TIETOHALLINNON JATKUVUUDENHALLINTA VALIKOIDUISSA SUOMALAISISSA SUURYRITYKSISSÄ VUONNA 2010

Jonna Järveläinen & Antti Lehtimäki

Sarja/Series KR-2:2011

Turun kauppakorkeakoulu
Turku School of Economics

ISBN 978-952-249-162-6 (nid.) 978-952-249-163-3 (PDF)
ISSN 0357-4687 (nid.) 1459-7632 (PDF)
UDK 65.012.45
65.012.2
65.017
658.11
658.512.3

65.012.45

Uniprint, Turku 2011

TIIVISTELMÄ

Tässä tutkimuksessa selvitettiin suomalaisten suuryritysten tietohallinnon jatkuvuudenhallintaa (engl. business continuity management, jatkossa myös BCM). Suuryrityksillä tarkoitetaan yli 250 henkilöä työllistäviä yksityisen sektorin organisaatioita, ja tutkimuksen puitteissa tehtiin 18 yrityksen tietohallinnosta tai tietoturvasta vastaavien haastattelua vuonna 2010. Haastattelut pohjautuivat Herbane, Elliot ja Swartzin (2004) julkaisemaan tieteelliseen viitekehykseen, jossa tutkittiin jatkuvuudenhallinnan strategisuutta Iso-Britannian pankki- ja vakuutussektorilla.

Tutkimuksen tuloksista käy ilmi, että monissa haastatelluissa organisaatioissa tietohallinnon BCM:llä on strateginen asema, mutta suurimmassa osassa haastateltuja yrityksiä se oli enemmän liiketoimintaa tukevassa asemassa. Haastatteluista kävi kuitenkin ilmi, että monissa yrityksissä liiketoiminta pysähtyy tai merkittävästi hankaloituu, kun kriittisissä tietojärjestelmissä on vakava häiriö, minkä vuoksi jatkuvuudenhallintaa myös tietohallinnon näkökulmasta tulisikin suunnitella ja johtaa organisaation ylimmästä johdosta asti operatiivisen toiminnan jäädessä liiketoimintayksiköihin ja tietohallintoon.

Lähes kaikissa yrityksissä oli kirjalliset jatkuvuudenhallinnan- tai toipumissuunnitelmat vähintään kriittisimmille tietojärjestelmille ja joissain niitä testattiin säännöllisesti. Suurin osa haastatelluista kertoi, että ylin johto osallistui jollain tavalla jatkuvuudenhallintaan ja suunnitelmien teko oli hajautettu liiketoimintayksiköihin. Suunnitelmat olivat vain asianosaisten saatavilla, eikä niistä kerrottu kaikille työntekijöille, mikä aiempien tutkimusten mukaan vaikeuttaa henkilökunnan sitouttamista häiriöttömän liiketoiminnan tavoitteluun. Muutosten hallinta näytti jatkuvuuden kannalta olevan yksi hankalimmista riskeistä, mutta yleisimmin oli varauduttu infrastruktuurin hajoamiseen tai tietoturvariskeihin.

Monissa suurimmissa yrityksissä oli ulkoistettu paljon IT-palveluita ja/tai infrastruktuuria, mutta pilvipalvelut (Software as a Service) eivät olleet vielä yleisiä, ainakaan vähemmän ulkoistaneissa pienemmissä yrityksissä. Tutkimuksessa selvisi useita hyviä käytänteitä, ja raportin lopussa onkin annettu muutamia suosituksia näihin pohjautuen.

SISÄLLYS

1 JOHDANTO

”Anteeksi, nyt kestää hetken. Tämä tietokone ei nyt toimi.”, kommentoi yhä useampi lääkäri, asiakaspalvelija, kassahenkilö, tullivirkailija jne. odottavalle asiakkaalle. Yritykset ovat tulleet hyvin riippuvaisiksi tietojärjestelmistä, ja kun tietokoneet eivät toimi, usein koko liiketoiminta on pysähdyksissä. Jotkut näistä keskeytyksistä ylittävät myös uutiskynnyksen, kuten maksuliikenneongelmat syksyllä 2010 Stockmannin Hulluilla Päivillä, mitkä hidastivat merkittävästi kaupantekoa muutamien ensimmäisten tuntien aikana. Uutiskynnyksen ylittävillä tietojärjestelmäongelmilla voi olla vaikutusta myös yrityksen imagolle, kuten Sampo Pankin ja Den Danske Bankin tietojärjestelmäfuusion aikana, jolloin kymmenet tuhannet asiakkaat vaihtoivat pankkia (Luoma-aho & Paloviita 2010).

Kriittisten tietojärjestelmien jatkuvan toiminnan keskeytyminen onkin noussut monien IT-osastojen suurimmaksi riskiksi (Ernst & Young 2010). Tietoteknisten häiriöiden vuoksi liiketoiminnalle aiheutuu usein merkittävää haittaa, ja tietotekniikalla on nykyään myös strategista merkitystä yrityksen liiketoiminnalle. Tämän vuoksi myös yrityksen liikejohdon tulisi olla kiinnostunut järjestelmien jatkuvuudesta. Enää ei pelkkä varmuuskopiointi riitä, vaan toipumissuunnitelmien lisäksi tarvittaisiin etukäteisvalmistautumista erilaisiin kriittisiin tietojärjestelmien ongelmiin, eli jatkuvuudenhallintaa (Herbane et al. 2004).

Tässä tutkimuksessa selvitetään, miten suomalaisissa suuryrityksissä tietohallinnon jatkuvuutta hallitaan, ja onko sillä strategista roolia yrityksessä. Tutkimuksen puitteissa haastateltiin 18 suomalaisten suuryritysten tietohallinnossa toimivaa päällikköä ja johtajaa vuonna 2010. Haastattelukysymykset keskittyivät jatkuvuudenhallintaan, mutta myös tietoturva-asioita, viestintää ja vastuita kartoitettiin. Haastatteluja tekivät Turun kauppakorkeakoulun tietojärjestelmätieteestä kaksi maisteritutkielman tekijää sekä tutkijatohtori, ja kevään sekä kesän 2010 haastatteluja on käytetty aineistona tekijöiden pro gradu-tutkielmissa.

Tutkimus on tehty Liikesivistysrahaston tukemana, mistä olemme erittäin kiitollisia. Kiitämme Essi Sarua kielioppiavusta. Kiitokset myös tutkimuksen johtajalle professori Reima Suomelle, joka on antanut tekijöille riittävän vapaat kädet toteuttaa tutkimusta itsenäisesti. Haluamme lisäksi kiittää Danish Islamia, jolla oli merkittävä rooli haastatteluiden valmistelussa, tekemisessä ja litteroimisessa sekä kaikkia haastateltavia mielenkiintoisista tiedoista.

2 AIKAISEMMAT TUTKIMUKSET

Jatkuvuudenhallinta (business continuity management, BCM) on melko uusi termi tieteellisissä julkaisuissa. Se voidaan ymmärtää kattokäsitteenä, joka sisältää useita iäkkäämpiä riskienehkäisy- ja toipumisprosesseja kuvaavia termejä kuten kriisienhallinnan (crisis management), valmiussuunnittelun (contingency planning) ja operatiivisen riskien hallinnan (operational risk management). Käsitteistä löytyy kuitenkin myös yhtäläisyyksiä ja niiden perusajatuksena on aina yrityksen toiminnallisuuden ylläpitäminen sekä häiriöiden hallinta. (Copenhaver & Lindstedt 2010; HB 292-2006 2006)

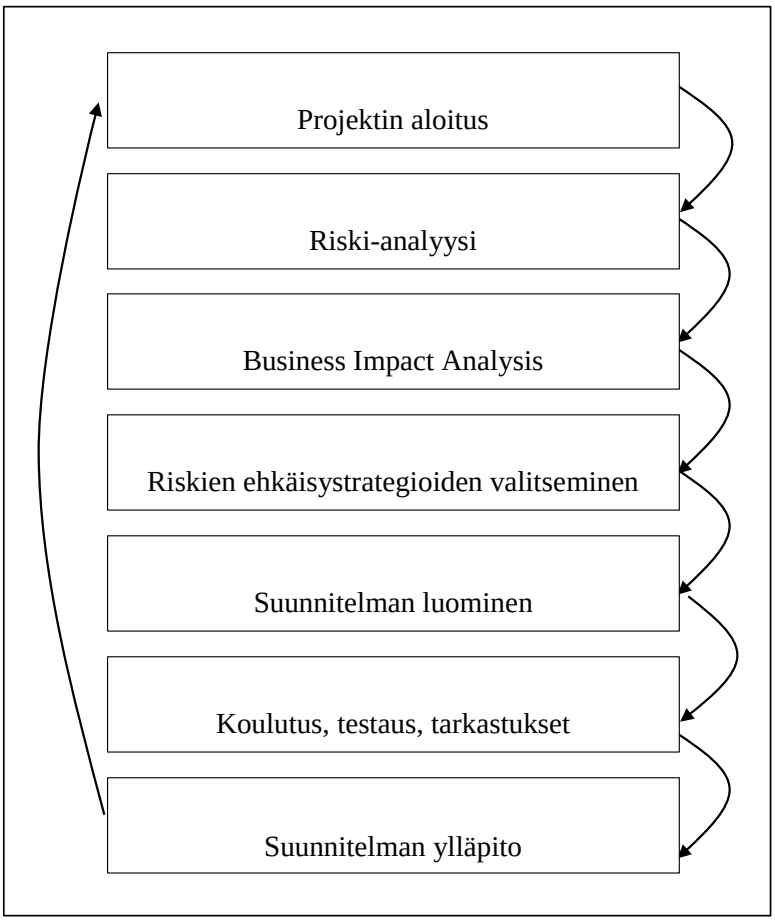
BCM:llä tarkoitetaan kaikkia niitä prosesseja, joilla ensin tunnistetaan yrityksen uhkatekijät ja haavoittuvuudet, sitten arvioidaan niiden mahdolliset vaikutukset ja lopulta suunnitellaan ja toteutetaan ehkäisytoimenpiteet, joilla riskejä ehkäistään ja minimoidaan haitallisia vaikutuksia – sekä ennalta, että tarvittaessa reagoiden. BCM:n 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 (Devargas 1999; Gibb & Buchanan 2006; Hecht 2002; Herbane et al. 2004).

On tärkeää huomata, että kokonaisvaltainen jatkuvuudenhallinta on koko yrityksen kattavaa ja luonteeltaan sosioteknistä. Se huomioi siis myös IT:n ulkopuoliset toiminnot sekä teknisen toteutuksen lisäksi myös ihmiset (Gibb & Buchanan 2006; Hecht 2002; Herbane et al. 2004). Henkilöstöä tulee kouluttaa, heille tulee viestiä ja heidät tulee pyrkiä sitouttamaan BCM-periaatteiden mukaiseen toimintaan, sillä suunnitelmien olemassa olo ei auta, mikäli kukaan ei toteuta tai tunne niitä. Jatkuvuudenhallintastandardi BS25999:kin kehottaa yritystä rakentamaan organisaatiokulttuurin, joka edistää jatkuvuudenhallintaa (Gallagher 2007).

2.1 Suunnitteluprosessi

Yksi jatkuvuudenhallinnan tärkeä ilmentymä on jatkuvuussuunnitelma, sillä sen muodostaminen pakottaa yrityksen tutkimaan omaa toimintaansa ja toimintaympäristöään. Suunnitteluprosessi sisältää aina tietyt perusasiat, jotka Snedaker (2007) on jakanut prosessin seitsemään eri vaiheeseen. 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 vaiheet esiintyvät myös Gibbin ja Buchananin (2006), Rittinghousen ja Ransomin (2005) sekä Devargasin (1999) julkaisuissa. Kuvio 1 esittää Snedakerin (2007, 31-35) mallin prosessista.



Kuvio 1. Jatkuvuussuunnitteluprosessi (Snedaker, 2007)

Vaikka jatkuvuussuunnittelu on prosessi, pitää se aloittaa, kuten mikä tahansa projekti, määrittelemällä vastuut, tavoitteet, vaatimukset, aikataulut ja budjetit. Mikäli jatkuvuudenhallinta ei ole syntynyt johdon aloitteesta, tulee ajatus myydä myös heille. Yritysjohto täytyy kyetä motivoimaan osoittamalla jatkuvuuden suunnittelun ja johtamisen liiketoiminnallinen kannattavuus sekä sen tuoma lisäarvo. (Hecht 2002; Laaksonen et al. 2006; Seow 2009; Snedaker 2007)

Riskianalyysissa pyritään tunnistamaan mahdolliset kriisinaiheuttajat sekä niiden syyt. Tässä vaiheessa tutkitaan yrityksen uhkia, haavoittuvuuksia sekä uhkien välttämiseksi käytettäviä suojakeinoja ja havaintojen pohjalta määritellään

uhkien toteutumisten todennäköisyyksiä ja vaikutuksia. Riskianalyysivaiheessa seurauksia tarkastellaan siis toteutuneiden ja mahdollisten uusien uhkien näkökulmasta. Siinä etsitään mahdollisesti haitallisia seurauksia aiheuttavat tekijät ja arvioidaan, kuinka ne voivat vaikuttaa organisaation toimintaan. (Snedaker 2007)

Tämän lisäksi yrityksen tulee tehdä myös liiketoiminnallinen vaikutusanalyysi (business impact analysis, BIA), joka lähestyy asiaa liiketoimintaprosessien kautta. Se on jatkuvuussuunnittelun kulmakivi (Snedaker 2007; Tammineedi 2010). Liiketoiminnallisen vaikutusanalyysin tarkoituksena on kertoa, minkälainen vaikutus tietyn järjestelmän toimimattomuudella on yritykselle. Sen perusteella voidaan päätellä, mitkä tietojärjestelmät ovat liiketoiminnan kannalta kriittisimpiä. Suurennuslasin alla ei siis ole se, mikä aiheuttaa kyseisen jatkuvuusongelman. Liiketoiminnallinen vaikutusanalyysi antaa jatkuvuudenhallinnalle rajat osoittamalla tärkeät ja vähemmän tärkeät järjestelmät. Näin resurssit käytetään suojelemaan yrityksen kannalta merkittävimpiä prosesseja. (Devargas 1999; Snedaker 2007; Tammineedi 2010)

Edellisten vaiheiden jälkeen voidaan etsiä ja arvioida ne vaihtoehdot, joita tunnistettujen riskien hallitsemiseksi on käytettävissä. Jotta yritys voisi valita haitallisten vaikutusten minimoimiseksi sovellettavat toimintatavat ja -mallit, sen tulee ensin valita strategiat, jolla riskejä pyritään ehkäisemään (Gibb & Buchanan 2006; Snedaker 2007; Sumner 2009). Näitä ovat välttäminen, siirtäminen ja rajoittaminen. Lisäksi strategiaksi lasketaan myös sellaisen riskin hyväksyminen, jolla ei ole vaikutusta riskiin. Riskeille voi olla olemassa useita ehkäisytapoja, joissa sovelletaan eri strategiaa. (Gibb & Buchanan 2006). 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 suuri vaikutus että korkea todennäköisyys, kanavoidaan myös eniten resursseja. (Gibb & Buchanan 2006; Sumner 2009)

Suunnitelmien luomisvaiheessa kaikki edellisissä vaiheissa kerätyt tiedot nivoutuvat yhteen ja niitä käsitellään yksityiskohtien tasolla. Lisäksi tulisi luoda erillinen ylläpitosuunnitelma, josta ilmenee esimerkiksi, miten organisationaaliset tai toimintaympäristöön liittyvät muutokset huomioidaan suunnitelman ylläpidossa. Toipumissuunnitelmaan luodaan kommunikaatiosuunnitelma, jotta tiedetään, mistä asioista kriisitilanteessa tulee tiedottaa, kenelle informaatio suunnataan, milloin tiedon pitää liikkua ja mitä tiedotuskanavaa pitkin se siirretään. Kun suunnitelmaa muodostetaan, 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. Lisäksi suunnitelmalle asetetaan aktivointikriteerejä, joiden täyttyessä avainhenkilöt tietävät ryhtyä toimiin. (Snedaker 2007)

Suunnitelmien valmistumista seuraa koulutus-, testaus- ja tarkastusvaihe. Koulutuksella tarkoitetaan sitä, että henkilöstölle viestitään jatkuvuudenhallinnasta – sen hyödyistä ja tavoitteista (Gibb & Buchanan 2006). Avainhenkilöille kirkastetaan heidän roolinsa ja vastuunsa suunnitelmassa sekä opetetaan ne taidot, joita heiltä edellytetään (Snedaker 2007). Testaus taas on keino arvioida jatkuvuussuunnitelman toimintatapojen toimivuutta käytännössä (Tammineedi 2010). 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 testatessa myös koulutetaan väistämättä henkilöstöä (Snedaker 2007). Riskienehkäisystrategioiden ja toipumissuunnitelmien toimivuutta sekä koko jatkuvuussuunnitelmaa tulee testata ja tarkastaa riittävän usein ja kattavasti, jotta voidaan varmistua niiden ajantasaisuudesta (Gibb & Buchanan 2006; Snedaker 2007).

Suunnitelmat on luotu tietyllä ajanhetkellä vallinneen tilanteen ja saatavilla olleen informaation perusteella. Tilanteiden ja tietojen muuttuessa tulee siis myös jatkuvuus- ja toipumissuunnitelmien muuttua. Ylläpidolla varmistetaan BCM:n kyvykkyys, tehokkuus ja ajantasaisuus. Se saavutetaan valvomalla muutoksia, arvioimalla niiden vaikutuksia suunnitelmiin, sekä toteuttamalla tarvittavat ja taloudellisesti kannattavat sopeutustoimet. (Tammineedi 2010).

Suunnitelman 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 vuoksi. 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). Ylläpidonkin perusperiaatteet tulee olla kirjattuna jatkuvuussuunnitelmaan (Tammineedi 2010).

2.2 Jatkuvuudenhallinnan strategisuus

Jatkuvuudenhallinnan tarkoitus ei ole ainoastaan luoda yritykselle dokumentoitua toimintaohjetta, joka kaivetaan esiin kriisin sattuessa. Sen tavoitteena on turvata operaatioiden jatkuvuus aktiivisella toiminnalla ja antaa siten vakaa pohja yrityksen kilpailukyvylle. Sen lisäksi, että BCM auttaa säilyttämään saavutettuja etuja, se voi muodostua myös itsessään strategiseksi 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. BCM:ää ei tulekaan nähdä vain toiminnallisena, rajattuna

prosessina, vaan kyvykkyytenä, joka tukee organisaation kehittymistä ja strategisten tavoitteiden saavuttamista. (Herbane et al. 2004).

Herbane ym. (2004) ovat tutkineet BCM:n roolia. Heidän mielestään strategisen BCM:n tulisi olla luonteeltaan sosioteknistä, kattaa yhden toiminnon sijasta koko organisaatio sekä tuottaa hyötyä ja arvoa pitkällä tähtäimellä. Näiden ominaisuuksien lisäksi Herbane ym. (2004) erittelevät tutkimuksessaan neljä tekijää, joiden avulla yrityksen jatkuvuudenhallinnan roolia voidaan arvioida. Nämä tekijät ovat toipumisnopeus (speed), joustavuus (configuration resilience), pakollisuus (obligation) ja sulautuminen (embeddedness).

Toipumisnopeus on kriittistä BCM:ssä. Yleisestikin ottaen kyky saavuttaa tavoitteet kilpailijoita nopeammin on yrityselämässä merkittävä strateginen kilpailuetu. Herbane ym. (2004) 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. Toipumisnopeus on Herbanen ja kumppaneiden (2004) mukaan kyvykkyys, jonka taso riippuu siitä, kuinka nopeasti ongelmat havaitaan, miten tehokkaasti niiden hoitaminen on organisoitu ja kuinka hyvin niihin on valmistauduttu ennalta.

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 et al. 2004).

Sulautuminen on jatkuvuudenhallinnan strategisuutta ilmentävä tekijä, joka kuvaa, missä määrin BCM-periaatteet ovat levittäytyneet osaksi koko yritystä, sen henkilöstöä ja toimintatapoja. Sulautumista on havaittavissa, mikäli strateginen jatkuvuusajattelu on levinnyt myös ylimmän johdon ulkopuolelle saaden aikaan henkilöstön sitoutumista sen periaatteisiin ja tavoitteisiin. BCM ei tällöin ole yritykselle ainoastaan dokumentoitu suunnitelma, vaan osa päivittäistä toimintaa yksilötasolla asti. Herbane ym. (2004) ovat sitä mieltä, että sulautuminen on ehdoton edellytys jatkuvuudenhallinnan strategiselle roolille, koska vain sulautuneet prosessit voivat tukea yrityksen pitkän tähtäimen strategisia tavoitteita. Muussa tapauksessa BCM on vain ajoittain ilmenevä tukitoiminto, jonka rooli jää operatiiviseksi.

Organisaation BCM-periaatteet 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 BCM:n toteuttamiseen. (Herbane et al. 2004).

BCM:n roolia yrityksessä voidaankin tarkastella pakollisuuden asteen avulla. Ensin tulee selvittää, mitä jatkuvuudenhallintaan kuuluvia asioita yritykseltä vaaditaan esimerkiksi laeilla, minkä jälkeen vaatimuksia voidaan verrata yrityksen toimintaan. Organisaatio voi valita, noudattaako se määräyksiä kirjaimellisesti vai syvällisemmin. Minimivaatimusten ylittäminen viittaa siihen, että yritys tiedostaa jatkuvuudenhallinnan arvon ja käyttää sitä hyödyksi tavoitteidensa saavuttamisessa. Se on samalla osoitus BCM:n strategisemmasta roolista. Eri toimialoilla ja eri yrityksillä saattaa kuitenkin olla erilaisia jatkuvuudenhallintavaatimuksia, joten määräysten ylittämisen merkitystä tulee aina pohtia tapauskohtaisesti. (Herbane et al. 2004).

3 MENETELMÄT

Tarvittiin empiiristä aineistoa, jotta voitiin vastata tutkimuskysymykseen ” miten suomalaisissa suuryrityksissä tietohallinnon jatkuvuutta hallitaan ja onko sillä strategista roolia yrityksessä”. Koska BCM:ää on tutkittu vielä verrattain vähän ja halusimme myös selvittää muutamia tietoturvaan liittyviä kysymyksiä, päädyimme henkilökohtaisiin haastatteluihin. Tähän vaikuttivat aikaisemmat tutkimukset (Kotulic & Clark 2004; Albrechtsen & Hovden 2009), joissa on havaittut, että yritykset vastaavat nihkeästi lomakekyselyissä tietoturvakysymyksiin.

Päätimme keskittyä tutkimuksessa suuriin yksityisellä sektorilla toimiviin yrityksiin, joiden oletettiin omaavan jatkuvuudenhallintaan liittyviä käytänteitä laajemmin sekä syvällisemmin kuin pienemmät tai julkiset organisaatiot. Suurina yrityksinä käsitettiin Tilastokeskuksen määritelmän mukaan yli 250 henkilöä työllistäviä organisaatioita. Toisena kriteerinä yritysten valinnassa käytettiin toimialaa. Haastateltavia haluttiin monilta eri toimialoilta, jotta saataisiin mahdollisimman kattava kuva ilmiöstä. Näiden kriteerien avulla etsittiin tietoa erilaisista yrityksistä esim. Internet-sivuilta sekä Fonecta Profinder-palvelusta. Käytännöllisistä syistä ensimmäiset haastatellut yritykset pyrittiin valitsemaan Turun seudulta, koska haastattelijoina toimivat opiskelijat niin toivoivat. Myöhemmin maantieteellistä aluetta laajennettiin Länsi- ja Etelä-Suomeen.

Kriteerit täyttävistä yrityksistä etsittiin edelleen Internet-sivujen, Fonecta Profinder-palvelun sekä henkilökohtaisten kontaktien avulla tietohallinnosta tai tietoturvasta vastaavia henkilöitä, ja heitä lähestyttiin sähköpostitse sekä puhelimitse. Keväällä 2010 haastattelupyyntöjä lähetettiin yhteensä 25 yritykseen ja syksyllä 31 yritykseen, lisäksi muutamat tutkijat Turun kauppakorkeakoulun tietojärjestelmätieteessä lähestyivät omia kontaktejaan haastattelupyynnöin (lukumäärästä ei ole tarkkaa tietoa). Kevät-kesällä haastatteluja tehtiin yhteensä 11, joista kolme tehtiin pääkaupunkiseudulla. Syksyllä tehtiin yhteensä 7 haastattelua, joista 5 pääkaupunkiseudulla. Saatu haastatteluaineisto on pieni, eikä sen perusteella ole tarkoitus tehdä yleistyksiä vaan kuvailla nykytilannetta.

Haastattelut kestivät yleensä noin 45–60 minuuttia, muutama lyhyempi ja pidempi mahtui myös joukkoon. Kaikki haastattelut nauhoitettiin, lukuun ottamatta yhtä, jossa haastateltava kieltäytyi nauhoituksesta; tässä tapauksessa molemmat haastattelijat tekivät muistiinpanoja, joiden pohjalta analyysi voitiin tehdä. Nauhoitukset litteroitiin jälkeenpäin ja niissä tapauksissa, joissa haastateltava oli pyytänyt nähdä kirjallisen dokumentin, litterointi lähetettiin sähköpostilla tarkastet-

tavaksi. Nauhoitukset tuhottiin tämän jälkeen. Kustakin haastattelusta kertyi noin 8-12 sivua litteroituna, joten materiaalia on runsaasti.

Taulukossa 1 esitellään haastatellut yritykset sekä haastateltavat. Kahdessa haastattelussa oli useampi haastateltava, jotka olivat yhtä aikaa haastateltavina. Toimialaluokitus on hyvin väljä, koska emme halua paljastaa yrityksiä. Kuten sanottu, 8 haastattelua tehtiin pääkaupunkiseudulla, ja loput Turun seudulla. Lisäksi 10 yritystä toimii useissa maissa, ja 5 Suomessa useissa kaupungeissa.

Taulukko 1. Tutkimuksen haastateltavat.

	Toimiala	Työntekijöiden määrä	Haastateltavan asema
1	IT	1 000	Tietohallintopäällikkö
2	IT	5 000	Senior manager, IT assurance
3	IT	17 000	Tietohallintojohtaja
4	Palvelu	510	Tietohallintojohtaja
5	Palvelu	700	ICT manager
6	Palvelu	2 300	Talousjohtaja
7	Palvelu	2 500	Tietoturvapäällikkö
8	Palvelu	7 000	Yritysturvallisuusjohtaja
9	Pankki ja vakuutus	390	Tietohallintopäällikkö
10	Pankki ja vakuutus	1 000	IT-palvelupäällikkö
11	Pankki ja vakuutus	5 100	Turvallisuusjohtaja, Riskienhallinta-johtaja
12	Pankki ja vakuutus	8 000	Tietoturvajohtaja
13	Tuotantoteollisuus	250	Järjestelmäpäällikkö
14	Tuotantoteollisuus	600	IT manager
15	Tuotantoteollisuus	1 100	Tietoturvajohtaja
16	Palvelu	3 000	Tietoturvajohtaja
17	Tuotantoteollisuus	4 500	Tietohallintojohtaja, Tietoturvapäällikkö, Tietoturva-asiantuntija
18	Tuotantoteollisuus	24 000	Tietoturvajohtaja

Tulokset on analysoitu Herbanen et al.:n (2004) teoreettisen viitekehyksen perusteella. Kukin litteroitu haastattelu on luettu useampaan kertaan. Kullakin kerralla kerättiin avainsanoja ja mielenkiintoisia havaintoja, jotka dokumentoitiin mindmap-tyyliseen puurakenteeseen ja ryhmiteltiin viitekehyksen mukaan. Havaintoja on vertailtu kahteen aiemmin mainittuun maisteritutkielmaan sekä teoriaan, jonka jälkeen nämä havainnot on sitten tiivistäen raportoitu seuraavaan lukuun.

Luvun lopussa on tehty yhteenvetomainen analyysi jatkuvuudenhallinnan strategisuudesta haastatelluissa yrityksissä. Menetelmä on kuvattu tarkemmin ko. alakappaleessa. Tässä raportissa kuvatut tulokset ovat kuitenkin alustavan analyysin tuloksia, joilla kuvaillaan nykytilannetta ja syvempi tulkinta jätetään jatkotutkimukseen.

4 TULOKSET

Jatkuvuudenhallinta määriteltiin haastatelluissa yrityksissä useimmiten varautumisena erilaisiin liiketoiminnan häiriötilanteisiin. Tietohallinnon näkökulmasta sen tavoitteena on varmistaa, että liiketoiminnalle tärkeimmät tietojärjestelmät ovat käytettävissä, silloin kun niitä tarvitaan. Pankki- ja vakuutussektorilla BCM määriteltiin myös operatiivisten riskien hallinnaksi erotuksena liiketoimintariskien hallinnasta. Jatkuvuudenhallinta ei siis ole vain uusi nimitys riskienhallinnalle, vaan niillä on joitakin yhtymäkohtia. Esimerkiksi jatkuvuussuunnitelmia tehtäessä määritellään, mitä riskejä kriittisille järjestelmille on olemassa ja kuinka niitä käsitellään. Tutkimuksen mukaan kaikki näyttää kulminoituvan siihen, että asiakkaalle ei saa näkyä jatkuvuusongelmia; siten jatkuvuudenhallinta voi olla vaikka osa tuotannon laadun varmistusta.

> *”…näkisin ehkä tämän jatkuvuudenhallinnan työkaluna riskienhallinnalle. Jatkuvuudenhallinnalla haetaan sitä, että mikä on se riskitaso mille me halutaan tämä palvelu asettaa. Ja sitten taas bisneksen puolelta tulee tiettyjä tarpeita, että nämä asiat on meille kriittisiä ja halutaan ajaa joko matalalla tai kohtalaisella riskillä ja sitä kautta me mietitään IT:n puolella, että minkälaisia ratkaisuja pitää rakentaa. […]. Ja mun mielestä se riskienhallinta määrittää sen, että kuinka paljon rahaa meidän kannattaa pistää sen kyseisen palvelun jatkuvuuteen.”*

> *”Jos jatkuvuudenhallinta saisi päättää, autossa olisi neljä vararengasta, mutta koska riskienhallinta tietää jotain todennäköisyyksistä, siinä on vain yksi“*

4.1 Suunnitelmat

Tietojärjestelmien jatkuvuussuunnitelmien teko oli yli tuhannen hengen yrityksissä hajautettu liiketoimintayksiköille, kun taas pienemmissä IT-osasto tai järjestelmien omistajat hoitivat suunnitelmat. Vain yhdessä pienessä yrityksessä ei ollut tehty IT-järjestelmien toipumissuunnitelmaa. Kolmessa muussa pääkaupunkiseudun ulkopuolella haastatellussa yrityksessä oli dokumentoitu lähinnä periaatteet toipumiselle, mutta ei järjestelmäkohtaisesti. Syynä dokumentoinnin puuttumiselle annettiin väistämättä massiivisen dokumentoinnin ylläpidon mahdotto-

muus. Muutamassa yrityksessä viime vuosina oli suunnitelmien tekoa selkeytetty niin, että jatkuvuusvastuuta oli yritetty siirtää enemmän liiketoimintaan, IT-asiantuntijoiden roolin muodostuessa enemmän neuvovaksi ja operatiiviseksi kriisin sattuessa.

Useimmiten suunnitelmien tekemisen taustalla olivat yrityksen ulkoiset vaatimukset. Joissain tapauksissa asiakkaat olivat vaatineet jatkuvuussuunnitelmia, joissain tapauksissa viranomaiset. Lisäksi erityisesti ulkomaisissa pörsseissä listautuneiden yritysten tuli noudattaa SOX-vaatimuksia, joiden vuoksi myös tietojärjestelmien palautumiskyvyn tulee olla hyvä (Elliott et al. 2001).

Riskianalyysin tai liiketoiminnan vaikutusanalyysin olivat tehneet lähes kaikki yritykset. Usein aloitettiinkin jatkuvuussuunnitelmien teko pohtimalla, mitkä järjestelmät olivat kriittisimpiä liiketoiminnalle, esimerkiksi keskustelemalla liiketoiminnan asiantuntijoiden kanssa.

> *”No itse asiassa me laitettiin [..] palvelujen omistajille tuota heidän järjestelmistä meille listaus ja pyydettiin ilmoittamaan, kuinka kriittinen se on heidän tuotannolle...”*

Vaikuttavuusanalyysi voitiin tehdä yksinkertaisen tehokkaasti, kuten yllä lainauksessa on kuvailtu. Eräässä yrityksessä jokaiselle järjestelmälle käytettiin Cobit-mallin mukaista kysymyspatteristoa arvioimaan sen kriittisyyttä, ja tämä arviointi tehtiin myös uusille järjestelmille. Yhdessä organisaatiossa tehtiin järjestelmille myös ns. arvoketjuanalyysi, jossa pohdittiin myös mitkä muut yksiköt tarvitsivat ko. järjestelmää. Tämä tieto kerättiin tietoturvaosastolle, jotka sitten häiriön sattuessa pystyivät informoimaan myös näitä muita yksiköitä.

> *”Me käytämme sanaa ydinprosessi, se on yhtä kuin kriittinen […] Kaikkein kriittisin josta se alkaa, on sellainen prosessi, jonka nimi on ”XXX” –prosessi. Se on se meidän kaikkein kriittisin prosessi, koska sillä saadaan sitä asiakaskantaa talon sisälle. Ilman sitä ei tapahdu mitään. […] On tärkeää, että ihminen kun toteaa, että aamulla herään ja olen sairas, haluan päästä tänään lääkäriin. Jos se prosessi ei pelitä, niin silloin se asiakaskaan ei tule meille – menee kilpailijoille tai jonnekin muualle.!*

Tietojärjestelmien kriittisyyden perusteena suurimmassa osassa yrityksiä oli, että asiakkaalle ei saa näkyä mitään, jolloin tuotannon ja asiakaspalvelun oli toimittava; jos asiakas huomaa ongelmat, on monesti kyseessä myös yrityksen maine. Muutamassa organisaatiossa priorisointi oli tehty käyttäjämäärän perusteella, eli kuinka monen työt keskeytyisivät, jos ko. järjestelmä olisi alhaalla. Taloudelliset syyt priorisoinnille mainitsi myös moni haastateltava. Järjestelmien varmistuksiin oli käytetty paljon resursseja, esimerkiksi jos vahingot olisivat ”miljoonaluokkaa”, pörssiraportointi tai uusien tuotteiden kehitystyö viivästyisi. Eräässä yrityksessä mainittiin, että toiminnanohjausjärjestelmän varmistuksissa raha ei ollut esteenä, koska jos laskutettavia tunteja ei voida merkitä järjestelmään, yri-

tyksen talous olisi vaikeuksissa. Useammat haastateltavat mainitsivat myös, että tiedon saatavuus oli liiketoiminnan kannalta tärkeämpää kuin luotettavuus tai eheys, tästä poikkeuksena pankki- ja vakuutussektori ja terveydenhuoltoala.

Suuremmissa organisaatioissa oli yleensä tehty ohjeistuksia, malleja, linjauksia jatkuvuussuunnitelman tekoon, jonka pohjalta yksittäiset suunnitelmat tehtiin. Malleja oli saatu esim. Internetistä, konsulteilta sekä erilaisista standardeista (ISO27001-27002, BS17799, BS 25777, BS 25999, Vahti) ja governancemalleista (ITIL, Cobit, ISF). Vain yksi IT-sektorin yritys oli hankkinut sertifikaatteja, joita tarvittiin pörssilistattujen ja julkishallinnon asiakkaiden vaatimuksesta. Monet yritykset kuitenkin poimivat liiketoimintaansa sopivia käytäntöjä standardeista, ja osa haastateltavista myös koki niiden noudattamisesta olevan markkinoinnissa hyötyä.

Ohjeistuksissa oli selostettu, mitä dokumentin tulee vähintään sisältää ja kuinka järjestelmiä priorisoidaan (esim. henkilöturvallisuus, asiakasvaikutus, vaikutus henkilökuntaan jne.). Eräässä organisaatiossa oli tehty jatkuvuussuunnittelulle kolmisivuiset periaatteet, joissa mm. kerrotaan seuraavat asiat:

- jatkuvuusjärjestelyt eivät saa tulla kalliimmiksi kuin liiketoiminnan keskeytyminen
- ennakkoon varautuminen on yleensä helpompaa ja edullisempaa kuin jälkikäteen korjaaminen
- miten suunnitelma laaditaan, päivitetään, koulutetaan ja testataan (sisältäen testausmenetelmät ja -syklit)

Yhdessä yrityksessä oli liiketoimintayksiköille tehty jatkuvuudenhallinnan kypsyysmalli, muutamassa yrityksessä käytettiin johdon raportoinnissa liikennevaloja kuvaamaan järjestelmäkohtaista jatkuvuuden kypsyyttä ja oltiin ottamassa käyttöön Huoltovarmuuskeskuksen HUOVI-ohjeistuksen 5-kohtaista kypsyysmallia.

Suunnitelmassa oli yleensä ainakin tiedot, kuka suunnitelmasta vastaa, kuinka usein sitä päivitetään sekä kontaktilista. Eräässä organisaatiossa oli toipumissuunnitelman teko otettu osaksi jatkuvuudenhallinnan kurssia: järjestelmän omistajille tarjottiin puolen päivän kurssi, jossa käydään läpi jatkuvuudenhallinnan periaatteet ja kurssilta pääsi läpi vasta kun yhden järjestelmän suunnitelma oli tehty. Suunnitelmat oli suunnattu vain tietyille ryhmille, eikä koko henkilökunnalla ollut pääsyä niihin. Herbanen ja kumppaneiden (2004) mukaan jatkuvuuteen liittyvät toimintatavat tulisi jakaa koko organisaatiossa ja siten sulauttaa jatkuvuudenhallinta-ajattelua myös yritysjohdon ulkopuolelle.

4.2 Vastuut ja resurssit

Tietoturva-asiat organisoitiin suurimmassa osassa yrityksiä tietohallintoon tai IT-osastolle, mutta myös talousosastolle, turvallisuusorganisaatiolle tai HR-osastolle. Jatkuvuudenhallinnassa tietoturva-asiantuntijat tekivät usein yhteistyötä organisaation riskienhallintaosaston tai yleisestä turvallisuudesta vastaavien kanssa, kun taas liiketoiminnan asiantuntijat antoivat informaatiota tietojärjestelmien priorisointiin. Yhdessä yrityksessä tietoturvasta vastaavat korostivat, että he toimivat vain neuvovina asiantuntijoina ja pitivät tietoturva-asioita esillä; jos he olisivat mukana esim. suunnitelmien toteutuksessa, voisi ilmetä ”not invented here” vastarintaa. Yhdessä yrityksessä oli myös jokaisella tietohallinnon osastolla oma jatkuvuuspäällikkönsä.

Lähes kaikilla haastatelluilla yrityksillä oli etukäteen määritelty kriisitiimi, joka hälytettiin, kun tietojärjestelmähäiriö havaittiin. Pienimmissä yrityksissä kriisitiimi voi olla sama kuin yrityksen IT-osasto, mutta monissa yrityksissä mukana oli myös toimitusjohtaja ja johtoryhmän jäsenet. Muutamassa organisaatiossa ryhmää laajennettiin paikallisesta kriisitiimistä tarpeen mukaan konsernitasolle; vakavamman häiriön kohdalla piti yritysjohdosta etsiä esim. toimitusjohtaja ”kameroiden eteen” hoitamaan viestintää sekä tekemään päätöksiä. Monissa kriisitiimeissä oli johtoryhmän jäsenien tai tärkeiden liiketoimintayksiköiden johtajien lisäksi erikoisasiantuntijoita, kuten tietoturvapäällikkö tai yritysturvallisuusjohtaja, ja häiriöstä riippuen tiimin koko voi vaihdella muutamasta henkilöstä parin kymmenen tiimiin. Asiantuntijoita oli yleensä kuitenkin useammilta yrityksen alueilta, ei pelkästään IT:stä.

Pienimmissä yrityksissä voitiin kutsua kriisitiimiin myös ulkopuolisia jäseniä, ja niissä yrityksissä joissa oli ulkoistettu IT-palveluita tai infrastruktuuria, kriisitiimejä oli sekä toimittajan puolella että asiakkaan puolella.

> *”…Kun meillä on tää meidän kriisiporukka kasassa niin oikeestaan suurin tehtävä meillä on pitää tää oma porukka tietosena ja informoituna siitä mis mennään, koska ei me voida tehdä oikeestaan meidän järjestelmille, tietoliikenteelle, millekkään yhtään mitään, koska ne hoitaa sen täysin ja eikä ne edes päästä meitä sinne, koska se on niitten vastuulla.”*

Tieteellisen kirjallisuuden mukaan johdon sitoutumisesta jatkuvuudenhallintaan kertoo esimerkiksi se, raportoidaanko tietohallinnon jatkuvuusasioista säännöllisesti yrityksen johtoryhmälle. Vain 4:ssä yrityksessä 18:sta säännöllistä raportointia ei ollut, suurempien ongelmien jälkeen selvitys johdolle vaadittiin näistä kuitenkin muutamissa. Joissain yrityksissä tämä koettiin vakavaksi puutteeksi, koska loppujen lopuksi liiketoiminnan jatkuvuudesta on vastuussa toimitusjohtaja. Säännöllinen raportointi osoittaisi muulle organisaatiolle, että jatkuvuusasiat ovat tärkeitä ja niistä ollaan kiinnostuneita.

Yrityksen ylin johto vaikutti jatkuvuussuunnitteluun monin eri tavoin:

- antamalla riittävästi resursseja
- hyväksymällä toipumissuunnitelmat
- käynnistämällä tai osallistumalla jatkuvuusprojektiin
- asettamalla tavoitteet (esim. saatavuus, tavoitetoipumisajat, luotettavuus, kustannustaso)
- osallistumalla kriisitiimiin ja kriisinhallintaan
- olemalla vastuussa toiminnasta ja jatkuvuudesta

Yleisesti yrityksissä koettiin, että tietoturvaan ja jatkuvuudenhallintaan oli käytössä riittävästi resursseja (kuten henkilöstöä, kykyä, laitteita ja ohjelmistoja), vaikka muutama haastateltava huomauttikin, että *”aina voisi olla paremmin resurssoitu”*. Hyvin harvoissa yrityksissä kuitenkaan käytettiin henkilökohtaisia kannustimia kuten tulospalkkioita sitouttamaan henkilöresursseja tietoturvalliseen toimintaan tai jatkuvuudenhallintaan. Niissä organisaatioissa, joissa kannustimia oli käytössä, ne oli lähinnä suunnattu päällikkö- tai johtajatason henkilöille.

Noin puolet haastatelluista kertoi, että liiketoimintayksiköillä oli omat tietoturvavastaavansa, kun taas toisella puolella tietoturva-asiat oli keskitetty yhteiseen yksikköön, joka palveli muita liiketoimintayksiköitä esim. neuvovassa ja kouluttavassa roolissa. Mielenkiintoinen käytäntö oli yhdessä yrityksessä, josta oli poistettu tietoturvajohtajan titteli, jotta kussakin yksikössä ja kunkin järjestelmän omistaja ottaisi tietoturva-asiat vastuulleen jo järjestelmän suunnitteluvaiheessa. Tällöin sen huomioiminen oli yksinkertaisinta ja edullisinta. Muutamassa muussa yrityksessä oli myös huomattu kannattavammaksi ottaa tietoturva-asiantuntija alusta asti kehitystyöhön.

> *”Aikasemmin se oli vähän niin, että ensin tehtiin ja sitten tuli tietoturvakaveri ja katso ja kauhistui ja sitten korjattiin, mutta nyt ensin katsotaan ja varmistetaan, että tämä on kestävällä pohjalla tämä ratkaisu ja sitten lähdetään tekemään.”*

Eräässä yrityksessä kehitysvaiheessa järjestelmän tuli täyttää tietyt tietoturvavaatimukset, ja nämä testattiin ennen tuotantoon siirtoa; kriittisimmissä sovelluksissa testaajana oli ulkopuolinen auditoija. Toisessa yrityksessä järjestelmäkehitystä suunniteltiin kehitettäväksi tietoturvallisemmaksi niin, että jo konseptivaiheessa tehtäisiin tietoturva-arviointi. Mikäli järjestelmä päätettiin toteuttaa, määrittelyvaiheessa tehtäisiin riskianalyysi, ja ennen tuotantoon siirtoa testien lisäksi vaadittaisiin myös jatkuvuussuunnitelma.

4.3 Uhat, varautuminen ja häiriöselviytyminen

Tässä tutkimuksessa tunnistettiin monia erilaisia uhkia tietojärjestelmille ja tietohallinnolle: luonnonkatastrofeista tietoturvaan. Laitteisto- ja yhteysriskeihin oli

varauduttu kaikissa haastatelluissa yrityksissä hyvin peilaamalla, kahdentamalla, virtuaaliympäristöllä jne. ja usein laitteistoviat pystyttiin tunnistamaan niin hyvissä ajoin, ettei vahinkoa päässyt sattumaan. Tietoturvauhkiin oli myös varauduttu hyvin: useampi haastateltava muisteli vuosituhannen alun palvelinhyökkäyksiä ja virusongelmia, joita ei viime vuosina ole ollut. Yhdessä yrityksessä kriisitiimin historia johtikin näihin kymmenen vuoden takaisiin ongelmiin.

Useimmin haastatteluissa mainittu riski oli muutos: usein kun tietojärjestelmiin tehtiin muutoksia, niitä ei ollut testattu riittävän hyvin tai ne eivät sopineet yhteen jonkun tietoturva- tai käyttöjärjestelmäpäivityksen kanssa. Muutamat yritykset olivatkin varautuneet näihin riskeihin erityisillä muutosprosesseilla, jotka toisaalta nähtiin byrokraattisina, mutta välttämättöminä.

> *”Siinä vaiheessa kun ihan tuntuu, että mä olen tehnyt tämän jo niin monta kertaa että kyllähän mä tän osaan ja sitten pyritään vähän oikasemaan prosessista, koska onhan muutoshallintaprosessissa monta tarkistuspistettä, mikä tekee siitä ehkä hieman byrokraattisen ja jäykän, ja sitten nyt mun pitää saada äkkiä tää ja sitten kun tätä on ennenkin tehty ja sitten ei huomatakaan jotakin ja silloin se yleensä napsahtaa ja joku menee pieleen.”*

Lisäksi muutokset pyrittiin ajoittamaan muuhun ajankohtaan kuin kuukauden-, kvartaalin- ja vuodenvaihteeseen, jolloin useimmiten oli kriittistä pitää esim. talousjärjestelmät toiminnassa.

Henkilöriskejä haastateltavat tunnistivat myös useita. Inhimilliset virheet aiheuttavat joskus paljonkin vahinkoa, eläköitymisen seurauksena voi taas arvokasta tietoa kadota yrityksestä. Eräässä yrityksessä olikin kriittisimmille järjestelmille vaatimus, että organisaation palveluksessa pitää olla vähintään kolme osaajaa: jos yksi lähtee vaikka lomalle, ja toinen sairastuu, niin vielä löytyy yksi asiantuntija. Avainhenkilöille ei myöskään tule antaa liian suuria oikeuksia, eli vastuita oli jaettava, sekä väärinkäytösriskin vuoksi että osaamisen kehittymisen kannalta. Joskus oli varauduttu liian vähäisin henkilöresurssein, jolloin joillekin ihmisille kasautui liikaa työkuormaa. Strategiseksi riskiksi nähtiin IT- ja tietoturvanäkemyksen puuttuminen yrityksen johtoryhmästä: johtoryhmässä asetetaan tavoitteet ja strategiat, ja koska tietojärjestelmät ovat monelle yritykselle hyvin keskeisiä – jos järjestelmät eivät toimi, koko toiminta pysähtyy – johtoryhmän näkemystä tarvitaan.

Kymmenessä yrityksessä kriittisimmät järjestelmät peilattiin jatkuvasti, joissain jopa kolmelle eri palvelimelle ja eri konesaleihin, jotka ovat maantieteellisesti merkittävästi erillään. Jos toinen palvelin vahingoittuu, voidaan toinen ottaa heti käyttöön, jolloin mitään tietoa ei menetetä. Viidessä yrityksessä kriittisimmät järjestelmät kahdennettiin ja kolmessa pienemmässä yrityksessä käytettiin nauhavarmistusta, joka tehtiin öisin ja joskus myös keskellä päivää. Nauhat vietiin joko eri paloalueelle, paloturvakaappiin tms. turvalliseen paikkaan. Monissa or-

ganisaatioissa oli kuitenkin jo siirrytty nauhavarmistuksista erilaisiin levyvarmistuksiin, koska levytekniikka oli riittävän kehittynyttä.

Yhdessä organisaatiossa varmuuskopioiden ottaminen ei aina onnistunut, ja yrityksen tietoturvasta vastaava koki tämän varsin huolestuttavaksi, kuten myös asenteen, joka ei tuntunut halukkaalta parantamaan varmuuskopioiden onnistumisprosenttia. Eräässä yrityksessä tietoturvasta vastaavaa henkilöä huolestutti taas riippuvuus IP-verkosta: dataliikenteen lisäksi puhelinliikennettä siirrettiin hyödyntämään VoIP-tekniikkaa, jolloin jos IP-verkko ei toimisi sekä sähköposti että puhelut olisivat poissa käytöstä.

Kuten aiemmin on kerrottu, järjestelmiä luokiteltiin monissa yrityksiä kriittisiin ja vähemmän kriittisiin. Erään yrityksen luokittelu on esitetty taulukossa 2. Luokitteluun oli yhdistetty palautuminen ja testaaminen helposti muistettavalla tavalla. Viidessä haastattelussa tuli ilmi myös varautuminen kansallisen tason kriiseihin, eli yritykset olivat huolehtineet huoltovarmuudesta.

Taulukko 2. Esimerkki järjestelmien kriittisyysluokittelusta.

Luokka	Palautuminen	Testaus
0	ei siedä katkoksia	testaus joka vuosi, pääjärjestelmän alasajo ja varajärjestelmän testi, tuotantoa vaarantamatta
1	alkaa heti	
2	alkaa yhden arkipäivän kuluessa	testaus joka toinen vuosi
3	alkaa yhden työviikon kuluessa	testaus joka kolmas vuosi
4	järjestelmä on käytettävissä kuukauden kuluessa	testaus joka neljäs vuosi

Häiriöselviytyminen oli hyvinkin samanlaista kussakin haastatellussa yrityksessä. Kun häiriö ensin tunnistettiin, sen jälkeen tuli ottaa yhteyttä esimieheen, käyttäjätukeen, IT-osastolle tai muulle nimetylle taholle. Jos ongelma oli suuri, ja sitä ei saatu esim. käyttäjätuessa ratkaistua, otettiin yhteyttä kriisitiimiin, jonka jälkeen ongelmaa alettiin ratkoa ja samalla informoida kaikkia asianosaisia. Muutamassa ITIL:iä soveltavassa yrityksessä haastatellut kertoivat, että vaikean ongelman kohdalla käyttöön otettiin Major incident management -prosessi (MIM), jossa oli tarkoin määritelty mm. viestintä. Yhdessä organisaatiossa jokainen tähän kategoriaan kuuluva häiriö raportoitiin myös yrityksen ylimmälle johdolle. MIM:n aikana kriisitiimi oli yhteydessä toisiinsa muutaman tunnin välein ja päätti jatkotoimenpiteistä.

> *”Todetaan tilanne, annetaan sitten paras estimaatti, koska me saatais tämä tieto. Ja tämä tiedotetaan kaikille, että tällainen on tapahtunut, meillä ei ole tietoa mitä on oikeasti, mutta seuraava info tulee vaikka tunnin päästä.”*

Ongelmasta kärsiville osapuolille viestitettiin määrämuotoisesti ongelman laatu, arvioitu kesto, koska tulee seuraava tiedote sekä onko olemassa jokin korvaava järjestelmä. Tämä vapautti ongelmaa selvittävän tahon jatkuvilta puhelinsoitoilta ja helpotti ongelmasta kärsiviä, jotka kaipasivat mahdollisimman paljon tietoa tilanteesta. Viestintämedioina toimivat intranetin ja sähköpostin lisäksi tekstiviestit, bulletin boardit, keskusradiokuulutukset tai paperitiedotteet ongelmakohdissa. Yhdessä organisaatiossa oli käytössä ulkopuolinen hätäviestipalvelu, jonne oli etukäteen talletettu yhteystietoja, ja häiriön sattuessa tietyt ihmiset ottivat konferenssipuhelun listan ihmisille.

Niissä yrityksissä, joissa oli useampia tuotantolaitoksia tai asiakaspalvelukonttoreita häiriöselviytymisessä käytettiin verkostoa hyväksi: jos yksi tai useampi oli poissa toiminnasta, ohjattiin asiakkaat tai tuotanto toisiin yksiköihin esim. lakkotilanteessa muihin maihin. Jos infrastruktuuri oli ulkoistettu, vastuunjaot olivat hyvinkin tarkkoja: vain ulkoistuspalvelujen tarjoaja pääsee konesaliin korjaamaan vikaa. Ongelmasta kärsivän organisaation oli keskityttävä informaation jakamiseen. Joissain yrityksissä kriittisimmille prosesseille oli olemassa myös manuaalisia vaihtoehtoprosesseja, joiden käyttöönotossa kuitenkin oli ongelmansa:

> *”..käytännössä useesti käy nii et tota sitä ei haluta helposti ottaa käyttöön koska sen manuaalitoiminnon palauttaminen sitten myöhemmin takasin on iso työmäärä niin mielummin vaikka odotellaan vähän aikaa jos se sit kuitenkin tulis ja sit päästäs niinku jatkamaan..”*

4.4 Testaus, auditoinnit ja koulutus

Lähes kaikissa haastatelluissa yrityksissä testattiin jatkuvuuteen tai tietoturvaan liittyviä asioita säännöllisesti. Testejä oli lähtien infrastruktuurin perusskannauksista ja varmuuskopioiden säännöllisistä palautustesteistä kerran vuodessa ulkopuolisten tekemiin järjestelmäauditointeihin. Kahdessa yrityksessä sanottiin, ettei säännöllistä testausta ole toistaiseksi tarvittu, koska jatkuvuussuunnitelmat oli todettu toimiviksi käytännössä.

Jatkuvia tai vähintään kerran kuussa tehtäviä testauksia tehtiin mm. verkolle, josta skannattiin virusten ja haittaohjelmien lisäksi päivitysten tilannetta: jos päivityksiä ei ole tehty, otetaan yhteyttä asianosaisiin ja mikäli mitään ei tapahdu lyhyen ajan sisällä, kone poistetaan verkosta. Lisäksi eräs terveydenhuoltoalalla toimiva yritys tarkasti säännöllisesti tietosuojarikkomusten varalta lokeja. Yhdessä organisaatiossa tarkastettiin joka kuukausi jokin ulkoistettu järjestelmä ja sen tietoturva. Koulutuksiin liittyen eräässä yrityksessä tarkastettiin puolivuosittain, että uudet työntekijät ovat käyneet viimeistään kuukauden kuluessa töiden aloi-

tuksesta perehdytysosion Intranetissä, johon liittyivät myös tietoturva-asiat. Eräs haastateltava kertoi, että heillä esimiehet havainnoivat alaistensa tietoturvakäyttäytymistä ja raportoivat siitä puolivuosittain sisäiselle tarkastukselle. Eräässä organisaatiossa sisäinen tarkastus teki vähintään kerran vuodessa toimipaikkoihin tarkastuskäyntejä.

> *”Eikä sitten salasanoja ole näppiksen alla näkyvissä. Ja sitten me valvomme tuota. Vähintään kerran vuodessa on toimipaikassa tarkastus niin, että meidän sisäinen tarkastus tekee tietyn checklistan perusteella ja yhtenä asiana on sitten tietoturvallisuus.”*

Muutama organisaatio teki kvartaaleittain jonkun auditoinnin tietylle painopistealueelle, tarkastaen esim. SaaS-sovellusten jatkuvuussuunnitelmat. Monissa tuotantoyrityksissä asiakkaat tekivät auditointeja yritykseen, joita saattoi olla kymmeniä vuodessa ja osassa niissä oli mukana myös IT-osaston auditointi. Lisäksi haastatellut yritykset olivat usein varanneet itselleen tai kolmannelle osapuolelle oikeuden auditoida esim. IT-palveluja tuottavat yritykset mm. tietoturvakäytäntöjen osalta, ja tätä oikeutta myös käytettiin.

Muutamissa yrityksissä jatkuvuussuunnitelmat myös tarkastettiin säännöllisesti, kerran vuodessa tai joka toinen vuosi. Yhdessä yrityksessä IT-osasto teki järjestelmille toipumissuunnitelmat ja tietoturvajohtaja haastatteli liiketoimintayksiköiden johtajia ja arvioi niiden haastattelujen perusteella suunnitelmien toimivuuden.

Tietoturvakoulutusta tarjottiin useimmissa haastatelluissa yrityksissä. Muutamassa haastateltava koulutti uudet työntekijät henkilökohtaisesti. Monet taas käyttivät joukkoluentoja, joissa yhtenä osiona oli tietoturva. Lisäksi erilaisia Intranetissä olevilla verkkokursseilla ja henkilökohtaisella vaikuttamisella levitettiin tietoturvatietoutta. Mutta kuten eräässä yrityksessä huomautettiin: tietoisuuden levittämisessä tulee olla taukojakin, muuten yleisö tylsistyy viestiin.

Koulutusta tarjottiin myös muille ryhmille kuin uusille työntekijöille: esimiehille, alihankkijoille, ulkomaan komennukselle lähteville sekä järjestelmäasiantuntijoille. Yhdessä organisaatiossa tietoturva-asiat olivat tulossa myös jokaiselle henkilökunnan jäsenelle pakolliseen henkilökorttikoulutukseen, mikä oli uusittava viiden vuoden välein. Samassa paikassa oli muutenkin koulutukseen kiinnitetty paljon huomiota: sponsorina toimiva varatoimitusjohtaja oli lähettänyt kaikille työntekijöille henkilökohtaisen kirjeen ja kehottanut osallistumaan koulutukseen. Esimiesten koulutuksessa tietoturvan lisäksi käsiteltiin mm. henkilöstöturvallisuutta, tietojen luokittelua ja jatkuvuuden- sekä riskienhallintaa. Tietoturvapolitiikka oli lähes kaikissa haastatelluissa organisaatioissa, useimmiten ”piilotettuna” Intranetiin, mutta sitä tuotiin näkyviin erityisesti uusille työntekijöille.

4.5 Ulkoistaminen

Tutkimuksessa selvitettiin myös tietohallinnon ulkoistamisen tilaa, koska sen vaikutusta tietoturvaan ja jatkuvuudenhallintaan on tutkittu akateemisesti hyvin vähän, mutta globalisoituvassa maailmassa yrityksen ulkopuoliset tietoliikenneyhteydet ovat arkipäiväisiä.

Vain kolme haastateltua yritystä ei ollut ulkoistanut mitään, lähinnä koska sen koettiin lisäävän reaktioaikaa esimerkiksi juuri häiriö- ja päivitystilanteissa. Nämä yritykset ovat kooltaan pienempiä ja sijaitsevat pääkaupunkiseudun ulkopuolella. Toisessa ääripäässä oli taas viisi suurempaa organisaatiota, jotka olivat käytännössä ulkoistaneet kaiken: infrastruktuurin, tietoliikenteen sekä tietojärjestelmät. Yksi haastateltava kertoi, että heillä oli vielä 2000-luvun alkupuolella ollut muutaman sadan henkilön suuruinen IT-osasto hajautettuna useampaan liiketoimintayksikköön, ja joitain ulkoistettuja järjestelmiä; kunnes vuosikymmenen puolivälissä konsernin IT-osastolla oli vain 6 ja nykyisellään 16 ihmistä sekä kaikki tietojärjestelmät oli ulkoistettu. Kahdessa yrityksessä järjestelmät ja infrastruktuuri oli ulkoistettu konsernin keskustoimittajalle. Yksi organisaatio käytti konsernin toiminnanohjausjärjestelmää ja hoiti vain talon sisäisen tietoliikenteen, konserni hallinnoi ulkoista verkkoa.

> *”Käytännössä voisi sanoa, että se on kahteenkin kertaan ulkoistettu. Että kun nämä kassajärjestelmät ja sitten myöskin taloushallinnon järjestelmät. Niin niistä vastaa ryhmätason tietohallinto […]. Niin se on ulkoistettu heille ja he ovat sen ulkoistaneet joko kokonaan tai osin vielä sitten – on se sitten IT-Yritys X tai IT-Yritys Y tai vastaava. Että nykykäytäntö on, että pyritään löytämään jokaiselle osa-alueelle kustannustehokas ja paras ammattitaito.”*

SaaS (Software as a service) sovelluksia tai pilvipalveluja käytettiin kuudessa organisaatiossa ja kahdessa oli käytössä virtuaaliympäristö, eli ainakin palvelinkapasiteetti ostettiin pilvipalveluna. Suurin osa haastatelluista siis ei käyttänyt tätä, ja itse käsite ei ollut kaikille myöskään tuttu. Eräs haastateltava kertoi, että tärkein syy käyttämättömyydelle oli tietoturvakäytännön puute; osittain esim. palomuurin kohdalta. Siellä missä SaaS-sovelluksia käytettiin, tietoturvakäytännöt olivat jo standardoituneet. Nämä organisaatiot käyttivät palveluntoimittajan hyväksymiseen standardiprosessia, jossa oli kontrollit mm. kirjautumiskäytäntöön ja tiedon turvallisuuden takaamiseksi, ja jos toimittaja läpäisi tämän testin, solmittiin standardisopimus ja mahdollisesti NDA:t, jossa varattiin oikeus auditointiin sekä ulkopuolisen tai itse yrityksen tekemään. Yhdessä yrityksessä SaaS-sovelluksia ostettiin vain sertifioiduilta toimittajilta.

Ulkoistuksen ja ulkopuolisten yhteyksien tietoturvan hoitamiseen oli monia eri tapoja:

- SLA-sopimukset, joissa tietoturvaliite

- salassapitosopimukset (NDA)
- kontrollijärjestelmät tai tarkistuslistat, joissa edellytetään esim. jatkuvuussuunnitelmaa
- pienimmän käyttöoikeuden periaate tai esim. secure id –kortti
- ulkopuolisia ei päästetä sisäverkkoon: ”hiekkalaatikko”, DMZ-alue, ekstranet tms.
- ulkopuoliset päästetään sisäverkkoon: VPN-yhteys, palomuuriavaus vain kumppaneille

Yhdessä organisaatiossa käytettiin jo ennen tietojärjestelmän ulkoistamista tarjouspyyntötilanteessa tietoturvakriteerejä: tietoturvavaatimusten täyttäminen oli yksi osa-alue, jolla arvioitiin tarjouspyyntöjä. Eräs haastateltava oli suunnitellut tietoturvaliitteen käyttöönottoa ulkoistussopimuksissa, missä määriteltäisiin miten yrityksen tietoja tulisi käsitellä, mitä toimittajan järjestelmiltä vaaditaan, miten toimittajan henkilöstöä tulisi ohjeistaa. Lisäksi liitteessä varattaisiin oikeudet auditointeihin ja asetettaisiin kertaluonteisia euromääräisiä sanktioita sopimuspoikkeuksista, vaikka vahinkoa ei olisikaan sattunut.

4.6 Strategisuuden arviointi

Haastattelukysymyksissä kysyttiin lopuksi, kokevatko yritykset jatkuvuudenhallinnan strategisena tai kilpailullisena etuna vai lähinnä liiketoiminnan mahdollistavana tekijänä. Suurin osa haastatelluista koki jatkuvuudenhallinnan lähinnä kilpailullisena tekijänä, mutta moni perusteli vastaustaan sillä, että ”haluamme toipua nopeammin kuin kilpailijat häiriöistä” tai ”pitkäaikaiset häiriöt haittaisivat imagoamme” tai ”haluamme osoittaa asiakkaillemme olevamme luotettava kumppani”. Herbane et al. (2004) esittivät, että nimenomaan toipumisnopeus ja yrityksen joustavuus häiriötilanteissa ovat sidoksissa strategisuuteen, kuten myös jatkuvuuskäytäntöihin sitoutuminen muuallakin kuin yritysjohdossa sekä ulkoiset vaikuttimet, kuten lainsäädännön asettamat vaatimukset.

Teimme yksinkertaisen analyysin haastateltujen yritysten jatkuvuudenhallinnan tilasta pisteyttämällä eri strategisuuden merkkejä, joita haastatteluissa tuli ilmi. Herbanen et al.:n (2004) mukaan toipumisnopeus riippuu yrityksen kyvystä havaita häiriötilanteet ja aloittaa toipuminen nopeasti sekä etukäteisvalmisteluista. Tässä tutkimuksessa näitä havainnoitiin kysymällä suunnitelmien olemassaolosta, niiden testaamisesta ja kriisitiimeistä. Saman tutkimuksen mukaan yrityksen joustavuus riippuu yrityksen kyvystä sopeutua erilaisiin häiriöihin niin että liiketoiminta pystyy jatkumaan. Tässä tutkimuksessa tätä selvitettiin kysymällä erilaisten varmistusmenetelmien käytöstä (peilaus, kahdennus, nauhavarmennus) ja henkilökunnan koulutuksesta. Lisäksi analyysissa huomioitiin mikäli haastattelussa tuli ilmi muita joustavuuteen liittyviä tekijöitä, esim. kontto-

ri/tuotantolaitosverkoston mahdollisuudet paikata häiriöstä kärsiviä yksiköitä, tai panostukset toimittaja- tai asiakasketjun monipuolistamiseksi.

Herbanen et. al.:n (2004) mukaan myös jatkuvuudenhallinnan käytäntöjen sulautuminen yrityksen ylimmän johdon ulkopuolelle vaikuttaa myös strategisuuteen. Tässä tutkimuksessa tätä mitattiin seuraamalla, tehtiinkö jatkuvuussuunnitelmat liiketoimintayksiköissä vai keskitetysti esim. IT-osastolla. Mikäli haastattelussa kävi ilmi jotain ongelmia, esimerkiksi ettei ylin johto tai liiketoimintayksiköt olleet sitoutuneita suunnitelmien tekemiseen tämä huomioitiin pisteytyksessä. Neljäs tekijä, joka vaikuttaa jatkuvuudenhallinnan strategisuuteen, oli pakollisuus, eli silloin kun esim. lait tai viranomaiset olettavat, että jatkuvuutta hallitaan yrityksessä, on kyse pakollisuudesta.

Pisteytyksessä pyrittiin huomioimaan yrityksen koko, koska samat käytännöt eivät välttämättä sovellu tai ole tarkoituksenmukaisia erikokoisille yrityksille. Käytetyt kriteerit siis olivat (pienellä yrityksellä tarkoitetaan alle 1500 hengen yritystä):

Toipumisnopeus:

- järjestelmäkohtainen jatkuvuudenhallintasuunnitelma tai pienissä yrityksissä kirjalliset toipumisperiaatteet kriittisille järjestelmille 1 pistettä
- suunnitelmien säännöllinen testaaminen 1 pistettä
- etukäteen suunnitellun kriisitiimin olemassa olo 1 pistettä

Joustavuus:

- varmistusmenetelmä: peilaus 1p, kahdennus 0,75p, nauhavarmistus 0,5p; pienissä yrityksissä kahdennus 1p ja nauhavarmistus 0,75 pistettä
- tietoturvakoulutuksen tarjoaminen henkilöstölle 1 pistettä
- muut tekijät: konttoriverkosto/ panostus toimittaja- tai asiakasketjun monipuolisuuteen 1 pistettä

Sulautuminen:

- liiketoimintayksiköissä tehdyt jatkuvuussuunnitelmat tai pienissä yrityksissä riskianalyysi tms. 2 pistettä; mikäli joitain ongelmia esim. yksikköjen tai johdon sitoutumisessa 1 piste

Pakollisuus:

- laki- tai viranomaisvelvoite, tai Huoltovarmuuskeskuksen vaatimukset jatkuvuudenhallinnalle 1 pistettä

Pisteytysmenetelmä on yksinkertainen ja kritiikille altis. Esimerkiksi voidaan miettiä, tulisiko pisteitä antaa ennemminkin siitä, että jatkuvuudenhallintaa on suunniteltu ilman lakivelvoitteita, kuin toisin päin. Esimerkiksi pankki- ja vakuutussektori suoriutuu tästä pisteytyksestä täysin pistein, koska Finanssivalvonta edellyttää heiltä juuri näitä asioita.

Tämän analyysin tuloksena voidaan siis todeta, että haastatellut yritykset sijoittuivat 2,5–9 pisteen välimaastoon, siten että yhdeksän yritystä saa vähintään 7 pistettä. Parhaat pisteet saavat pankki- ja vakuutussektori, kaksi IT-yritystä, sekä

kaksi palvelusektorin ja yksi tuotantoteollisuuden edustaja. Näistä viittä haastateltiin pääkaupunkiseudulla ja viisi on kansainvälisen konsernin tytäryhtiöitä tai osia. Loppupäähän sijoittuvat viisi yritystä, jotka saivat 2,75–5 pistettä tällä arvioinnilla, ovat suurimmillaan n. 1000 hengen yrityksiä, joista neljän pääkonttori sijaitsi pääkaupunkiseudun ulkopuolella.

5 JOHTOPÄÄTÖKSET

Tässä tutkimuksessa selvitettiin, miten suomalaisissa suuryrityksissä tietohallinnon jatkuvuutta hallitaan ja onko sillä strategista roolia yrityksessä. Tutkimus tehtiin haastattelututkimuksena, joka perustui tieteelliseen kirjallisuuteen eli kysymykset oli muotoiltu Herbane et. al:n (2004) tutkimuksen pohjalta. Yhteensä 18 suomalaista suuryritystä osallistui haastatteluihin. Tutkimuksen perusteella voidaan sanoa, että tietohallinnon jatkuvuutta hallitaan erityisesti suuremmissa ja kansainvälisissä organisaatioissa hyvinkin strategisesti, ja monissa tämän tutkimuksen piirissä olevissa pienemmissä (vaikka Suomen mittakaavassa suurissa) yrityksissä tarkoituksenmukaisesti, vaikka parannettavaa toki on.

5.1 Jatkuvuudenhallinnan strategisuus

Havaintojen lopuksi tehtiin yksinkertainen analyysi, kuinka strategista jatkuvuudenhallinta haastatelluissa yrityksissä on. Tulosten perusteella voidaan vetää seuraavia johtopäätöksiä. Parhaiten sijoittuneilta yrityksiltä laki- tai viranomaiset velvoittivat jatkuvuudenhallintaa, ja selkeästi sillä on saavutettu kypsempiä ja strategisempia jatkuvuudenhallinnan käytäntöjä. Mielenkiintoista on, että hyväkään jatkuvuudenhallinta ei suojaa välttämättä häiriöiltä, koska haastattelujen tekemisen jälkeen muutama analyysissa korkealle sijoittunut yritys on kokenut liiketoiminnassa tietotekniikasta johtuvia häiriöitä ja niistä on kerrottu myös mediassa. Uutisten perusteella kuitenkin häiriöt ovat olleet yrityksen ulkopuolisissa yhteyksissä tai ulkoistuspalvelujen tarjoajilla. Tutkimuksen perusteella ei voida kuitenkaan sanoa, että ovatko ulkopuoliset velvoitteet olleet ainoita syitä miksi käytäntöjä on kehitetty, mutta näyttäisi siltä, että esimerkiksi kansainvälisyys tai valveutunut yritysjohto voivat myös vaikuttaa tilanteeseen.

Koska tässä analyysissa pienimmät yritykset sijoittuivat suurimmaksi osaksi häntäpäähän, voidaan siitä vetää muutamia johtopäätöksiä. Ensinnä, Iso-Britanniassa kehitettyyn teoriaan pohjautuva pisteytysmenetelmä selkeästi suosii yrityksiä, joissa on ulkopuolisia velvoitteita jatkuvuudenhallinnalle, ja menetelmää pitääkin kehittää jatkossa Suomen olosuhteisiin sopivammaksi. Toiseksi voidaan pohtia, pitääkö pienemmissä yrityksissä jatkuvuudenhallinnan olla yhtä säänneltyä kuin suurissa yrityksissä. Pienen yrityksen vahvuus on juuri ketteryydessä ja joustavuudessa, ja ei ole välttämättä tarkoituksenmukaista esim. doku-

mentoida kaikkien järjestelmien toipumisprosesseja, kun voitaisiin keskittää vähäiset resurssit kriittisten tietojärjestelmien ylläpitoon.

Tutkimukseen osallistunut maisterintutkielman tekijä kehitti havaintojen pohjalta kypsyysmallin, joka myös kuvaa strategisuutta. 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 kategoriaan, 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 vähäisemmin tavoittein. 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.

Kategorisointi kuvaa paremmin, mitkä ovat merkittävimmät erot yritysten jatkuvuudenhallinnassa ja ajattelutavoissa. Yksittäinen yritys voidaan sijoittaa yhteen kategoriaan. Taulukko 3 nimeää eri kategoriat ja kuvailee niiden tärkeimmät ominaispiirteet.

Ensimmäinen kategoria koostuu yrityksistä, joiden jatkuvuudenhallinta perustuu pääasiassa asiakkaiden tai lainsäädännön vaatimuksiin. Tämän kategorian yritykset näkevät BCM:n 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 on vaikeuksia sitouttaa koko organisaatiota jatkuvuudenhallintaan 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 yrityksen ylimmässä johdossa. Organisaatiot siis tiedostavat jatkuvuudenhallinnan hyödyt osittain, mutta eivät osaa käyttää niitä pitkän tähtäimen tavoitteidensa tukena tai kilpailukeinona.

Taulukko 3. Jatkuvuudenhallinnan roolit suurissa suomalaisissa yrityksissä.

Jatkuvuudenhallinnan rooli	Ominaispiirteet
1. Liiketoiminnan mahdollistaja	- Tavoitteena lainsäädännön tai asiakkaan vaatimusten täyttäminen - Jatkuvuudenhallinta ja strategia eivät liity 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 - Jatkuvuudenhallinnalla muodollinen asema - Vastuuta hajautettu
3. Strateginen	- 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)

Jatkuvuussuunnitelman luomiseksi on toisen kategorian yrityksissä mahdollisesti käytetty strategisia työkaluja, mutta ne eivät välttämättä 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 ainakin suurempien häiriöiden yhteydessä.

Kolmanteen kategoriaan kuuluvissa yrityksissä voidaan jatkuvuudenhallintaa pitää strategisena menestystekijänä. Näissä yrityksissä BCM on mahdollisista ulkoisista vaatimuksista huolimatta lähtöisin liiketoiminnan tarpeista ja siihen kiinnitetään huomiota organisaation kaikilla osa-alueilla. Suunnitelmia 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 BCM-keskustelufoorumin käyttö viestinnän ja kehityksen tukena.

Moneen tutkimuksen tapausyritykseen liittyy piirteitä, jotka viittaavat kolmanteen kategoriaan, 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 kategoriaan. 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 pieni enemmistö haastatelluista suomalaisista yrityksistä lukeutuukin kahteen ensimmäiseen luokkaan. Yleisesti voidaan siis todeta, että jatkuvuudenhallinnan rooli on suurissa suomalaisissa yrityksissä yleensä muu kuin strateginen.

5.2 Jatkuvuudenhallinnan kehittäminen yrityksissä

Tulosten perusteella voidaan tehdä joitain suosituksia tai koota hyviä käytänteitä niille yrityksille, jotka haluavat kehittää jatkuvuudenhallintaansa. Suositukset voidaan edelleen jakaa alle 1500 hengen yrityksille ja sitä suuremmille, koska näissä kokoluokissa näyttää olevan merkittävästi erilaiset käytännöt.

Alle 1500 henkeä työllistävät yritykset:

1. Yritysjohdon sitouttaminen: Kaiken kokoisissa yrityksissä yritysjohto on vastuussa liiketoiminnan jatkuvuudesta. Yritysjohdolle tulisi voida osoittaa tietojärjestelmien häiriöiden vaikutukset liiketoiminnalle erilaisin esimerkein, joita medioissa aina silloin tällöin näkee. Tällä tavoin voidaan vakuuttaa yritysjohto, että heidän tulisi seurata säännöllisesti tilannetta. Yksinkertainen ja käytetty raportointimuoto on kriittisten tietojärjestelmien ja tietohallinnon resurssien toipumisvalmius esitettynä liikennevalomerkinnöillä.
2. Liiketoiminnan vaikuttavuusanalyysi tai riskianalyysi: Kaikissa yrityksissä oli tiedostettu kriittisimmät liiketoiminnat (yleensä tuotanto ja asiakaspalvelu) ja sen myötä voidaan pohtia, miten tietohallinto tukee näitä liiketoimintoja. Tämän jälkeen voidaan analysoida, mitkä tietojärjestelmät tai muut IT-resurssit ovat kriittisimpiä, ja millaisia vaikutuksia niiden häiriöillä olisi yrityksen liiketoiminnalle. Melko mutkaton tapa on toteuttaa tämä järjestelmälistauksella, jolla muutamat keskeiset päälliköt määrittelevät kriittisimmät resurssit.
3. Toipumissuunnittelun periaatteet ja kriisitiimi: Toipumisnopeuteen vaikuttavat varmistusten lisäksi ennakkosuunnittelu, ja sitä varten on hyvä olla dokumentoituna periaatetasolla toipumisprosessi ja pahimpia on-

gelmia varten nimetty kriisitiimi. Periaatteissa voi olla esimerkiksi käsitelty viestintää, ja miten järjestelmiä priorisoidaan sekä häiriön jälkeiset toimet kuten raportointi johdolle.

4. Varmistukset, testaaminen, kouluttaminen: Oli kyseessä peilaaminen, kahdennus tai vaikka nauhavarmistukset, on hyvä varmistaa testaamalla säännöllisesti, että prosessit todella toimivat ja varmuuskopiointi ja sieltä palautus toimii. Varmuuskopioita voidaan viedä toiseen rakennukseen, mutta paloturvakaapitkin ovat hyvä vaihtoehto. Myös itse prosessia on hyvä testata säännöllisesti sekä ajoittain tehdä erillisille järjestelmille toipumistestejä, ja ulkopuoliset auditoijat voivat auttaa näkemään ongelmakohtia. Uusille ja vanhoillekin työntekijöille tulisi järjestää tietoturvakoulutusta, johon olisi hyvä sisällyttää jollain tasolla jatkuvuuden periaatteita, jotta koko organisaatio ymmärtää miksi liiketoiminnan häiriöttömyys on tärkeää.
5. Ylläpito: Toipumisperiaatteiden sekä liiketoiminnan vaikutusanalyysin päivittäminen on myös pienemmissä yrityksissä tarpeen, koska tietotekninen ympäristö muuttuu jatkuvasti ja uusia riskejä ilmenee. Joissain yrityksissä suunnitelmat käytiin läpi joka toinen vuosi, vaikka muutoksia ei tulisikaan, voi olla järkevää palauttaa mieleen periaatteet sekä häiriöiden vaikutukset.

Yli 1500 työllistävät yritykset:

1. Koko yrityksen sitouttaminen: Joissain haastatelluissa yrityksissä oli ongelmia ylimmän liikejohdon sitouttaminen jatkuvuudenhallintaan, mutta lähes kaikki yritykset pitivät jatkuvuus- tai toipumissuunnitelmat salaisina. Tekniset yksityiskohdat eivät kuulu kaikille eivätkä edes kiinnosta, mutta liiketoiminnan jatkuvuuden tulisi kiinnostaa. Työntekijöiden tulisi sitoutua ja ymmärtää toimiensa vaikutukset, ja tietoturvaperiaatteiden lisäksi voisi olla perusteltua – vaikka yksinkertaisin esimerkein – kouluttaa, miten yksittäinen työntekijä voi vaikuttaa häiriöttömyyteen.
2. Liiketoiminnan vaikutusanalyysin järjestelmällisyys: Monissa yrityksissä oli tehty ainakin kriittisimmille järjestelmille riskianalyysi tai liiketoiminnan vaikutusanalyysi (BIA), kun taas joissakin yrityksissä tämä oli sisällytetty esim. uuden järjestelmän käyttöönottoon tai muuhun prosessiin, jolloin siitä tulee säännöllistä. Koska suurissa yrityksissä on erilaisia projekteja meneillään jatkuvasti, voi olla perusteltavaa sisällyttää analyysit säännölliseen toimintaan, kuin muutaman vuoden välein tehdä suurempi projekti kaikille järjestelmille. Paras vaihtoehto varmasti on näiden kahden vaihtoehdon yhdistäminen.
3. Jatkuvuussuunnittelun hajauttaminen ja järjestelmällisyys: Lähes kaikissa suuremmissa yrityksissä jatkuvuussuunnittelu oli hajautettu liiketoimintayksikkötasolle, mutta muutama haastateltava kommentoi, että yksi-

köissä ei välttämättä osata tehdä toimivia tai vaikuttavia suunnitelmia. Näissä tapauksissa voi olla aiheellista tarkastaa keskitetysti suunnitelmat tai kouluttaa ja ohjeistaa tekijöitä perusteellisemmin. Liiketoimintayksiköiden johtajien vastuulla on vastata yksikkönsä toiminnan jatkumisesta, ja heidät tulisi sitouttaa myös tähän vaikka tuloksellisuusmittarein.

4. Testaamisen säännöllisyys: Muutamissa yrityksissä suunnitelmien testaaminen oli satunnaista ja aikaa vievää. Joissain yrityksissä tehtiin testausta järjestelmän kriittisyystason mukaan, toisissa testaus oli jatkuvaa, kolmansissa tehtiin kvartaaleittain jollekin järjestelmälle testi. Säännöllinen testaus parantaa toipumisnopeutta, koska käytännöt pysyvät mielessä ja tosi tilanteessa pystytään toimimaan ja toisaalta voidaan huomata ongelmakohdat suunnitelmissa; mutta kunkin organisaation täytyy itse miettiä millainen säännöllisyys on resurssien käytön kannalta järkevää.
5. Raportoinnin säännöllisyys: Tämän tutkimuksen mukaan kun yrityksen ylin johto vaatii jatkuvuudenhallinnan tilanteesta raportin esim. vuosittain ja suurempien häiriöiden jälkeen, muu organisaatio kokee työnsä jatkuvuudenhallinnassa tärkeämmäksi.

5.3 Hyvät käytännöt

Useimmat tässä mainittavat hyvät käytännöt näyttävät olevan peräisin joko erilaisista IT:n governancemalleista tai hyvin koulutetuilta ja tutkimuksessa haastatelluilta tietoturva-asiantuntijoilta. Muutamalla haastatellulla olikin esim. CISSP-koulutus ja ensimmäiseksi voidaan todeta, että sertifioitu tietoturva-asiantuntija näyttää olevan arvokas lisä organisaatiolle.

Häiriöviestinnän määrämuotoisuus on tärkeää häiriötilanteessa, ja tämän tutkimuksen mukaan selkein viestintämalli sisältää yleisen kuvauksen häiriöstä, kuinka kauan sen arvioidaan kestävän ja koska seuraava tieto annetaan jatkotoimenpiteistä. Lisäksi voidaan kertoa, ketä häiriö todennäköisesti koskee ja onko jotain korvaavia järjestelmiä käytössä tai mitä toimenpiteitä vaaditaan käyttäjiltä. Hyvällä ja selkeällä viestinnällä saadaan IT-osaston resurssit kohdistettua häiriön ratkaisemiseen, eivätkä he joudu selittämään kaikille käyttäjätukeen soittaville samaa viestiä.

Tietoturvan hajauttaminen liiketoimintayksiköiden vastuulle ja tietoturvapäällikön toimen lakkauttaminen oli mielenkiintoinen, vaikkei välttämättä kaikkiin yrityksiin sopiva käytäntö. Liiketoimintayksiköiden päälliköt ja järjestelmäkehityksestä vastaavat huolehtivat itse tietoturvan huomioinnista esim. kehitysprojekteissa, sen sijaan että he yrittävät ”ulkoistaa” tietoturvaa asiantuntijalle kutsumalla vain paikalle tietoturva-asiantuntijan, jolla ei välttämättä ole riittävästi arvovaltaa. Tällä tavoin vastuun tietoturvasta koettiin olevan sillä, jolle se kuuluikin.

Suunnitelmamallit olivat hyödyllinen käytäntö. Malleissa kysyttiin ja ohjeistettiin olennaisia asioita jatkuvuuteen tai järjestelmän toipumiseen liittyen. Mallin kysymyksiin vastatessa tulee pohdittua olennaiset asiat kuten testaustavat, järjestelmien väliset riippuvuudet jne.

Muita hyviä käytänteitä olivat: testauksen sitominen kriittisyysluokitukseen (ks. Taulukko 2), sponsorit koulutuksen kutsujina (ks. luvun 4.4 loppu), testauksen säännöllisyys (ks. 5.2) ja testauksen sitominen järjestelmänkehitykseen (ks.luvun 4.2 loppu).

5.4 Jatkotutkimuskohteet ja rajoitukset

Tämä tutkimus on hyvä alku laajemmalle jatkuvuudenhallinnan tutkimukselle Turun kauppakorkeakoulun tietojärjestelmätieteessä. Tätä aineistoa analysoimalla on löydetty monia kokonaisuuksia, joita pitää tarkastella tarkemmin ja syvällisemmin. Esimerkkinä mainittakoon strategisuuden arviointi, ja verkostoituneen yrityksen jatkuvuudenhallinta. Lisäksi tutkimus on ollut tässä vaiheessa lähinnä määrällistä ja kuvailevaa, ja syvemmät tulkinnat on jätetty myöhempään ajankohtaan.

Jatkossa olisi mielenkiintoista tehdä kattavampi kyselytutkimus suuremmalle joukolle yrityksiä sekä Suomessa että ulkomailla. Lisäksi tässä tutkimuksessa havaittiin, että paremman kuvan todellisesta jatkuvuudenhallinnan tilasta olisi saanut haastattelemalla myös liiketoiminnasta vastaavia sekä työntekijöitä, jotka toteuttavat käytänteitä. Muutosten hallinta on osoittautunut haastavaksi monissa yrityksissä samoin kuin ulkoistukseen, pilvipalveluihin ja muihin yritysten ulkopuolisiin yhteyksiin liittyvät asiat. Näihin olisi hyvä perehtyä tarkemmin, koska tietoliikenneyhteydet yrityksien ulkopuolelle ovat arkipäivää ja niistä on tehty hyvin vähän akateemista tutkimusta.

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 tutkimuksen 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.

SUMMARY

In this research project, we have studied business continuity management of IT departments in 18 large private companies in Finland. The report is based on interviews of IT and information security managers, which were conducted in these organisations during 2010. The companies employed at least 250 persons and operated on different industrial sectors, in finance, IT, manufacturing and services.

Based on theoretical literature (Herbane et al. 2004), business continuity management (BCM) can be considered to have strategic importance for a company if during a disruption 1) recovery is fast, 2) the company is resilient, and 3) the business continuity practices have been embedded in organisation's processes as well as 4) there are legislative or other drivers for continuity management. We discovered that in eight interviewed companies BCM had a strategic role, but in other studied organisations it had only a supportive role. We also found out that business is still interrupted or severely complicated in many companies when critical information systems are experiencing a disruption. This indicates that business continuity of IT department should be planned and managed by top management, and implemented in business units and in the IT department.

Almost all studied companies had documented business continuity or disaster recovery plans at least for the most critical information systems and in many they were regularly tested. In most organisations, top management participated in BCM and in larger companies plans were designed by business units. According to previous studies, the business continuity plans would be better embedded in business processes if everybody would know about the plans, which was not the case in interviewed companies. All organisations had prepared well for infrastructure and information security risks, but changes in for example information systems were still triggering problems for continuity.

Many larger companies had outsourced the majority of IT services and infrastructure, and the experienced outsourcers also used cloud computing but in smaller companies of this study did not use cloud services. We discovered several best practices during these interviews and make recommendations based on them in the end of the report.

LÄHTEET

Albrechtsen, E. – Hovden, J. (2009) The information security digital divide between information security managers and users. *Computers & Security*, Vol. 28(6), 476-490.

Copenhaver, J. – Lindstedt, D. (2010) From cacophony to symphony: How to focus the discipline of business continuity. *Journal of Business Continuity & Emergency Planning*, Vol. 4(2), 165–173.

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

Elliott, D. – Swartz, E. – Herbane, B. (2011). *Business continuity management: a crisis management approach.* New York: Routledge.

Ernst & Young (2010) *Borderless security: Ernst & Young's 2010 Global Information Security Survey*.<http://www.ey.com/GL/en/Services/Advisory/IT-Risk-and-Assurance/13th-Global-Information-Security-Survey-2010---Information-technology--friend-or-foe->, haettu 24.3.2011.

Gallagher, M. (2007) Business Continuity Management Emerging Standards. *Accountancy Ireland*, Vol. 39(3), 34-36.

Gibb, F. – Buchanan, S. (2006) A framework for business continuity management. *International journal of information management*, Vol. 26(2), 128–141.

HB 292-2006 (2006) A Practitioners Guide to Business Continuity Management (sample). <http://www.saiglobal.com/PDFTemp/Previews/OSH/as/misc/handbook/HB292-2006.pdf>, haettu 24.3.2011.

Hecht, J.A. (2002) Business continuity management. *Communications of the Association for Information Systems*, Vol. 8(30).

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

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

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

Luoma-aho, V. – Paloviita, A. (2010) Actor-networking stakeholder theory for today's corporate communications. *Corporate Communications: An International Journal*, Vol. 15(1), 49-67.

Rittinghouse, J.W. – Ransome, J.F. (2005) *Business continuity and disaster recovery for infosec managers*, Elsevier Digital Press, doi:10.1016/B978-155558339-2/50007-3.

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

Snedaker, S. (2007) *Business continuity & disaster recovery for IT professionals*, Syngress Media Inc.

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

Tammineedi, R.L. (2010) Business Continuity Management: A Standards-Based Approach. *Information Security Journal: A Global Perspective*, Vol. 19(1), 36–50.

TURUN KAUPPAKORKEAKOULUN JULKAISUSARJASSA KESKUSTELUA JA RAPORTTEJA OVAT VUODESTA 2010 LÄHTIEN ILMESTYNEET SEURAAVAT JULKAISUT

KR-1:2010 Niina Nummela & Mélanie Raukko (eds.)
Managing cross-border acquisitions

KR-2:2010 Anna-Maija Kohijoki
Päivittäistavarakaupan palvelujen saavutettavuus liikuntavammaisten kuluttajien näkökulmasta

KR-1:2011 Sabine Grasz & Joachim Schlabach
Business students' choices of foreign languages

KR-2:2011 Jonna Järveläinen & Antti Lehtimäki
Tietohallinnon jatkuvuudenhallinta valikoiduissa suomalaisissa suuryrityksissä vuonna 2010

Kaikkia edellä mainittuja sekä muita Turun kauppakorkeakoulun julkaisusarjoissa ilmestyneitä julkaisuja voi tilata osoitteella:

KY-Dealing Oy
Rehtorinpellonkatu 3
20500 Turku
Puh. (02) 333 9422
E-mail: ky-dealing@tse.fi

All the publications can be ordered from

KY-Dealing Oy
Rehtorinpellonkatu 3
20500 Turku, Finland
Phone +358-2-333 9422
E-mail: ky-dealing@tse.fi