakin valmiutta sitoutumiselle, sillä mikäli toimintaa ei nähdä millään tavoin hyödyllisenä, ei siihen todennäköisesti myöskään sitouduta. Negatiiviset mielikuvat vaikeuttavat jatkuvuudenhallinnan sulautumista toimintatapoihin.

Haastatteluaineiston perusteella jatkuvuudenhallintaa pidetään yleisesti hyödyllisenä, vaikka kaikki organisaatiot eivät sitä itse laajassa mittakaavassa toteutakaan. Se viittaa siihen, että jatkuvuudenhallinnan sulautumiselle on olemassa hyvät edellytykset. Haastateltavilta kysyttiin, näkevätkö he jatkuvuudenhallinnan ainoastaan liiketoiminnan mahdollistajana, vai onko siitä strategista hyötyä esimerkiksi kilpailuedun muodossa. Näkemys kertoo paljon henkilön asenteesta, sillä mikäli jatkuvuudenhallintaa pidetään vain liiketoiminnan mahdollistajana, on se oikeastaan vain välttämätön tukitoiminto, jolla ei useinkaan ole strategista roolia.

Yhtä haastateltavaa lukuun ottamatta kaikki mainitsivat jatkuvuudenhallinnan olevan ainakin jollain tavoin strateginen etu. Tämä näkemys ei mielestäni takaa sitä, että jatkuvuudenhallinta olisi yritykselle strateginen voimavara, mutta viittaa siihen, että henkilö on tunnistanut jatkuvuudenhallinnan hyötyjä, mikä saattaa johtaa korkeampaan sitoutumisen asteeseen. Haastateltavien joukossa sitoutuminen vaikuttaisi siis olevan yleistä. Yksittäisen haastattelun tuloksia ei tosin voida yleistää edes kyseiseen yritykseen, koska näkemykset ovat hyvin subjektiivisia.

Pankki- ja vakuutusalalla on vaikea erottua kilpailijoista paremmalla jatkuvuudenhallinnalla, koska vaatimukset ja perustaso ovat kaikille yhtä korkeat. Eräs alan yrityksen edustaja totesi, että kaikki pankki- ja vakuutusalan yritykset tekevät samoja asioita, mikä johtaa siihen, ettei jatkuvuudenhallinnalla voi juuri erottua. Eri toimialojen yrityksiin verrattuna kilpailuetua voisi hänen mukaansa olla, mutta ne eivät luonnollisesti kilpaile samoilla markkinoilla. Muut pankki- ja vakuutusalan yritysten haastateltavat pitivät kuitenkin jatkuvuudenhallintaa selvästi strategisena etuna.

> *Näen sen strategisena etuna siinä mielessä, että toki teemme paljon yhteistyötä Finanssialan keskusliiton kanssa, mutta emme tietenkään jaa kaikkea sisäistä tietoa. Näemme sen niin, että se on meille ilmeinen etu, jos pystymme pyörittämään toimintaamme pidempään kuin joku muu.*
> (Turvallisuusjohtaja, pankki- ja vakuutusala)

Lähes kaikki haastateltavat mainitsivat siis jatkuvuudenhallinnan mahdolliseksi strategisen edun tuojaksi. Yrityksestä riippuen tämän näkemyksen voimakkuus kuitenkin

vaihteli huomattavasti. Osa piti riskien ehkäisyä ja häiriöttömyyttä selvänä kilpailuetuna kun taas toiset totesivat siitä olevan hyötyä vain joissakin erikoistapauksissa. Esimerkkinä eräs pankki- ja vakuutusalan yritys mainitsi mahdollisuudesta palvella asiakkaita sähköpostitse, mihin kaikki eivät kykene. Se vaatii yritykseltä erittäin hyvää tietoturvan tasoa. Ainoastaan yksi haastateltu henkilö kertoi näkevänsä jatkuvuudenhallinnan vain liiketoiminnan mahdollistavana tekijänä. Kyseisessä yrityksessä ei ole jatkuvuus- tai toipumissuunnitelmaa.

> *Minun mielestäni strategia… strategista etua siinä ei pitäisi olla. Jos siinä on, niin ollaan vähän niin kuin pielessä.*
> (Tietohallintojohtaja, palveluala)

Paremman toipumisnopeuden ja joustavuuden suoman kilpailuedun ohella viidessä haastattelussa nousi esiin myös jatkuvuudenhallinnan positiivinen vaikutus organisaation kehitykseen. Kun yritys pyrkii ehkäisemään häiriöitä, tulee sen tunnistaa riskejään analysoimalla säännöllisesti kriittisiä resurssejaan ja toimintaympäristöään. Tämä saattaa johtaa siihen, että organisaatio priorisoi prosessejaan tai resurssejaan uudelleen tai löytää toiminnastaan tehostamiskohtia.

> *…kun teemme niitä (suunnitelmia), meidän tulee ajatella koko liiketoimintaa, prosesseja, riippuvuussuhteita ja tietojärjestelmiä ja meidän täytyy tehdä tämä säännöllisin väliajoin. Se parantaa organisaatiotamme: löydämme asioita, joita voimme tehdä paremmin tai joita olemme unohtaneet ja sitten muistamme, että se tehdään näin tai noin. Eli uskon, että se (jatkuvuudenhallinta) parantaa organisaatiota.*
> (IT-palvelupäällikkö, pankki- ja vakuutusala)

Muutamat haastateltavat mainitsivat jatkuvuudenhallinnan eduksi erikseen yrityksen arvon säilymisen. Arvon säilyttäminen on hyvin perustavanlaatuinen jatkuvuudenhallinnan tuoma kyvykkyys, joka tukee yrityksen muiden strategisten toimintojen menestystä. Jatkuvuudenhallinta suojelee yrityksen hankkimaa arvoa ehkäisemällä riskejä, parantamalla yrityksen toipumisnopeutta ja minimoimalla häiriöistä aiheutuvia vahinkoja (Herbane ym. 2004, 437). Tämän hyödyn tunnistaminen saattaa parantaa jälleen työntekijän sitoutumishalukkuutta, koska henkilö voi kokea hyötyvänsä jatkuvuudenhallinnasta esimerkiksi työpaikkansa säilymisen kautta.

Useat yritykset ovat tiedostaneet jatkuvuudenhallinnan hyödyn yrityksen imagolle. Häiriöiden tehokas käsittely parantaa organisaation toipumiskykyä, mikä voi vaikuttaa yrityksen imagoon. Imago taas vaikuttaa sidosryhmien halukkuuteen tehdä yhteistyötä myös kriisin jälkeen. Mikäli asiakkaita riittää myös jatkossa, on normaalitila helpompi

saavuttaa. Toisaalta hyvällä jatkuvuudenhallintaimagolla voi olla positiivisia vaikutuksia myös ilman, että yrityksen tarvitsisi kohdata kriisiä, jos se saa vakuutettua esimerkiksi asiakkaat häiriöidenkäsittelykyvyistään. Herbanen ym. (2004, 446-447) tutkimuksesta kävi ilmi, että eräs yritys oli saanut houkuteltua uusia asiakkaita vakuutettuaan ne hyvistä toipumiskyvyistään. Myös osa tämän tutkimuksen yrityksistä tiedostaa häiriöttömyyden merkityksen ulkoiselle imagolle:

> *Se on yrityskuvallinen merkitys, että tietojärjestelmät toimivat ja tämä jatkuvuudenhallinta on kunnossa. Sen paikkaaminen on todella hankalaa, jos yrityskuva on menetetty.*
> (Tietoturvapäällikkö, pankki- ja vakuutusala)

Toimittajayrityksen tai asiakkaan hyvä joustavuus tai toipumisnopeus on haastattelujen perusteella kuitenkin vain harvoin pääasiallinen kriteeri valittaessa liikekumppania, minkä vuoksi jatkuvuudenhallintaan liittyvät asiat eivät tule neuvotteluissa tai kaupankäynnissä välttämättä esille lainkaan. Organisaatiot eivät siis ole kovin innokkaita panostamaan ulkoiseen jatkuvuudenhallintaimagoonsa. Haastatteluissa ei erikseen tutkittu ulkoisen imagon rakentamista, mutta erään palvelualan yrityksen edustaja kuvasi tietoturvan merkitystä asiakashankinnassa seuraavasti:

> *Sehän on vaikea erottua paremmalla tietoturvalla, koska jos sinulla on hyvä tietoturva, niin ethän sinä julista sitä niinkään kauheasti, etkä mainosta siitä mitään. Niin se on vähän sellainen, että totta kai jos on hyvä tietoturva, niin se on etu asiakkaiden kannalta, mutta se on ennemminkin sitten siinä vaiheessa, kun ollaan jo aika pitkällä siinä asiakassuhteessa. Että neuvotellaan siitä sopimuksesta ja he kyselevät kaikenlaista ja silloin me tietenkin annetaan informaatiota meidän järjestelmistämme. Kun tehdään sopimusta tai tehdään jonkinnäköistä auditointia.*
> (ICT Manager, palveluala)

Edellisen toteamuksen perusteella jatkuvuudenhallintaimago ei siis vaikuttaisi olevan ratkaiseva tekijä uusien liikekumppaneiden hankkimisen ja nykyisten säilyttämisen kannalta. Jatkuvuudenhallinnalla voi kuitenkin olla merkittävä vaikutus yrityksen kokonaisimagoon. Imagon menettämisen seurauksia on pohdittu vastausten perusteella useammassakin yrityksessä:

> *Vaikka me saisimmekin teknisesti asiat hoidettua, mutta emme imagomielessä, niin sillä voi olla meille paljon suurempi liiketoiminnallinen haitta*

> *kuin mistään yksittäisestä palosta, koska me olemme kuitenkin varautuneet tällaisiin häiriötekijöihin vakuuttamisella.*
> (Talousjohtaja, palveluala)

Näkemys, jonka mukaan organisaation jatkuvuus riippuu myös yrityskuvasta, edustaa strategista ja liiketoimintalähtöistä ajattelutapaa. Se kertoo, että jatkuvuuden ei nähdä riippuvan ainoastaan teknisistä tai yrityksen sisäisistä asioista.

4.5.5 Yhteenveto

Jatkuvuudenhallinnan tulisi perustua yrityksen liiketoimintastrategiaan ja sen tarpeisiin ja tukea strategisten tavoitteiden saavuttamista (Herbane ym. 2004, 448). Havaintojen perusteella motiivit jatkuvuudenhallinnan toteuttamiselle vaihtelevat merkittävästi. Osalla toiminta on hyvin liiketoimintalähtöistä, mutta toisilla pääroolissa ovat ulkoiset, lainsäädännön tai asiakkaiden vaatimukset. Pankki- ja vakuutusalan jatkuvuudenhallintaa koskeva lainsäädäntö on erityisen tiukka, mutta myös muilla aloilla voi esiintyä erityisvaatimuksia. Suuremmat yritykset uskovat jatkuvuudenhallintansa olevan vaatimuksia paremmalla tolalla ainakin joiltain osin. Pienemmillä organisaatioilla resursseja on vähemmän ja ne kanavoidaan ensisijaisesti ydinliiketoimintoihin, joten jatkuvuudenhallinta jää niissä helpommin pimentoon.

Jatkuvuudenhallintastandardien noudattaminen tai sertifiointi on erittäin harvinaista, sillä vain ylivoimaisesti suurin tapausyritys käyttää sellaisia hyväkseen. Pankki- ja vakuutusalan yritykset noudattavat Finanssivalvonnan standardia, mikä selittää niiden haluttomuutta käyttää yleisiä standardeja. Tietoturvastandardeja sovelletaan yleisesti kaikilla aloilla pankki- ja vakuutusalaa lukuun ottamatta. Trendinä on, että niistä poimitaan parhaat palat tai kenties noudatetaan kokonaisuudessaankin, mutta sertifikaattiin ei investoida siitä saatavien vähäisten hyötyjen vuoksi.

Onnistunut jatkuvuudenhallinta edellyttää johdon sitoutumista (Seow 2009, 201). Johdon sitoutuminen nähdään yleisesti ottaen vähintään kohtuullisena, sillä siinä ei havaittu moitittavaakaan. Osoituksina sitoutumisesta pidetään esimerkiksi virallisia jatkuvuudenhallintavaatimuksia ja osallistumista riskien- ja kriisinhallintaan. Henkilöstöä pyritään sitouttamaan esimerkiksi jakamalla jatkuvuudenhallintaan liittyviä vastuita ja valvonnalla. Kannustinjärjestelmien käyttö todettiin jo edellisessä kappaleessa hyvin harvinaiseksi.

Jatkuvuudenhallinnan hyötyjen tiedostaminen vaikuttaa merkittävästi työntekijöiden asenteisiin, joten ne tulee kertoa ja demonstroida (Seow 2009, 207). Jatkuvuudenhallintaa pidetään yleisesti hyödyllisenä, joten sen sulautumiselle on hyvät edellytykset. Etuina nähdään esimerkiksi toipumisnopeus, yrityksen joustavuuden ja imagon paranemi-

nen, arvon säilyminen sekä edellisten avulla saavutettava kilpailuetu. Havaittavissa oli myös osin vastakkaisia mielipiteitä, sillä jotkut pitivät jatkuvuudenhallintaa lähinnä liiketoiminnan mahdollistajana, josta ei tulisi saada kilpailuetua. Kilpailuetu olisi merkki siitä, että yrityksen ydinliiketoiminnassa on jokin pielessä.

5 LOPUKSI

5.1 Yhteenveto

Kuten mainittua, eri teemat voivat antaa erilaisen kuvan jatkuvuudenhallinnan roolista yksittäisessäkin yrityksessä. Esimerkiksi tiedonvarmennus saattaa olla hyvin hoidettu, mutta samaan aikaan suunnittelu, viestintä ja johdon sitoutuminen ovat huonolla tolalla. Kaiken kaikkiaan tutkimuksen eri yritykset, toimialat ja teemat antavat jatkuvuudenhallinnan roolista hyvin epäyhtenäisen kuvan. Tämä viittaa siihen, ettei yrityksen jatkuvuutta useinkaan johdeta suunnitellusti ja kokonaisvaltaisesti, jolloin sen on hyvin vaikea nousta strategiseen rooliin.

Jatkuvuudenhallintaan liittyvien vastuu- ja henkilöstökysymysten perusteella yritykset jakautuvat jonkin verran. Parhaimmillaan jatkuvuudenhallinta viittaa strategiseen lähestymistapaan, mutta heikommillaan se on hyvin operatiivista ja vahvasti IT-painotteista. Suunnittelu- ja toteutusvastuun jakaminen ylimmän johdon ulkopuolelle on sitä todennäköisempää, mitä suurempi yritys on kyseessä. Näin organisaation eri osat tekevät itsenäistä työtä jatkuvuudenhallinnan hyväksi ja henkilöstö sisäistää sen osaksi arkipäiväistä toimintaa. Vaikka jatkuvuudenhallinta olisikin jaettu erikseen liiketoiminnan ja IT:n prosesseihin, on IT:n rooli kuitenkin käytännössä monessa yrityksessä huomattava.

Suuret yritykset huolehtivat Suomessa hyvin tiedon saatavuudesta, sillä varmuuskopiointi on vakiintunutta ja useissa tapauksissa reaaliaikaista. Tiedot siirretään usein eri paikkakunnalle tai jopa useisiin eri sijainteihin. Riittävän osaamisenkin saatavuudesta on huolehdittu etenkin IT:n osalta. IT on joko ulkoistettu riittävän osaamisen turvaamiseksi, tai sitten ajoittain tarvittavat kapasiteettitoimittajat on määritelty etukäteen.

Jatkuvuudenhallinnan tulee pohjautua oikeaan ja riittävään tietoon, jotta se pystyy tukemaan yrityksen jatkuvuutta. Kaikilla organisaatioilla on havaittavissa jonkinlaista riskien tunnistamistoimintaa ja se ulottuu usein myös toimittajiin ja asiakkaisiin. Yrityksen ulkopuolella olevien toimitusketjun osien riskejä pyritään vähentämään esimerkiksi palvelutaso-, tietoturva- ja suunnitteluvaatimusten avulla. Strategisten työkalujen hyödyntäminen suunnittelussa on sitä yleisempää, mitä suurempi yritys on kyseessä.

Enemmistö suuryrityksistä erottaa jatkuvuudenhallintaan liittyvät prosessit liiketoiminnan ja IT:n prosesseihin, mutta varsinkin vertailujoukon pienemmissä yrityksissä painopiste on IT:ssä ja vahinkoriskeissä. IT on merkittävässä roolissa erityisesti niissä organisaatioissa, joissa IT-infrastruktuuri on päätetty hoitaa itse. Tiedon saatavuus on niin oleellista liiketoiminnan jatkuvuuden kannalta, että sen varmistamiseen joudutaan uhraamaan paljon resursseja. IT:n ulkoistaneille yrityksille jää ilmeisesti enemmän aikaa pohtia myös liiketoiminnallisia näkökulmia.

Jatkuvuussuunnitelma löytyy suurimmasta osasta yrityksiä, mutta sen sisältö voi vaihdella hyvinkin paljon. Puutteellisinta suunnittelu on pienemmissä yrityksissä. Pankki- ja vakuutusala erottuu edukseen, sillä sen kaikilla edustajilla on suunnitelma – kuitenkin pitkälti lainsäädännöstä johtuen. Käytännössä kaikille suuryrityksille pakollinen pelastussuunnitelma löytyy myös niiltä organisaatioilta, jotka eivät ole jatkuvuussuunnitelmaa laatineet. Nekin joutuvat siis lain nojalla suojaamaan vähintään henkilöstönsä.

Pankki- ja vakuutusala loistaa myös suunnitelmien ylläpidossa. Niiden päivitys- ja testauskäytännöt ovat selvästi organisoiduimmat ja säännöllisimmät. Ylläpito on kirjattu yrityksen virallisiin toimintaohjeisiin, mikä edistää jatkuvuudenhallinta-ajattelun sulautumista. Pankki- ja vakuutusalaa lukuun ottamatta suunnitelmien testaus keskittyy pääosin IT-osastoon ja teknisiin asioihin. Erityisen tärkeässä roolissa näytti olevan jälleen tiedonvarmennus ja tiedon saatavuus.

Jatkuvuudenhallinnan viestintä on parhaimmillaan monimuotoista, aktiivista ja jatkuvaa, mutta huonoimmillaan passiivista ja sisällöltään suppeaa. Puutteita esiintyi varsinkin palvelualan yrityksissä, joissa viestintä ei aina ulotu edes suunnitelmasta vastuullisille henkilöille. Jatkuvuussuunnitelmasta kommunikoidaan kokonaisuutena vain harvoin, mutta esimerkiksi tietoturva-asioista viestitään erittäin yleisesti. Intranet on viestintäkanavana suosittu, mutta myös luentoja, palavereja, henkilökohtaisia perehdytyksiä sekä sähköpostia käytetään.

Valvontaa ei ole hyödynnetty kovin yleisesti jatkuvuudenhallintaan liittyvissä asioissa, vaikka sen vaikutus yrityksen häiriöttömyyteen voisi olla positiivinen. Pankki- ja vakuutusalalla valvonta on kuitenkin yleistä. Valvonnan harvinaisuus on saattanut vaikuttaa siihen, ettei jatkuvuuteen liittyviä kannustinjärjestelmiäkään ole juuri olemassa. Kannustimien ongelmaksi on lisäksi koettu oikeanlaisten mittareiden puuttuminen.

Jatkuvuudenhallinnan virallinen asema edistää jatkuvuusajattelun sulautumista. Merkkejä virallisuudesta ovat esimerkiksi viralliset jatkuvuustiimit, koordinaattorit, vastuut ja säännöllinen ylläpito. Kriisienhallintatiimit ovat yleisiä, mutta riskejä proaktiivisesti ehkäisevät taas harvinaisempia. Suuremmissa yrityksissä vastuu yrityksen jatkuvuudesta annetaan yleensä ylimmän johdon ulkopuolelle, mikä sitouttaa henkilöstöä. Vastuisiin liittyy usein raportointi- ja ylläpitovelvoitteita. Eräällä organisaatiolla on käytössään itse kehitetty jatkuvuudenhallinnan kypsyysmalli, joka liittää jatkuvuudenhallinnan olennaiseksi osaksi jokaista osastoa.

Syy jatkuvuudenhallinnalle voi olla peräisin liiketoiminnan tarpeista tai esimerkiksi toimialan ja lakien vaatimuksista. Suurimmissa yrityksissä liiketoiminta on tärkein jatkuvuudenhallinnan ajuri kaikilla alueilla, mutta muissa organisaatioissa liiketoiminnan vaatimuksia pohditaan korkeintaan osittain – esimerkiksi tiedon saatavuuden osalta. Pienemmät yritykset toimivat yleensä lain minimivaatimusten mukaisesti, mutta suuremmat kehittävät prosessejaan usein pidemmälle. Syynä tähän ovat ilmeisesti yksinkertaisesti resurssit, joita kohdistetaan ensisijaisesti ydinliiketoiminnan prosesseihin.

Jatkuvuudenhallintastandardien vapaaehtoinen noudattaminen tai sertifiointi on hyvin harvinaista, mutta esimerkiksi tietoturvastandardeja käytetään hyväksi usein. Niitä ei kuitenkaan sertifioida, vaan päältä noukitaan parhaat palat. Yritykset eivät näin ollen ole virallisesti sitoutuneet ylläpitämään lainsäädännön vaatimuksia parempaa tietoturvan tasoa. Sertifioinnista ei koeta saatavan riittävästi lisäarvoa, jotta sen hankkiminen olisi kannattavaa. Pankki- ja vakuutusalalla noudatettavaa Finanssivalvonnan standardia ei voida laskea jatkuvuudenhallinnan strategisuuteen viittaavaksi standardiksi, sillä sen noudattaminen ei ole vapaaehtoista.

Henkilöstön asenteita kartoitettiin johdon sitoutumisen ja havaittujen hyötyjen avulla. Johdon koetaan yleisesti ottaen tukevan jatkuvuudenhallintaa, sillä sitoutumisessa ei mainittu olevan puutteita. Johto esimerkiksi osallistuu suunnitteluun ja harjoitteluun, vaatii suunnitelmien päivittämistä, johtaa kriisienhallintaa ja antaa resursseja, kunhan perustelut ovat hyvät. Perusteluina voidaan käyttää jatkuvuudenhallinnan havaittuja hyötyjä, jotka voivat olla esimerkiksi omavaraisella IT-osastolla aikaansaatu tehokkaampi toipuminen, imagon parantuminen tai henkilöstön koulutuksen kautta saavutettu joustavuus.

5.2 Johtopäätökset

Tämän tutkimuksen ensisijaisena tarkoituksena oli vastata kysymykseen: **Millainen on jatkuvuudenhallinnan rooli suurissa suomalaissa yrityksissä?** Havaintojen perusteella voidaan lyhyesti todeta, että rooli on vaihteleva, mutta tällä suppealla kuvauksella ei ole juurikaan arvoa. Sen sijaan kiinnostavaa on, että jatkuvuudenhallinnan roolit voidaan luokitella kolmeen eri luokkaan, joista jokaisella on omat erityispiirteensä. Tähän päätelmään päädyttiin, sillä havainnot antoivat hyvin monissa tarkastelukohdissa kolmentyyppisiä tuloksia. Osa yrityksistä toteuttaa jatkuvuudenhallintaansa poikkeuksellisen hyvin, osa kohtalaisesti ja osa heikosti. Useat yritykset sijoittuivat eri tarkastelukohdissa eri tavoin, eli niiden jatkuvuudenhallinta ei ole yhtenäistä koko organisaation laajuudella. Jotkin asioista hoidetaan paremmin kuin toiset. Tarkasteltuun joukkoon mahtui kuitenkin muutama yritys, joissa jatkuvuudenhallinnan rooli vaikutti hyvin samanlaiselta eri näkökulmista katsottaessa.

Luokittelu kuvaa paremmin, mitkä ovat merkittävimmät erot yritysten jatkuvuudenhallinnassa ja ajattelutavoissa. Yksittäinen yritys voidaan sijoittaa jatkuvuudenhallintansa perusteella yhteen luokkaan. Taulukko 2 nimeää eri luokat ja kuvailee niiden tärkeimmät ominaispiirteet.

Taulukko 2 Jatkuvuudenhallinnan roolit suurissa suomalaisissa yrityksissä

Jatkuvuudenhallinnan rooli	**Ominaispiirteet**
1. Liiketoiminnan mahdollistaja	- Tavoitteena lainsäädännön tai asiakkaan vaatimusten täyttäminen - Jatkuvuudenhallinta ja strategia eivät ole liitoksissa toisiinsa - Ei jatkuvuussuunnitelmaa / suunnitelma vain asiakasta varten
2. Tukitoiminto	- Monia toipumisnopeutta, joustavuutta ja sulautumista edistäviä toimintatapoja - Jatkuvuudenhallinta ei kuitenkaan palvele koko organisaation jatkuvuutta - Jatkuvuussuunnitelma ja/tai toipumissuunnitelma, josta viestitään - Strategisten työkalujen hyödyntäminen yrityksen sisällä - Jatkuvuudenhallinnalla muodollinen asema - Vastuuta hajautettu - Off-site tiedonvarmennus
3. Strateginen	- Jatkuvuudenhallintaa pidetään strategisena menestystekijänä - Liiketoimintayksiköt suunnitteluvastuussa - Johdon tuki ja osallistuminen - Lähtökohtana liiketoiminnan tarpeet - Koko organisaatio huomioitu tasapainoisesti - Suunnitelmien säännöllinen päivitys ja testaus - Valvonta - Strategisten työkalujen hyödyntäminen myös yrityksen toimitusketjujen ulkoisiin osiin - Poikkeukselliset toimintamallit (kilpailuetu)

Ensimmäinen luokka koostuu yrityksistä, joiden jatkuvuudenhallinta perustuu ainoastaan asiakkaiden tai lainsäädännön vaatimuksiin. Tämän kategorian yritykset näkevät jatkuvuudenhallinnan ja strategian selvästi erillisinä asioina, eli ne eivät tunnista jatkuvuudenhallinnan roolia pitkän aikavälin tavoitteiden saavuttamisessa tai kilpailuedun luomisessa. Ne huolehtivat lakisääteisistä asioista, kuten tietosuojasta ja pelastussuunnitelmista sekä niiden kouluttamisesta, mutta pitävät tason muilta osin hyvin alhaisena. Ensimmäisen luokan yrityksillä ei ole jatkuvuussuunnitelmaa tai se on luotu vain asiakkaan pyynnöstä ja asiakasta varten.

Toiseen luokkaan kuuluvat yritykset, jotka soveltavat teorian mukaisia jatkuvuudenhallinnan periaatteita monin eri tavoin, mutta joilla se ei ole liiketoimintalähtöistä tai painottuu rajattuihin organisaation osiin kuten tietohallintoon. Näillä yrityksillä on selvä pyrkimys parantaa toipumisnopeuttaan ja joustavuuttaan joidenkin riskien suhteen, mutta jatkuvuudenhallinnan tavoitteita ei ole liitetty yrityksen strategisiin tavoitteisiin. Ne

siis tiedostavat jatkuvuudenhallinnan hyödyt osittain, mutta eivät osaa käyttää niitä pitkän tähtäimen tavoitteidensa tukena tai kilpailukeinona.

Jatkuvuussuunnitelman luomiseksi on toisen luokan yrityksissä mahdollisesti käytetty strategisia työkaluja, mutta ne eivät ulotu yrityksen ulkoisiin sidosryhmiin tai toimitusketjuihin. Suunnitelmista viestitään vähintään vastuuhenkilöille. Jatkuvuudenhallinnalla on organisaatiossa muodollinen asema siten, että siihen liittyviä vastuita ja vaatimuksia on määritelty ja niiden toteutumisesta raportoidaan ylimmälle johdolle. Tiedonvarmennus on toteutettu off-site -ratkaisuna, eli tiedon saatavuuden suuri merkitys yrityksen liiketoiminnalle on tiedostettu.

Kolmanteen luokkaan kuuluu vain hyvin pieni osa suomalaisista suuryrityksistä. Ne pitävät jatkuvuudenhallintaa strategisena menestystekijänä. Näissä yrityksissä jatkuvuudenhallinta on mahdollisista ulkoisista vaatimuksista huolimatta lähtöisin liiketoiminnan tarpeista ja siihen kiinnitetään huomiota organisaation kaikilla osa-alueilla. Jatkuvuussuunnitelmia luotaessa huomioidaan myös ulkoisten toimitusketjujen riippuvuussuhteet ja käytetään hyväksi joitakin strategisia suunnittelutyökaluja. Suunnitelmista myös viestitään ja niitä päivitetään ja testataan säännöllisesti. Kolmannen luokan yritykset soveltavat toimialan, Suomen ja jopa maailman mittapuulla harvinaisia toimintamalleja, joilla ne pyrkivät saavuttamaan poikkeuksellista suorituskykyä ja kilpailuetua. Hyviä esimerkkejä ovat riskien tunnistamisessa ja suunnitelmien luomisessa tukevien koordinaattoreiden hyödyntäminen, jatkuvuudenhallinnan kypsyysmalli ja kannustimet sekä erityisen foorumin käyttö viestinnän ja kehityksen tukena.

Moneen tutkimuksen tapausyritykseen liittyy piirteitä, jotka viittaavat kolmanteen luokkaan, eli jatkuvuudenhallinnan strategiseen rooliin. Liiketoimintalähtöisyys, toiminnan kokonaisvaltaisuus, yrityksen toimitusketjujen ulkoisten osien huomioiminen sekä kilpailuetuun tähtäävät toimintamallit ovat kuitenkin vaatimuksia, jotka aiheuttavat useiden yrityksen sijoittumisen ensimmäiseen tai toiseen luokkaan. IT-strategia saattaa huomioida IT-toimintojen jatkuvuuden, mutta jatkuvuudenhallinnan liittäminen ainoastaan IT:n strategisiin tavoitteisiin ei kuitenkaan tee siitä strategista koko yrityksen kannalta. Tutkimuksen perusteella enemmistö suurista suomalaisista yrityksistä lukeutuukin kahteen ensimmäiseen luokkaan. Yleisesti voidaan siis todeta, että jatkuvuudenhallinnan rooli on suurissa suomalaisissa yrityksissä yleensä muu, kuin strateginen.

Tutkimuksella pyrittiin selvittämään myös **miten jatkuvuudenhallinta voi ilmetä yrityksen toiminnassa häiriötilanteiden ulkopuolella**. Jatkuvuudenhallinnan tulisi olla keskeytymätön prosessi, joten tähän kysymykseen odotettiin löytyvän myös vastauksia.

Suurin osa organisaatioista näkee jatkuvasti tai säännöllisesti vaivaa jatkuvuutensa turvaamiseksi. Hyviä esimerkkejä ovat erityisesti pankki- ja vakuutusalalla esiin nousseet riskienhallintaorganisaatiot sekä viralliset koordinaattorit, jotka molemmat tunnistavat ja analysoivat keskeytyksettä yrityksen riskejä. Ne myös tukevat jatkuvuussuunni-

telmien laatimisessa ja valvovat sen ajantasaisuutta. Kaikissa yrityksissä riskien tunnistaminen ei ole jatkuvaa, mutta analyysi tehdään kuitenkin vähintään vuosittain.

Toinen arkipäiväinen osoitus jatkuvuudenhallinnasta on sen viestintä. Yritys voi viestiä jatkuvuudenhallintaan liittyvistä asioista esimerkiksi koulutuksilla, harjoituksilla, sähköpostin tai intranetin kautta tai vaikkapa kannustinjärjestelmillä. Kriisiajan viestintä on tärkeää, mutta vielä tärkeämpää on sitä edeltävä kommunikaatio. Uhista ja niiltä suojautumisesta tiedottamalla yritys voi onnistua välttämään monta kriisiä. Esimerkiksi tietoturvaohjeistukset ja -koulutukset voivat estää tunkeutujien pääsyn järjestelmään.

Myös tiedonvarmennus ja tietoturvariskien hallinta on yrityksille arkipäivää. Niissä yrityksissä, joissa IT-infrastruktuuri on omalla vastuulla, tulee tiedonvarmennuksesta ja tietoturvan riittävyydestä huolehtia jatkuvasti itse. Niiden tulee luoda datasta toistuvasti varmuuskopioita ja seurata aktiivisesti, että tietoturvariskien viimeisimmiltä uhilta on suojauduttu. Muissa yrityksissä riittää palvelutason hallinta sekä palveluntarjoajan toiminnan ja riskien valvonta, mutta näidenkin toimien tulee olla toistuvia.

Tutkimuksen kolmantena mielenkiinnon kohteena oli, **millaista kilpailuetua jatkuvuudenhallinnalla pyritään saavuttamaan**. Hieman yllättäen jatkuvuudenhallintaa pidetään hyvin harvoin todellisena kilpailuetuna omalle yritykselle. Sen potentiaaliset hyödyt kilpailukyvylle tiedostetaan yleisesti, mutta toteutusasteelle tai edes tavoitteeksi asti se ei useinkaan päädy. Tämä viittaa siihen, ettei jatkuvuudenhallintaa nähdä merkittävänä kilpailuetuna. Ensimmäiseen rooliluokkaan kuuluvat yritykset voivat jopa ajatella jonkin olevan pielessä, mikäli jatkuvuudenhallinta muodostuu strategiseksi eduksi.

Ne organisaatiot, jotka etua kuitenkin havittelevat, pyrkivät yleisimmin imagoetuun. Kilpailijoita parempi kyky ratkaista vaikeitakin ongelmia ja tuottaa tasalaatuisempaa palvelua saattaa olla eduksi asiakashankinnassa. Toinen haviteltu kilpailuvaltti on joustavuus- ja toipumisetu, jonka merkityksestä myös Herbanen ym. (2004, 440) kertoivat. Kun yrityksen liiketoiminta voi jatkua kilpailijoita pidempään tai se toipuu muita nopeammin, on yrityksen mahdollista saavuttaa sekä imago- että taloudellista hyötyä.

5.3 Hyvät käytännöt

Tutkimuksen yhtenä tavoitteena oli pyrkiä löytämään jatkuvuudenhallinnan **hyviä käytäntöjä**, jotka voivat parantaa yrityksen toipumisnopeutta tai joustavuutta tai edistää prosessien sulautumista. Hyviksi käytännöiksi katsotaan toimet, joita kaikki kilpailijat eivät toteuta ja jotka mahdollisesti johtavat parempaan jatkuvuuteen. Niiden tunnistaminen ja yhteen kokoaminen tarjoaa yritysjohdoille hyviä ja valaisevia vertailukohtia, sillä asioista päättävät eivät aina ole edes tietoisia, kuinka jatkuvuudenhallintaa voitaisiin kehittää. Lisäksi hyvät käytännöt voivat saada johdon näkemään jatkuvuudenhallinnan laajemmin kuin ainoastaan varmuuskopiointina tai paloturvallisuutena.

Hyvä jatkuvuudenhallinta huomioi teknisten asioiden ohella ihmiset, eli heidän merkityksensä yrityksen häiriöttömyydelle. Se edellyttää sitouttamista ja vaikuttamista asenteisiin, joka tapahtuu esimerkiksi vastuiden ja viestinnän kautta. Varsinkin suuremmissa yrityksissä on yleistä, että suunnitteluvastuu on annettu liiketoimintayksiköille. Tämä on suuryritysten tapauksessa mielestäni hyvä käytäntö, sillä samalla kun se sitouttaa henkilöstöä läpi organisaation, se myös parantaa suunnitelmien laatua ja soveltuvuutta liiketoimintayksikön häiriöihin. Suunnitelmia laatimassa ovat ne henkilöt, jotka toteuttavat jatkuvuudenhallinnan myös käytännön tasolla, joten suunnitelmien tuntemus on parempaa. Mukana on henkilöstöä niin liiketoiminnan kuin tietohallinnon puolelta. Parhaassa tapauksessa suunnitelmien laatimista avustavat erityiset koordinaattorihenkilöt tai riskienhallintaorganisaatiot, jotka ovat riskienhallinnan ja jatkuvuussuunnittelun asiantuntijoita.

Kriisienhallintavastuiden osalta oli havaittavissa kolmenlaisia toteutustapoja, joista parhaana näen etukäteen ja tilannekohtaisesti luotujen kriisienhallintatiimien yhdistelmän. Näin toipumista ryhtyvät hoitamaan häiriöalueen vastuulliset, joilla on paras tietämys kyseisen alueen liiketoiminnasta. Se johtaa todennäköisesti liiketoiminnan kannalta parhaisiin ratkaisuihin. Liiketoimintaosaajien ohella kriiseihin osallistuu aina myös etukäteen määritelty tiimi, jonka jäsenet ovat esimerkiksi viestinnän ja henkilöstöasioiden ammattilaisia. Liiketoimintajohto voi näin keskittyä siihen, mitä parhaiten osaa ja jättää tukitoiminnot asiantuntijoille. Tämä vaikuttaa todennäköisesti toipumisnopeuteen.

Jatkuvuudenhallinnan viestinnän hyviin käytäntöihin kuuluu, että se on säännöllistä ja monipuolista, parhaimmillaan kohderyhmän mukaan räätälöityä. Hyvä viestintä sitouttaa henkilöstöä jatkuvuudenhallinnan periaatteisiin. Intranetin lisäksi tulee hyödyntää eri viestintätapoja, kuten keskustelufoorumeita henkilökohtaisia perehdytyksiä ja luentoja. Myös kannustimet ovat hyvä tapa viestiä jatkuvuudenhallinnan merkityksestä, mutta niiden sitominen oikeanlaisiin kriteereihin voi olla ongelmallista.

Tiedon varmennus on suurissa suomalaisissa yrityksissä hyvällä tasolla, mutta pieniä erojakin yritysten väliltä löytyy. Paras tilanne on, mikäli käytössä on peilaava varmuuskopiointi, jolloin edes pienen aikavälin tietojen häviäminen on hyvin epätodennäköistä. Varmuuskopioinnissa ei tule luottaa yhteen kopioon, vaan tiedot pitää tallentaa useaan eri paikkaan. Näiden tallenteiden sijainti tulee olla vähintään eri paloalueella, mutta parempi on, mikäli alkuperäinen ja varmennettu data sijaitsevat aivan eri osoitteissa. Näin varmistetaan joustavuus esimerkiksi palvelinvikojen suhteen ja parannetaan tiedon saatavuutta.

Jatkuvuudenhallinnassa on oleellista, että se perustuu riittävään ja oikeaan tietoon. Riskiltä on vaikea välttyä, jos sitä ei tunneta tai jos se arvioidaan paljon todellista pienemmäksi. Mahdollista on myös, että yritys näkee paljon vaivaa ehkäistäkseen ”vääriä” riskejä, jotka ovat hyvin epätodennäköisiä tai joilla on vain pieni vaikutus yrityksen

liiketoimintaan. Hyvä käytäntö näiden virheiden ehkäisemiseksi onkin analysoida riskejä ja riippuvuuksia jatkuvasti tai vähintään säännöllisesti kaikkien liiketoimintojen ja prosessien näkökulmista. Apuna voidaan käyttää esimerkiksi arvoketjuanalyysiä tai liiketoiminnallista vaikutusanalyysiä, jotka tulee ulottaa myös ulkoisiin toimitusketjun osiin. Tärkeiden toimittajien tai asiakkaiden ongelmien vaikutukset yrityksen liiketoimintaan tulee arvioida. Riittävään tietoon pohjautuvat suunnitelmat parantavat sekä joustavuutta että toipumisnopeutta, koska monilta ongelmilta voidaan suojautua jo ennalta ja niiden ratkaisemiseksi on kehitetty lääkkeitä.

Hyväksi käytännöksi voidaan laskea myös jatkuvuussuunnitelman tekeminen ja erityisesti sen ylläpito. Suunnittelu edellyttää syventymistä omaan liiketoimintaan, mikä saattaa paljastaa uusia kehityskohtia, riippuvuussuhteita ja prioriteetteja. Se voi parantaa yrityksen joustavuutta ja toipumisnopeutta. Suunnitelman olemassa olo ei kuitenkaan vielä itsessään riitä, vaan sitä tulee ylläpitää, jotta se hyödyttäisi yritystä myös tulevaisuudessa. Säännöllinen ja tiheästi toistuva ylläpitoprosessi on erityisen hyödyllinen käytäntö, sillä se suojaa uusilta riskeiltä ja kouluttaa samalla vastuuhenkilöitä.

Standardien käyttäminen jatkuvuudenhallinnassa on hyödyllistä, mutta niiden sertifiointi ei ole välttämättä taloudellisesti kannattaa. Yrityksen olisikin hyvä etsiä jatkuvuutta edistävistä standardeista sen liiketoiminnalle soveltuvia osia ja toteuttaa ne. Näin yritys saa kuvan siitä, millä tasolla sen eri osa-alueet tällä hetkellä ovat ja se saa ilmaisia ideoita jatkuvuutensa kehittämiseen.

Yleisesti ottaen paras käytäntö jatkuvuudenhallinnassa on, että se perustuu liiketoiminnan tarpeisiin. Vaikka lait ja asetukset saattavat asettaa vaatimuksia, tulisi jatkuvuudenhallinnan olla yritystä varten. Jokaisen yrityksen strategisten tavoitteiden saavuttamiseen vaikuttaa monenlaisia uhkia, joiden hallitseminen vaikuttaa siis myös tavoitteiden saavuttamiseen (Herbane ym. 2004, 438). Kun yritysjohto tiedostaa jatkuvuudenhallinnan strategisen merkityksen, se toteuttaa sen liiketoiminnan ehdoilla, joka johtaa yleensä monin tavoin parempaan jatkuvuuteen ja mahdollisesti jopa kilpailuetuun.

5.4 Tutkimuksen rajaukset

Tutkimuksella on useita huomioitavia rajauksia. Tämän tutkimuksen havaintoaineisto kerättiin ainoastaan suurista suomalaisista yrityksistä. Se ei siis anna minkäänlaista kuvaa pienten, keskisuurten tai ulkomaalaisten yritysten jatkuvuudenhallinasta. Lisäksi tutkittavia tapauksia on ainoastaan yksitoista ja toimialoja kolme, eli havaintoja ei voida yleistää koskemaan kaikkia suuria yrityksiä.

Useimmat haastatellut henkilöt ovat taustaltaan hyvin tietoturva- tai tietohallintopainotteisia ja tutkimuskysymyksiin pyrittiin siksi vastaamaan tietohallinnon jatkuvuudenhallintaa tarkastelemalla. Vaikka asia onkin tiedostettu, on se saattanut vaikuttaa tutki-

muksen tuloksiin. IT:n rooli on saattanut ylikorostua ja liiketoiminnallinen puoli on vastaavasti voinut jäädä pimentoon. Riittämättömien aikaresurssien vuoksi useiden henkilöiden haastatteleminen yhdessä yrityksessä ei ollut mahdollista.

Tämä tutkimus keskittyi ainoastaan jatkuvuudenhallinnan strategiseen rooliin. Sillä ei siis pyritty selvittämään esimerkiksi jatkuvuudenhallinnan kannattavuutta tai suunnitelmien käytännön toimivuutta. Operatiivisia ratkaisuja, kuten tiedon varmennusta, analysoitiin siinä määrin, että niistä voitiin tehdä päätelmiä jatkuvuudenhallinnan roolin suhteen. Hyvät käytännöt perustuvat siihen, mikä on niiden vaikutus jatkuvuudenhallinnan rooliin, mutta niiden käytännön tehokkuutta ei kyetä arvioimaan. Esimerkiksi aktiivinen ja monipuolinen viestintä viittaa strategiseen jatkuvuudenhallintaan, mutta sen todellista vaikutusta viestin omaksumiseen ei tiedetä.

5.5 Aiheita jatkotutkimukselle

Tutkimus on toistaiseksi yksi harvoista jatkuvuudenhallinnan rooliin syventyneistä tutkimuksista. Siinä analysoidaan jatkuvuudenhallintaa yhdessätoista suuressa suomalaisessa yrityksessä. Tämä tarjoaa kuitenkin vain hyvin suppean näkemyksen jatkuvuudenhallinnan roolista ja sitä tulisikin tutkia laajemmassa mittakaavassa. Esimerkiksi pienet ja keskisuuret yritykset sekä useat eri toimialat kaipaavat tutkimusta jatkuvuudenhallinnan näkökulmasta.

Tämän tutkimuksen yhtenä rajoittavana tekijänä on haastateltavien henkilöiden tausta. Ongelma voitaisiin ratkaista toteuttamalla tutkimus, jossa haastateltaisiin erikseen sekä liiketoiminnan että IT:n jatkuvuudesta vastaavia henkilöitä samassa yrityksessä. Se antaisi selkeämmän kuvan jatkuvuudenhallinnan laajuudesta.

Mielenkiintoinen tutkimuskohde olisi toipumissuunnitelman rooli luottamuslausekkeena. Tämän tutkimuksen havainnot viittaavat siihen, että toipumissuunnitelma katsotaan tarpeelliseksi vain IT-infrastruktuurin ulkoistamistapauksissa, jolloin se toimii eräänlaisena kovenanttina. Olisi hyödyllistä tietää, parantaako toipumissuunnitelma IT:n toipumisnopeutta, mikäli sitä ei ole ulkoistettu ja mikä ulkoistamisratkaisu on yleisesti ottaen toipumisnopeuden kannalta paras.

Yritykset viestivät jatkuvuudenhallinnastaan monin tavoin, mutta tutkittavaa olisi siinä, mikä viestintätapa tai viestintämix johtaa parhaaseen omaksumistasoon tai muokkaa asenteita tehokkaimmin. Henkilöstön asenne on hyvin merkittävä tekijä jatkuvuudenhallintaperiaatteiden toteutushalukkuudelle ja siten yrityksen häiriöttömyydelle. Esimerkiksi tietoturvan laatuun vaikuttaa suuresti käyttäjien halu noudattaa ohjeita. Kaikkea ei kyetä ratkaisemaan teknisin menetelmin.

Johdon ja työntekijöiden asenteisiin vaikuttavia tekijöitä tulisi tutkia viestinnän ohella myös muista näkökulmista. Tämä tutkimus raapaisi pintaa jatkuvuudenhallinnan ha-

vaittujen hyötyjen osalta, mutta syvällisemmät tutkimukset jatkuvuuden havaituista ja todellisista eduista olisivat tarpeen. Millainen on esimerkiksi jatkuvuudenhallinnan vaikutus asiakkaan tai toimittajan imagoon yhteistyöyrityksen mielestä ja mitkä ovat tärkeimmät vaikuttavat tekijät? Millainen merkitys jatkuvuudenhallintaimagolla on käytännön liiketoimintaan ja missä määrin yrityksen jatkuvuus on riippuvainen imagosta?

Maailmanlaajuisesti jatkuvuudenhallinta tulee varmasti kasvattamaan merkitystään, sillä esimerkiksi 2000-luvun luonnonilmiöt ja verkkorikollisuus ovat vaikuttaneet monien huonosti varautuneiden yritysten toimintakykyyn. Maanjäristykset tai pyörremyrskyt eivät kenties ole merkittävin uhka Suomen yrityksille, mutta riskejä on silti olemassa valtava määrä. Esimerkiksi lumimassojen aiheuttamat sähkökatkot aiheuttivat vahinkoa tammikuussa 2011. Jatkuvuudenhallinnan tutkimus onkin arvokasta ja sitä tulisi jatkaa, sillä sen avulla voidaan turvata ja kehittää yritysten menestystekijöitä.

6 LÄHTEET

Asnar, Y. – Giorgini. P. (2008) Analyzing business continuity through a multi-layers model. Teoksessa: *Lecture Notes in Computer Science*, 212-227. Springer Berlin / Heidelberg.

BCMpedia (2010) Business Continuity Management. BCM Institute. <http://www.bcmpedia.org/wiki/Business_Continuity_Management_(BCM)>, haettu 24.5.2010.

BCM Institute (2010) BCMpedia <http://www.bcmpedia.com>, haettu 24.5.2010.

Calder, Alan (2008) *Business Continuity and BS25999: a Combined Glossary*. IT Governance Publishing, Cambridgeshire, UK.

Chung, K. – Chung, D. – Joo, Y. (2006) Overview of administrative simplification provisions of HIPAA. *Journal of Medical Systems.* Vol. 30(1), 51-55.

Devargas, Mario (1999) Survival is not compulsory: An introduction to business continuity planning. *Computers & Security*, Vol. 18(1), 35-46.

Eriksson, P. – Kovalainen, A. (2008) *Qualitative methods in business research.* SAGE Publications Ltd, London, UK.

Eskola, J. – Suoranta, J. (1996) *Johdatus laadulliseen tutkimukseen.* Lapin yliopistopaino, Rovaniemi, Suomi.

Finlex (2011a) Pelastuslaki. <http://www.finlex.fi/fi/laki/ajantasa/2003/20030468?search%5Btype%5D=pika&search%5Bpika%5D=pelastuslaki>, haettu 3.1.2011.

Finlex (2011b) Valtioneuvoston asetus pelastustoimesta 4.9.2003/787. <http://www.finlex.fi/fi/laki/ajantasa/2003/20030787?search%5Btype%5D=pika&search%5Bpika%5D=pelastussuunnitelma>, haettu 3.1.2011.

Gallagher, Michael (2007) Business continuity management: Emerging standards. *Accountancy Ireland*, Vol. 39(3), 34-36.

Ghauri, P. – Gronhaug, K. (2002) *Research methods in business studies*. Pearson Education Limited, Essex, UK.

Gibb, F. – Buchanan, S. (2006) A framework for business continuity management. *International Journal of Information Management*, Vol. 26, 128-141.

Green, R.P. – Mark, R. (2009) An executive primer on business continuity planning and related IT considerations. *CPA Technology Advisor*, Vol. 19(8), 32-33.

HB 292-2006, A practitioners guide to business continuity management (2006) Standards Australia. Standards Australia, Sydney.

Hecht, Jeffrey A. (2002) Business continuity management. *Communications of the Association of Information Systems*, Vol. 8, 444-450.

Herbane, B. – Elliott, D. – Swartz, E.M. (2004) Business continuity management: time for a strategic role? *Long Range Planning,* Vol. 37(5), 435-457.

Huoltovarmuuskeskus (2011) Huoltovarmuus Suomessa. Huoltovarmuuskeskus, Helsinki. <http://www.huoltovarmuus.fi/tietoa-huoltovarmuudesta/huoltovarmuus-suomessa/index.html/>, haettu 3.1.2011.

ISO (2010) International Organization for Standardization. <http://www.iso.org/>, haettu 22.6.2010.

Keller, S. – Powell, A. – Horstmann, B. – Predmore, C. – Crawford, M. (2005) Information security threats and practices in small businesses. *Information Systems Management*, Vol. 22(2), 7-19.

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

Kraemer, S. – Carayon, P. – Clem, J. (2009) Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security,* Vol 28(7), 509-520.

Laaksonen, M. – Nevasalo, T – Tomula, K. (2006) *Yrityksen tietoturvakäsikirja.* Oy Nordprint Ab, Helsinki 2006.

Long, John O. (2008) ITIL® *Version 3 at a glance.* Springer Science+Business Media, LLC, New York, USA.

McLoughlin, Roger (2008) What one must know about achieving BS25999-2 certification. *Journal of Business Continuity & Emergency Planning*, Vol. 3(2), 105-111.

McManus, D.S. – Carr, H.H. (2000) Risk and the need for business continuity planning. Teoksessa: *Best Practices, Volume 15: Business Continuity Planning: Protecting You'r Organization's Life,* toim. Ken Doughtry, 24-31. Auerbach Publishers Inc, Boca Ralton, FL, USA.

Messer, Ira (2009) Taking the business continuity programme to a corporate leadership role. *Journal of Business Continuity & Emergency Planning*, Vol. 4(1), 8-13.

Pfleeger, C.P. – Pfleeger, S.L. (2003) *Security in Computing.* Prentice Hall, Upper Saddle River, New Jersey, USA.

Preble, John F. (1997) Integrating the crisis management perspective into the strategic management process. *Journal of Management Studies,* Vol. 34(5), 769-791.

Richardson, Bill (1994) Crisis management and management strategy – time to "loop the loop"? *Disaster Prevention and Management,* Vol. 3(3), 59-80.

Rittinghouse, J.W. – Ransom, J.F. (2006) *Business Continuity and Disaster Recovery for InfoSec Managers*. Elsevier Digital Press, Burlington, MA, USA.

Sidosryhmäturvallisuus puolustusvoimissa (2005) Puolustusvoimien pääesikunta, turvallisuusosasto. <http://www.mil.fi/paaesikunta/paaesikunta/turvallisuus/liitteet/Sidosryhmaturvallisuus_Puolustusvoimissa_PAK_0701.pdf>, haettu 22.3.2010.

Seow, Kenny (2009) Gaining senior executive commitment to business continuity: Motivators and reinforcers. *Journal of Business Continuity & Emergency Planning*, Vol. 3(3), 201-208.

Snedaker, Susan (2007) *Business Continuity and Disaster Recovery Planning for IT Professionals.* Amorette Pedersen, Syngress Publishing, Inc., Elsevier, Inc., Burlington, MA, USA.

Standardi 4.4b. (2010) Finanssivalvonta. <http://www.rata.bof.fi/fi/Saantely/Maarayskokoelma/Rahoitussektori/4_Vakavaraisuus_ja_riskien_hallinta/Documents/4.4b.std4.pdf>

Sumner, Mary (2009) Information security threats: A comparative analysis of impact, probability, and preparedness. *Information Systems Management*, Vol. 26(1), 2-12.

Tammineedi, Rama L. (2010) Business continuity management: A standards-based approach. *Information Security Journal: A Global Perspective*, Vol. 19, 36-50.

Tilastokeskus (2011) PK-yritys. Tilastokeskus, Helsinki. <http://www.stat.fi/meta/kas-/pk_yritys.html>, haettu 22.2.2011.

Tilastokeskus (2010) Tietotekniikan käyttö yrityksissä 2010. Tilastokeskus, Helsinki.

Turner, Barry A. (1994) Causes of disaster: sloppy management. *British Journal of Management*, Vol. 5, 215-219.

Wade, Jared (2004) The weak link in IT security. *Risk Management*, Vol. 51(7), 32-37.

Valtionhallinnon tietoturvakäsitteistö (2003) Valtionhallinnon tietoturvallisuuden johtoryhmä. Edita Prima Oy, Helsinki.

von Solms, B. – von Solms, R. (2004) The 10 deadly sins of information security management. *Computers & Security*, Vol. 23, 371-376.

von Solms, Rossouw (1999) Information security management: why standards are important. *Information Management & Computer Security*, Vol. 7(1), 50-57.

von Solms, Rossouw (1998a) Information security management (1): why information security is so important. *Information Management & Computer Security*, Vol. 6(4), 174-177.

von Solms, Rossouw (1998b) Information security management (3): the code of practice for information security management. *Information Management & Computer Security*, Vol. 6(5), 224-225.

Whitman, Michael E. (2003) Enemy at the gate: Threats to information security. *Communications of the ACM,* Vol. 46(8), 91-95.

Wong, Wei N.Z. (2009) The strategic skills of business continuity managers: Putting business continuity management into corporate long-term planning. *Journal of Business Continuity & Emergency Planning*, Vol. 4(1), 62-68.

Yin, Robert K. (2009) *Case study research.* SAGE Publications, Thousand Oaks, CA, USA.

7 LIITTEET

LIITE 1 SAATEKIRJE

Haastattelupyyntö koskien yrityksenne jatkuvuudenhallintaa ja toipumissuunnittelua

Turun kauppakorkeakoulun puolesta pyydämme mahdollisuutta haastatteluun yrityksessänne. Haastattelu on osa maisterintutkielmakurssia ja sen tavoitteena on parantaa tietojärjestelmätieteen opiskelijoiden ymmärrystä erilaisten kriittisten liiketoiminnan häiriöiden johtamisesta.

Haastattelun tavoitteena on tutustua yrityksenne tietoturva-asioihin ja niiden merkitykseen jatkuvuudenhallinnassa ja toipumissuunnitelmassa.

Haastatteluteemat ovat liitettynä sähköpostiin, lisäksi haastattelija saattaa kuitenkin nostaa esiin myös muita oleellisia asioita. Haastattelun tavoitteellinen kesto on 45 minuutista yhteen tuntiin. Arvostaisimme, mikäli haastattelu olisi mahdollista toteuttaa englanniksi, mutta voimme haastatella myös suomeksi.

Tietoja käytetään kahdessa Turun kauppakorkeakoulun maisterintutkielmassa sekä pohjana laajemmalle tutkimukselle, joka käsittelee tietoturvaa suomalaisissa yrityksissä. Tulemme haastattelemaan myös muita suuria ja keskisuuria suomalaisia yrityksiä eri toimialoilla ja toimitamme Teille haastatteluanalyysien pohjalta tehdyn raportin. Kaikkea haastattelumateriaalia käsitellään luottamuksellisesti ja tutkimustulokset tullaan julkaisemaan sellaisessa muodossa, ettei yritystänne voida yksilöidä.

Otamme Teihin yhteyttä kolmen [3] arkipäivän kuluessa keskustellaksemme projektista. Mikäli Teillä on aiheesta kysyttävää, älkää epäröikö ottaa yhteyttä.

Kiitoksia ajastanne ja vaivannäöstänne.

Ystävällisin terveisin,

Jonna Järveläinen	Danish Islam	Antti Lehtimäki
KTT, tutkijatohtori	tutkielmantekijä	tutkielmantekijä

LIITE 2 HAASTATTELUTEEMAT JA -KYSYMYKSET

Disruptions

What disruptions has your company experienced?
How did it cope?
Does your company have a BCP or DRP?
What is the role of ISsec in BCP and DRP?
How vulnerable would your data be in the case of a disruption?

Strategy

Do you see the implementation of BCM or DRP as a competitive or strategic advantage or just as a business enabler?
Does the BCM improve the development of the organization?
Is the IT infrastructure outsourced?

Configuration and metrics

Does the company manage their own DRP?
Do you have all kinds of internal resources to manage disruption?
Do you have a contracted reserved supplier for crisis?
Do you have on-site, off-site (hot/cold) recovery capabilities?
How long would it take to resume normalcy after an interruption?
If an alternate process runs successfully during a sizable disruption, will it be adequate enough to replace the main business critical process for that time?

Legislation and standards

Does your company comply with any BC standard?
Do have any added incentive to conform to these standards?
Do you simply follow BC standards or they have a wider scope in the organisation?

Human resource and responsibilities

Who is responsible for BCM and DRP?
Who takes care of their implementation?
What are the backgrounds of the BCM team members?

Communication and embeddedness

How are BCM and DRP communicated in the organisation?
Does the staff in different departments know about DRP?
Is there a formal role of BCM in the organisation where there is continual reporting to senior management?
Are the employees committed to BC policies and do they execute them?

BC planning and Processes

Does the top management support the BCM and DRP?
Does the top management take part in planning of DRP and BCP?
How is the critical business functions prioritized?
How does BCM consider suppliers and customers?
What do you think is the most critical process/function in your organisation in terms of risk tolerance?

Attitudes and ownership

Are there any personal incentives to carry out BCM and DRP in the organsation?
Is there an Information security responsible in every business function?

LIITE 3 TARKASTELUKOHDAT ANALYYSISSÄ

Henkilöstö ja vastuut

1	Onko jatkuvuustiimiä?
2	Onko kriisienhallintatiimiä?
3	Jatkuvuustiimin koostumus / Jatkuvuudesta huolehtivat tahot (IT, liiketoiminnot, johto)
4	Jatkuvuustiimin johtajat (IT, liiketoiminnot, johto)
5	Kriisinhallintatiimin koostumus / Kriiseissä toimivat tahot (IT, liiketoiminnot, johto)
6	Kriisinhallintatiimin johtajat (IT, liiketoiminnot, johto)
7	Viestintävastuu jatkuvuudenhallinnasta (johto, linjaesimies, henkilöstölle, ulkopuolisille)
8	Onko määritetty raportointiketjua / toimintaprosessia?
9	Ihmisten jatkuvuusosaaminen / suunnitelmien tuntemus (tässä yhteydessä EI sitä, mitä kautta osaaminen saadaan, vaan miten hyvin osataan/tunnetaan) (valmius)
10	Organisaation IT osaaminen (vaikuttaa järjestelmien ja tietojen toipumisnopeuteen)
11	Jatkuvuussuunnittelun vastuiden määrittely (selkeä, epäselvä, ei määritelty)
12	Kriisiajan vastuiden määrittely (selkeä, epäselvä, ei määritelty)
13	Ylimääräiset henkilöstöresurssit (ristikkäinen osaaminen, toimittajilta saatava apu)

Tietovarat ja fyysiset resurssit

14	Tiedonvarmennus (mirroring, palvelinten fyysinen sijainti)
15	Onko IT infrastruktuuri ulkoistettu?
16	Tuotantolaitteiden kahdennus
17	Vaihtoehtoiset toimitilat
18	Saako BCM riittävästi taloudellisia resursseja?
19	Lähin datan palautuspiste? (viimeisin normaalitila, viime yö)

Jatkuvuussuunnittelu ja prosessit

20	Jatkuvuus- ja toipumissuunnitelmien roolit (sisällöt), ja suhteet toisiinsa (toinen, molemmat, ei kirjallista, ei lainkaan)
21	Muut dokumentit? (riskianalyysi, pelastussuunnitelma)
22	Suunnitelmien yksityiskohtaisuus? (yleinen taso, tarkka) (suunnittelun joustavuus ja luovuus -> vastuullisten improvisointi)
23	Suunnitelmien laatijat (jatkuvuustiimi, liiketoimintayksiköt)
24	Johdon osallistuminen suunnitteluun (vastuiden jakaminen)
25	Suunnitelmien laatijat = Kriisitilanteiden johtajat?
26	Riskienhallinta (uhat, haavoittuvuudet, vaikutukset, kuka tekee) (joustavuus, sulautuminen)
27	Mistä tiedot suunnitelmiin? (liiketoimintayksiköt toimittaa, jatkuvuustiimi päättelee / toteuttaa lainsäädännön tai vaatimusten mukaisesti)
28	Toimintojen priorisointiperuste (Riskianalyysi, VCA, BIA, omat arviot/mittarit)
29	Toipumissuunnitelman kattavuus (teknologia, yksikkö, divisioona, toimitusketju; kootaanko yksiköiden/divisioonien suunnitelmat yhteen ja integroidaan?)

30	Jatkuvuussuunnitelman kattavuus (teknologia, yksikkö, divisioona, toimitusketju; kootaanko yksiköiden/divisioonien suunnitelmat yhteen ja integroidaan?)
31	Räätälöinti toiminnon tai tuotteen mukaan
32	Miten toimittajat on huomioitu? (varatoimittajat, vaatimukset)
33	Toipumisaikatavoitteet / häiriöiden sietokyvyt?
34	Ylläpito, päivitys (säännöllisesti, ei lainkaan, kenen aloitteesta)
35	Testaus (säännöllisesti, ei lainkaan, kenen aloitteesta)

Viestintä ja rakenne

36	Mistä viestitään? (jatkuvuus- tai toipumissuunnitelma, tietoturva, pelastussuunnitelma)
37	Viestintäkanavat (intranet, sähköposti, koulutukset, kannustimet, harjoittelu)
38	Viestintätavat (virallinen, epävirallinen)
39	Kenelle viestitään?
40	Onko kriisiviestintä ulkoisille sidosryhmille huomioitu erikseen?
41	Onko viestintä räätälöity kohderyhmittäin?
42	Viestinnän jatkuvuus (säännöllisesti, usein, harvoin, ei lainkaan)
43	Muodollinen asema (organisaation hierarkiassa, raportointi)
44	Mistä asioista raportoidaan?
45	Kenelle raportoidaan?
46	Jatkuvuusorganisaation tukeva rooli (koordinoi, opastaa, kokoaa, tarkastaa)
47	Integroivat/tukevat koodinaattorit (epäviralliset, vapaaehtoiset, viralliset, tehtävät)

Asenteet ja sitoutuminen

48	Kannustinjärjestelmä (virallinen, jatkuvuudenhallinta, tietoturva, taloudellinen tulos, henkilökohtainen, osastottainen, yleinen)
49	Jatkuvuudenhallinnan valvonta (sisäinen tarkastus, koordinaattori, linjaesimies)
50	Tietoturvan valvonta (sisäinen tarkastus, koordinaattori, linjaesimies)
51	Miksi jatkuvuudenhallintaa on toteutettu (ydinajuri)? (lainsäädäntö, asiakkaat, kilpailijat, liiketoiminnan strategia ja tavoitteet)
52	Eroaako jatkuvuudenhallinta kilpailijoiden vastaavista? (tiettävästi)
53	Toimintaan vaikuttavat erityissäädökset/viranomaiset?
54	Noudatetaanko standardeja?
55	Sertifioidaanko standardeja?
56	Kannustimet standardien noudattamiselle
57	Onko BCM auttanut tunnistamaan yrityksen oleelliset toiminnot/prosessit/resurssit/uhat/haavoittuvuudet?
58	Onko BCM auttanut säilyttämään arvoa?
59	Onko BCM kilpailuetu / organisationaalinen etu?
60	Tukeeko johto BCM:ia? Miten? (Ei pelkkä kuluerä, jota ei oteta vakavasti)
61	Onko henkilöstö sitoutunut jatkuvuudenhallintaan?
62	Onko henkilöstö sitoutunut tietoturvaperiaatteisiin?
63	Onko resurssit, joilla selvitä häiriöistä?
64	Noudatetaanko standardeja / lainsäädäntöä vähimmäismitassa vai onko suurempi rooli?
65	Alan lainsäädännön tiukkuus?