

Alvar Perttunen

RISKIENHALLINTAA EDISTÄMÄSSÄ VAI HIDASTAMASSA?

Pk-yrityksille asetetut kontrollivaatimukset
kybervakuuttamisen näkökulmasta

TIIVISTELMÄ

Alvar Perttunen: Riskienhallinta edistämässä vai hidastamassa: Pk-yrityksille asetetut kontrollivaatimukset kybervakuuttamisen näkökulmasta

Ohjaaja: Timo Rintamäki

Pro gradu -tutkielma

Tampereen yliopisto

Kauppätieteen tutkinto-ohjelma, Vakuutustiede

Joulukuu 2024

Kybermaailma saattaa olla pk-yritykselle käsitteenä hieman hämärä ja jopa uhkakuvia mieleen tuova, mutta käytännössä se on nykypäivänä mille tahansa liiketoiminnalle täysin välttämätön osa-alue yrityksen koosta huolimatta. Digitalisaatio mahdollistaa yrityksille valtavan määrän tietoa, tehokuutta sekä työkaluja parantaa asiakaskokemusta ja kehittää liiketoimintaa. Edistyksellä on kuitenkin myös varjopuolensa – nimittäin kyberriskit. Ne ovat mittauksissa nousseet räjähdysmäisesti merkittävimmäksi yksittäiseksi riskilajiksi; tuhansia yrityksiä ajautuu niiden vuoksi konkurssiin ja miljardeja häviää kyberrikollisuuden kitaan vuosittain. Vakuutusyhtiöiden rooli on ollut läpi historian toimia riskienhallinnan edistäjinä, eivätkä kyberriskit tee tähän poikkeusta. Yhtiöiden rooli hakee kuitenkin vielä lopullista muotoaan kyberriskien kehittyessä dynaamisesti ja kasvavien vakuutusmarkkinoiden pyrkiessä seuraamaan muutosta. Osapuolten yhteinen intressi on tietysti riskien mitigointi, mutta miten tavoitella saavutetaan kybervakuuttamisen näkökulmasta onkin haastavampi kysymys.

Tämän tutkielman tarkoitus on syventyä kybervakuuttamiseen ja tarkemmin sen yhteen osa-alueeseen eli vakuutusyhtiöiden asettamiin kontrollivaatimuksiin. Kyberriskikontrolleilla pyritään pienentämään yrityksen riskitasoa ja suojautumaan mahdollisilta kyberriskeiltä. Niiden tavoitteena ei ole pelkästään pyrkiä keinoilla millä tahansa välttymään kyberhyökkäyksiltä, vaan myös nostamaan yrityksen valmiutta reagoida ja toipua mahdollisesta poikkeamatilanteista. Tutkielman tavoitteena on selvittää, minkälaisia vaatimuksia vakuutusyhtiöt asettavat pk-yrityksille ja mikä niiden rooli on isommassa kuvassa pk-yritysten kyberriskien hallinnan osalta. Tutkielma lähestyy käsiteltävää aihetta vakuutusyhtiöiden näkökulmasta. Tutkielma toteutetaan laadullisena tutkimuksena, joka palvelee parhaiten tavoitetta ymmärtää paremmin ilmiön taustaa ja kontrollien vaikutuksia. Teoriaosuus pohjautuu vakuutustieteen ja kyberturvallisuuden tieteenalojen kirjallisuuteen. Kyberriskien, pk-yritysten riskienhallinnan ja kontrollivaatimusten väliset suhteet pyritään määrittelemään mahdollisimman tarkasti, jotta haastatteluaineiston perusteella saatuja tuloksia voidaan peilata niitä vastaan. Empiriaosuuden aineisto on kerätty teemahaastatteluiden avulla ja analysoitu teoriasidonnaisella sisällönanalyysillä.

Kontrollivaatimusten voidaan ajatella olevan kaksiteräinen miekka kyberriskejä vastaan, toisaalta ne kertovat yritykselle vakuuttajan laajaan dataan perustuen vähimmäistason, jolla kyberturvan tulisi olla, mutta toisaalta ne voivat myös olla yrityksen liiketoimintaan epäsovivia ja vaatia yritykseltä joissain tilanteissa liian suuria resursseja niistä saatavaan hyötyyn nähden, jolloin riski saattaa jäädä kokonaan vakuuttamatta. Parhaimmillaan ne voivat motivoida ja asettaa standardin pk-yritystä kriittisen kyberturvan perustason saavuttamisessa, huonoimmillaan ne lannistavat ja hidastavat riskienhallinnan kehittymistä. Kontrollivaatimukset ovat konkreettinen mahdollisuus vakuutusyhtiöille vaikuttaa yritysten riskienhallinnan tekniseen ja hallinnolliseen tasoon ja isossa kuvassa myös toimia yhteiskunnallisena suunnannäyttäjänä, mutta tasapainon löytäminen vaatimustason ja riskinoton välillä on todellinen haaste.

Tutkielman tulosten perusteella voidaan todeta, että kybervakuuttaminen ja kontrollivaatimukset ovat tulleet pysyvästi jäädäkseen myös pk-sektorille, mutta kontrollitason vakiintumisesta ei voida vielä puhua. Vaatimukset vaikuttavat keventyvän vakuuttamisprosessin tehostamisen ja myyninedistämisen nimissä, jota pyritään paikkaamaan erilaisilla työkaluilla teknologian kehityksen myötä. Kontrolleilla on todistetusti merkittävä vaikutus kyberriskien toteutumisen todennäköisyyksiin, joten vakuuttajien valinnoilla tulee olemaan pidemmällä aikavälillä merkittävä vaikutus kybervakuuttamisen yleistyyssä.

Avainsanat: Kybermaailma, kyberriskit, kyberriskikontrollit, kontrollivaatimukset, kybervakuuttaminen, pk-yritys

Tämän julkaisun alkuperäisyys on tarkastettu Turnitin OriginalityCheck –ohjelmalla.

SISÄLLYSLUETTELO

1	JOHDANTO.....	5
1.1	Tutkielman tausta ja merkitys.....	5
1.2	Tutkimuksen tavoitteet ja tutkimuskysymykset	8
1.3	Keskeiset käsitteet	10
1.4	Tutkimuksen tieteenfilosofia	12
1.5	Tutkimusmenetelmät	13
1.6	Teoreettinen viitekehys ja tutkielman rakenne	15
2	KYBERRISKI JA SEN VAKUUTTAMINEN	19
2.1	Kybermaailma	19
2.2	Kyberriskit	20
2.3	Kyberriskien hallinta	22
2.3.1	Kyberriskien eri hallintakeinot	24
2.3.2	Standardeihin perustuva hallinta	26
2.4	Kybervakuuttaminen	30
2.4.1	Vakuuttamiskelpoisuus.....	33
3	KONTROLLIVAATIMUKSET	39
3.1	Vähimmäisvaatimukset	39
3.2	Kontrollivaatimusten merkitys	42
3.2.1	Vakuutusyhtiön näkökulmasta	43
3.2.2	Pk-yrityksen näkökulmasta.....	46
3.2	Kontrollivaatimukset osana riskienhallintaa.....	48
3.3	Resurssi- ja kustannusvaatimukset	49
3.4	Kontrollivaatimusten historia ja tulevaisuus	52
4	ASiantuntijoiden näkökulmia kybervakuutusten kontrollivaatimuksiin.....	55
4.1	Aineiston keruu ja käsittely	55
4.2	Nykyiset kontrollivaatimukset pk-yrityksille	58
4.2.1	Vähimmäisvaatimukset	59
4.2.2	Vakuuttajien painotukset ja muutosajurit	60
4.3	Vaatimusten merkitys yrityksen kyberturvallisuuden tasoon.....	63
4.3.1	Kontrollien soveltuvuus ja tarkastus.....	65
4.4	Kontrollivaatimusten haasteet	67
4.4.1	Tulevaisuuden kehitysmahdollisuudet	69
5	YHTEENVETO.....	72
5.1	Tutkimuskysymyksiin vastaaminen ja johtopäätökset	72

5.2 Tutkielman arviointi	79
5.3 Lopuksi	81
LÄHTEET	83
Kirjallisuuslähteet.....	83
Verkkolähteet.....	85
Henkilölähteet.....	89
LIITTEET	90
Liite 1: Asiantuntijoiden haastattelurunko	90

1 JOHDANTO

1.1 Tutkielman tausta ja merkitys

Tutkielman taustalla on kybermaailman jatkuva laajeneminen ja sen yhteiskunnallisen merkityksen kasvu. Samalla kun kybermaailma vaikuttaa laajemmin eri yhteiskunnan sektoreilla, sen riskit kasvavat ja se luo yhä merkittävämmän uhan eri organisaatioille. Kybervakuuttaminen on ollut pitkään jo yksi puhutuimmista vakuutuslajeista. Syitä tähän on tietysti monia, mutta keskeisimpinä teknologian levittäytyminen kaikkiin yhteiskunnan osa-alueisiin, kyberrikollisuuden ammattimaistuminen ja aktivoituminen sekä kyberriskien hallinnan tietoisuuden parantuminen. Vaikkakin vakuuttaminen on vain yksi mahdollisista riskienhallintakeinoista, on se yksi oleellisimmista keinoista; riskin siirtäminen ja yrityksen taseen suojaaminen ennalta-arvaamattomilta suurilta tappioilta on monille organisaatiolle ainoa keino selvitä laajamittaisesta kybervahingosta ilman ajautumista maksuvaikeuksiin. On siis perusteltua selvittää, miten kybervakuutusprosessi toimii, mikä merkitys on kontrollivaatimuksilla tässä prosessissa ja minkälaista problematiikkaa ja mahdollisuuksia näihin mahdollisesti liittyy.

Samoin kuin yksilöt, myös yritykset ovat yhä riippuvaisempia teknologiasta ja sen luomasta kybermaailmasta. Nykypäivänä tämä maailma mahdollistaa ja tehostaa lähes kaikkien yritysten liiketoimintaa, mutta sillä on myös varjopuolensa, kyberriskit. Kyberriskien hallinta on viime aikoina korostunut entisestään kybervahinkojen määrän ja globaaleiden riskien ja epävarmuuksien lisääntyessä. Turvallisuusalalla valitettavaa on, että usein vasta lähelle tulevat realisoituneet riskit aiheuttavat aktivoitumista riskienhallinnan suhteen. Kyberriskit eivät myöskään kosketa ainoastaan yrityksiä, vaan myös yksilöitä ja yhteiskuntia. Kyberrikollisuuden laajuutta voidaan havainnollistaa sen arvioidulla maailmanlaajuisella mittakaavalla; jos se suhteutettaisiin valtioihin, sen voitaisiin ajatella olevan maailman kolmanneksi suurin talous Yhdysvaltojen ja Kiinan jälkeen (World Economic Forum, 2024). Tavallisilta ihmisiltä ja yrityksiltä häviää kyberrikollisuuden kitaan arvioiden mukaan miljardeja euroja vuosittain ja summat ovat vain kohoamassa (IBM, 2024). Kyberrikollisuudesta puhutaankin usein digitaalisen vallankumouksen väistämättömänä varjopuolena.

Mikä vakuutusten rooli sitten tässä kokonaisuudessa sitten on? Vakuutusten voidaan ajatella olevan yhteiskunnan taloudellinen tukipilari. Ne luovat taloudellista turvaa, auttavat kestämaan katastrofeja ja tarjoavat riittävän riskienhallinnan, jotta markkinataloudelle elintärkeä ominaisuus eli riskinotto on

mahdollista (finanssialalle, 2024). Ilman vakuutuksia kukaan tuskin harkitsisi jättimäisiä vihreän siirtymän investointeja tällä hetkellä Suomeen tai muuallekaan. Harva kansalainen tulee ajatelleeksi niiden merkitystä arjessa, mutta loppujen lopuksi harva yhteiskunnan kriittinenkään toiminta olisi mahdollista ilman vakuutuksia. Riskien jakaminen ja niiden sattumanvaraisen luonteen muuttaminen tasaiseksi vakuutusmaksuksi sisältää yllättävän suuren arvon. Voidaan jopa ajatella, että suuri osa modernin yhteiskunnan toimista muistuttaa vakuutustoimintaa (Kivisaari & Rantala, 2020). Vakuutusyhtiöillä on myös valtava määrä historiatietoa riskeistä ja sattuneista vahingoista, mikä on kriittistä etenkin uuden riskityypin, kuten kyberriskin, hallintaa ajatellessa.

Kybervahingot ovat osoittaneet, että pienestäkin vaikeasti ennustettavasta erheestä voi seurata massiivisen kokoiset taloudelliset tappiot, jolloin vakuutuskorvaukset ovat eloonjäämisen kannalta välttämättömyys. Tähän kuitenkin liittyy myös suuri haaste; miten vakuuttajat kykenevät hallitsemaan lähes loputonta kybermaailman riskikenttää ja poimimaan sieltä vakuutettaviksi sellaisia riskejä, jotka he pystyvät arvioimaan riittävän täsmällisesti ja siten varmistamaan riskinkantokykynsä ja kannattavan liiketoiminnan. Puhutaan kyberriskikontrolleista ja niiden vaatimustenmäärittelystä, minkä avulla vakuutusyhtiöt pyrkivät varmistumaan siitä, millaisia kyberriskejä tietyn yrityksen toimintaan liittyy, miten se pyrkii niitä hallitsemaan ja toisaalta reagoimaan sekä palautumaan organisaationa, mikäli vahinko joka tapauksessa sattuu.

Vakuutusyhtiöillä on suuri vaikutusvalta riskienhallinnan kehitykseen etenkin Suomessa, jossa ala on hyvin keskittynyttä, riskienhallinta yleisesti hyvällä tasolla ja vakuutusyhtiöt luotettavia. Koska kybervakuutus on yhä useimmin välttämättömyys mahdollisuuden sijaan, asetetuilla kontrolleilla pystytään vaikuttamaan siihen, mihin suuntaan riskienhallintaa viedään ja mitä teknisiä ratkaisuja ja käytännön toimenpiteitä vaaditaan hyväksyttävään kontrollitasoon ja riskin vakuutettavuuteen. Samalla on kuitenkin hyvä muistaa, etteivät kontrollivaatimukset ole automaattisesti pelkästään hyvä asia. Kyberriskit muuttuvat nopeasti, eivätkä vakuutusyhtiöt ehdi aina muutosvauhtiin mukaan kontrollien osalta. Pk-yrityksiä kohdellaan usein isona massana ja vakuutus tuotteiden räätälöinti on harvinaisempaa, jolloin myös kontrollivaatimukset saattavat soveltua huonommin yrityksen liiketoimintaan eikä niiden teho välttämättä vastaa niihin käytettyjä resursseja.

Samoin kuten vakuutukset ovat hyvinvointiyhteiskunnan toiminnan kannalta hyvin oleellisia, ovat vakuutusyhtiöt näiden kulmakivien kantajia. Etenkin Suomessa vakuutusyhtiöt ovat läpi historian toimineet soihdunkantajina riskienhallinnan saralla, ja tässä roolissa asetettavat riskien kontrollivaatimukset ovat keskeinen työkalu. Usein kuulee puhuttavan siitä, kuinka Suomi on

yrityksille hyvä maa toimia, sillä luonnonkatastrofiriskejä ei käytännössä ole. Ei vulkaanista savua tupruttavia tai lunta vyöriä vuoria, ei järiseviä mannerlaattoja tai trooppisia hirmumyrskyjä. Kuitenkin koronapandemian levitessä ja ajaessa monia yrityksiä syvään ahdinkoon, saivat suomalaiset samalla muistutuksen toisenlaisesta mahdollisesta katastrofin olemassaolosta; nimittäin kyberkatastrofista. Traficomien alaisen kybeturvallisuuskeskuksen ylläpitämien tilastojen valossa vuonna 2020 Suomessa ilmoitettiin kyberhyökkäyksiä 1521 kappaletta, kun taas seuraavana vuonna ilmoitusten määrä nousi yli nelinkertaiseksi, 6795 kappaleeseen (Traficom, 2024). On kuitenkin syytä huomata, että kyse on suomalaisten organisaatioiden tekemistä virallisista ilmoituksista, eli todellisten hyökkäysten määrä lienee vielä suurempi. Joka tapauksessa luvut antavat osiittaa vahinkokehityksestä, jonka pohjalta vakuuttajien kiristyneet kontrolli- ja hintavaatimukset eivät ole ihme. Kyberriskien globaali luonne tarkoittaa, että kansainvälisesti luvut seurailevat samaa trendiä, mikä on myös nähtävissä kansainvälisten kybervakuutusten hintakehityksestä (kuvio 9).

Vakuuttajien tehtävä on luonnollisesti kannustaa yrityksiä vakuuttamaan omia kyberriskejä, mutta ei hinnalla millä hyvänsä. Kyberriskit ovat ennennäkemättömän dynaaminen riskilaji, joiden arvioiminen on haastavampaa johtuen ennen kaikkea jatkuvasta muutoksesta ja kehityksestä. Tämä puolestaan johtuu pitkälti teknologisen kehittymisen eksponentiaalisesta luonteesta. Siksi ennakointi ja ennaltaehkäisevät toimenpiteet nousevat yhä suurempaan rooliin, mikä on ollut vakuutusyhtiöiden intressissä jo pidempään (Kivisaari & Rantala, 2020). Kontrollivaatimukset ja niiden jatkuva kehittäminen ja analysointi ovat tästä hyvä esimerkki. Kyberriskien välttäminen on kaikkien yhteinen intressi, ja siinä vakuutusyhtiöillä on merkittävä asiantuntijan rooli. Asiakkailta kerättyä informaatiota hyödyntämällä, vakuutusyhtiöt kykenevät luomaan riittävän perustason omasuojaan ja parhaassa tapauksessa standardoimaan sen, jolloin yritysten rooli riskienhallinnassa helpottuu. Näin on käynyt myös perinteisemmissä riskilajeissa, kuten paloriskissä. Vakuuttajan tehdessä omat riskiarvionsa esimerkiksi tuotantolaitoksen paloriskeistä ja niihin liittyvistä suositeltavista suojelutoimenpiteistä, voi yrityspäätätjä suhteellisen rauhallisin mielin luottaa toimenpiteiden toteuttamisen jälkeen riskin olevan riittävältä osin hallittu. Etenkin Suomessa vakuuttajia on pidetty riskienhallinnan edistäjinä, kuten vaikkapa tuotantolaitosten automaattisten sammutusjärjestelmien laaja käyttöönotto osaltaan osoittaa (Karhunen, 2014). Kybervakuuttamisen saralla vastaavanlaista kehitystä on jo pienemmässä mittakaavassa havaittu.

Vakuuttajien panostaessa yhä enenevässä määrin riskien preventioon pelkän maksuntasajan roolin sijaan, on niiden rooli yksilön, yrityksen ja yhteiskunnan tasolla kasvavaa (Kivisaari & Rantala, 2020). Kybervakuuttamisen osalta sen merkitys on vielä laajemmassa mittakaavassa osittain hämärän

peitossa, johtuen toisaalta tutkimustiedon vähäisyydestä ja toisaalta ilmiön dynaamisuudesta; viimeiseltä viideltä vuodelta kerätty vahinkotieto ei ole millään tavalla tae tulevasta. Koska yritykset ovat yhteiskunnan hyvinvoinnin mahdollistaja, keskityn tässä tutkielmassa selvittämään sitä, kuinka kybervakuuttamisen ilmiö laajentuu yritys kentällä pienempiin yrityksiin, millaisilla kontrollivaatimuksilla vakuuttajat pyrkivät markkina laajenemista hallitsemaan ja minkälaisia ongelmia sekä mahdollisuuksia tähän ilmiöön liittyy. Pk-yritykset ovat relevantti rajaus, sillä vakuutusyhtiöt tarkastelevat isompia yrityksiä usein tapauskohtaisesti myös kontrollivaatimusten osalta, mutta niiden osuus Suomessa on vain 0,2%:a kaikista yrityksistä (Suomen Yrittäjät, 2020). Pk-yritykset muodostavat siis suuren markkina-alueen, mutta koska niille usein sovelletaan vakio muotoisia vaatimuksia vakuutettavuuden täyttämiseksi, on mielenkiintoista tutkia millaisia kontrolleja vakuuttajat tällä hetkellä ovat niille valinneet, ja mitä ajatuksia heillä on tulevaisuuden kehityksestä.

1.2 Tutkimuksen tavoitteet ja tutkimuskysymykset

Tutkielman tarkoitus on selvittää, millaisia vaatimuksia kybervakuutusta tarjoavilla vakuutusyhtiöillä on käytössä, minkälainen vaikutus niillä on kyberriskien hallintaan vakuuttajan näkökulmasta sekä millaisia haasteita ja mahdollisuuksia niihin liittyy. Tarkoituksena on kartoittaa ja määritellä minkälaisesta ilmiöstä nykypäivänä on kyse, ja millainen sen rooli on isommassa riskienhallinnan kuvassa. Tutkimuksen tavoitteena on kokonaisvaltaisesti parantaa ymmärrystä pk-sektoria edustavien yritysten kyberriskien hallinnasta ja sen kontrolloinnista vakuuttamisen kontekstissa. Erityisesti tavoitteena on analysoida vakuuttajien asettamien kontrollivaatimusten vaikutusta ja niiden roolia kyberriskienhallinnassa. Tutkielma rakentuu kolmen tutkimuskysymyksen pohjalle, jotka määrittelevät samalla tutkimuksen päätavoitteet ja -rajaukset.

Tutkielman tutkimuskysymykset ovat seuraavat:

- 1) Millaisia kontrollivaatimuksia vakuuttajat asettavat pk-yrityksille kybervakuuttamisen osalta?
- 2) Miten kontrollivaatimukset vaikuttavat pk-yritysten kyberriskien tasoon ja niiden hallintaan?
- 3) Millaisia haasteita ja kehittymismahdollisuuksia vakuuttajien asettamiin kontrollivaatimuksiin liittyy?

Ensimmäisen tutkimuskysymyksen avulla haetaan vastausta oleelliseen perustietoon: millaisia kontrollivaatimuksia ylipäätään on juuri pk-sektorin kokoluokan yrityksille. Tämän kysymyksen

avulla pohjustetaan muita tutkimuskysymyksiä ja pyritään luomaan läpileikkaus vakuuttajien kyberriskien hallinnan nykytilanteesta. Toinen tutkimuskysymys keskittyy vakuuttajien sijasta yrityksiin. Kysymyksen tavoitteena on selvittää, millä tavoilla vakuuttajien vaatimat kontrollit parantavat pk-yrityksen kyberturvallisuuden kypsyystasoa ja toisaalta, parantavatko vaatimukset organisaatioiden kyberriskien hallintaa tai yleisesti riskienhallintaprosesseja. Kolmas tutkimuskysymys keskittyy kartoittamaan nykytilanteessa havaittuja ydinhaasteita, ja sitä miten näistä haasteista katse voitaisiin siirtää kohti tulevaisuutta; miten ongelmat voitaisiin mahdollisesti ratkaista ja mitä mahdollisuuksia kontrollivaatimukset riskienhallintaan ja turvallisempaan kybermaailmaan tuo isossa kuvassa.

Lisäksi tutkimuskysymysten tarkoituksena on määritellä ja rajata aiheeseen liittyvää terminologiaa ja niiden välisiä vaikutussuhteita työn selkeyden sekä onnistuneiden tutkimushaastatteluiden saavuttamiseksi. Kysymykset täyttävät niille tutkimuksen kannalta oleellisia tehtäviä: 1) määrittelemään tutkimuksen suunnan, 2) rajaamaan riittävästi aihetta ja 3) tukemaan tulkintaa analyysivaiheessa (Hirsjärvi, Remes & Sajavaara, 2009). Hyvin laadittujen tutkimuskysymysten tarkoitus on taata riittävä fokus ja suunta tutkimukselle alusta lähtien. Tavoitteena on saada teoriaosuuden taustoituksella ja empiriatulosten analysoinnilla sekä niiden välisellä dialogilla mahdollisimman laadukkaat vastaukset valittuihin tutkimuskysymyksiin.

Tavoitteiden saavuttamisen kannalta on erityisen tärkeää määritellä ja rajata riittävän tarkasti käsiteltävät käsitteet ja aihealueet. Koska kyberriskejä tarkastellaan yrityksissä kokonaisvaltaisen riskienhallinnan ja siihen liittyvän päätöksenteon kannalta, on vakuuttaminen riskienhallinnan näkökulmasta lopulta vain yksi keino muiden joukossa. Keskeisin raja-alue liittyykin vakuuttamisen ja riskin kontrolloimisen tasapainoon. Yrityksen näkökulmasta vakuuttaminen ja kyberturvallisuuteen panostaminen ovat molemmat resursseja vaativia toimenpiteitä, joihin kuluviin investointien tasapainoa pyritään jatkuvasti arvioimaan. Tämä seikka on myös huomioitava vakuutusyhtiöissä kontrollivaatimusten kontekstissa; tekniset ja hallinnolliset kontrollit ja niiden merkitys kokonaisuuden kannalta on huomioitava arvioidessa optimaalista vaatimustasoa. Pk-yritysten kyberturvallisuuden kypsyystaso voi olla usein suhteellisen alkeellistakin ja tietämys heikkoa, minkä takia tutkielma lähestyy aihetta vakuutusyhtiöiden ja asiantuntijoiden näkökulmasta.

Lisäksi tutkielmassa keskitytään analysoimaan pk-sektoria edustavia yrityksiä. Tämä on perusteltua muutamasta syystä. Ensinnäkin vakuutusyhtiöt jakavat usein oman toimintansa kahteen yritysköön perusteella: pk-sektoriin ja suuryrityksiin. Tämän taustalla on tietysti riskin koko ja sen hallittavuus.

Pk-yrityksillä yksittäiset riskit ovat usein pienempiä ja sitä kautta myös vakuuttajan ottama riski on maltillisempi, jolloin riskiä ei lähtökohtaisesti analysoida yhtä tarkasti kuin suuryritysten vastaavia. Pk-yritysten osalta strategiana on usein rakentaa volyymiltaan suuri pooli, jonka avulla hallitaan sen riskejä ja jonka takia myös maksutaso voi olla maltillisempi (Kivisaari & Rantala, 2020). Siksi kontrollivaatimukset ovat usein laajempia suuryrityksille, mutta pk-sektorin osalta tilanne on hieman mutkikkaampi; mihin vakuuttajat vetävät rajan kybervakuuttamisen yleistyessä? Suhteessa suuriin yrityksiin vaatimuksia täytyy varmasti keventää, mutta kuinka paljon ja mitkä ovat kriittisiä kontrolleja säilyttää, ovat avainkysymyksiä jotka säilyvät vielä toistaiseksi avoimina.

1.3 Keskeiset käsitteet

Kyber-alkuiset käsitteet ovat monille vieraita, eikä kybermaailmaan liittyvien käsitteiden määrittely ei ole vielä täysin vakioitunutta. Universaaleja määritelmiä ei ole joissain tapauksissa edes olemassa, etenkin paikallisella kielellä. Suomenkielistä tieteellistä kirjallisuutta aiheesta on hyvin vähän olemassa ja käsitteitä ei välttämättä ole ollenkaan saatavilla, saati sitten tarkkoja määritelmiä niiden osalta. Tästä syystä on oleellista täsmentää tutkielmassa käsiteltävän teeman osalta keskeisimmät käsitteet ja niiden rajaus. Tämä lisää tutkielman selkeyttä, vähentää väärinymmärryksiä ja palvelee tutkimuksen tavoitteita. Käsitteiden määrittelyssä on pyritty valitsemaan alalla yleisesti käytettyjä termejä ja niiden määritelmiä. On hyvä huomioda, että eri tahojen välillä on vaihtelua siinä, kuinka käsitteet ymmärretään, mutta tässä tutkielmassa niitä sovelletaan seuraavasti:

Kybermaailmasta saatetaan käyttää myös termejä *kyberympäristö* tai *kyberavaruus*, mutta omasta mielestä kybermaailma on maanläheisin ja ymmärrettävin. Sillä tarkoitetaan eri tietojärjestelmistä, tietoverkoista ja tietotekniikkalaitteista muodostuvaa digitaalista kokonaisuutta (Limnell ym., 2014). Yksinkertaistaen voidaan sanoa, että kyberympäristö on se paikka, missä sähköinen viestintä ja tietojenkäsittely tapahtuu. Se luo oman ”maailmansa” perinteisen fyysisen maailman rinnalle, toisaalta niiden jatkuvasti integroitua tiiviimmin toisiinsa muodostaen sen todellisuuden missä elämme.

Kyberturvallisuus on ollut monien huulilla etenkin viime vuosina tietoisuuden lisääntyessä ja ihmisten paremmin ymmärtäessä sen arvon. Kyberturvallisuudella tarkoitetaan nimensä mukaisesti turvallisuutta kybermaailmassa. Tarkennettuna se syntyy toimenpiteistä, jotka luovat tavoitetilan turvallisuuteen digitaalisessa ympäristössä (Limnell ym., 2014). Turvallisuushan ei ole vaarojen ja riskien poissaoloa, vaan niiden onnistunutta hallintaa. Kyberturvallisuuden muodostaa neljä seikkaa:

teknologiset ratkaisut (esim. palomuurit ja varmuuskopiot), ihmisten käyttäytyminen (yksilöinä, yrityksissä ja yhteiskunnassa), harjoittelu ja varautuminen sekä vakuuttaminen.

Kyberriskit voidaan jakaa karkeasti kahteen; kyberhyökkäyksistä ja tietovuodoista muodostuvat riskit. Toki riskejä on paljon muitakin, mutta tällä jaolla haetaan sitä, että kaikki riskit eivät ole ulkoisia eivätkä edes rikollisten tai vihamielisten valtiollisten toimijoiden aiheuttamia, vaan usein sisäiset riskit näyttelevät isoa osaa, esimerkiksi työntekijöiden tekemät virheet aiheuttavat yli puolet tietovuodoista (IBM, 2024). Kyberriskit tarkoittavat siis mitä tahansa riskejä, jotka uhkaavat kyberturvallisuutta. Riski sisältää siis uhan, haavoittuvuuden ja vaikutuksen liiketoimintaan (Marotta ym., 2017). Kyberriskin realisoituessa syntyy yritykselle kybervahinko, joka voi olla korvattava kybervakuutuksesta, mikäli organisaatiolla sellainen on hankittu.

Kyberriskikontrollit ovat niitä toimenpiteitä, joita yritys harjoittaa parantaakseen omaa kyberturvallisuutensa kypsyystasoaan ja siten myös pienentämään riskitasoaan. Peruskontrollit (kuvio 4) ovat etenkin vakuuttajien toimesta suhteellisen vakioituja, mutta asetetun vaatimukset niiden osalta vaihtelevat voimakkaasti. Tavallisia perustason kontroleja, jotka kaikilla yrityksillä koosta huolimatta tulisi olla kunnossa on monivaiheinen tunnistautuminen, varmuuskopiointi ja sähköpostisuodatus. Yrityksen tehdessä riskienhallintaa, se arvioi kyberriskin kokonaistason nykyisillä kontroleillaan, ja mikäli se arvioi jäännösriskin liian suureksi, voi se sen jälkeen joko lisätä tai parantaa nykyisiä kontroleja tai vaihtoehtoisesti siirtää riskiä vakuuttajalle ostamalla kybervakuutuksen (Dambra, Bilge & Balzarott, 2020).

Kontrollivaatimuksilla tarkoitetaan tässä tutkielmassa taas niitä kybervakuuttajien asettamia vaatimuksia kontroleista, jotka tulisi olla tietyllä vaaditulla tasolla, jotta vakuutuksen voi ylipäättään hankkia. Vaatimukset vaihtelevat vakuutusyhtiöittäin, ja luonnollisesti myöskin vakuutusyhtiön sisällä asiakaskohtaisesti. Eri vakuuttajilla on hyvinkin erilaisia riskinottohalukkuuksia (risk appetite) kyberriskien osalta, johtuen strategisista valinnoista, mikä näkyy asiakkaille eritasoisina kontrollivaatimuksina sekä tietysti hintatasona ja ehtoeroina. Etenkin perustason kontrollit vaikuttavat merkittävästi kyberriskien todennäköisyyteen (Dambra ym, 2020), joten vakuuttaja on niiden tilasta erityisen kiinnostunut. Haaste onkin löytää tasapaino vaatimustasoon vakuuttamisen kontekstissa.

Pk-yritys määritellään yritykseksi, jonka palveluksessa on enintään 250 työntekijää, ja jonka vuosiliikevaihto on enintään 50 miljoonaa euroa tai taseen loppusumma 43 miljoonaa euroa. EU:n

alueella toimivista yhtiöistä 99%:a on luokaltaan pk-yrityksiä (Euroopan unioni, 2017). Pk-yritykset voidaan jakaa virallisessa määritelmässä vielä alakategorioihin, eli mikroyrityksiin (max. 10 työntekijää), pieniin yrityksiin (alle 50 työntekijää) ja keskisuuriin (alle 250 työntekijää). Mikroyritykset ovat kuitenkin rajattu tästä tutkimuksesta pois, johtuen kybervakuuttamisen vähyydestä kyseisen kokoluokan yrityksissä. Kyberturvallisuuden kontekstissa pk-yrityksille keskeisiä ominaisuuksia ovat ketteryys, niukat resurssit, tietoisuuden puute ja vahva palveluiden ulkoistaminen (Hoppe & ym., 2021).

1.4 Tutkimuksen tieteenfilosofia

Tieteenfilosofialla tarkoitetaan tutkimuksen osakokonaisuutta, jonka tutkijan tai tutkijoiden siihen liitetyt oletukset ja uskomukset muodostavat eli miten tietoa lähestytään. Tieteenfilosofia on oleellista määrittellä riittävän tarkasti ennen tutkimuksen varsinaista toteuttamista, sillä tutkijan oletukset vaikuttavat joka tapauksessa joko tiedostomatta tai tietoisesti tutkimuksen tuloksiin. Siksi tiedostetut valinnat oletuksiin liittyen ovat tärkeitä. Tutkimuksen tavoitteiden kanssa yhdensuuntaiset ja johdonmukaiset oletukset luovat vahvan perustan tutkimuksen tieteenfilosofialle. Se puolestaan ohjaa metodologian, tutkimusmenetelmien ja empiriaosuuden osalta tehtäviä valintoja tutkimuksen edetessä. Tutkimusprosessia selkeyttämään suunniteltu ”tutkimussipulin” (research onion) uloin kerros muodostuu juuri tutkimusfilosofiasta, eli siitä näkökulmasta voidaan tutkimusfilosofian ajatella olevan koko tutkimuksen perusta. (Saunders ym., 2019, 130–131.)

Eri tieteenfilosofisia suuntauksia on useita, joista tunnetuimpia esimerkkejä ovat positivismi, interpretivismi, realismi ja pragmatismi. Positivismi keskittyy ajatukseen todellisuudesta objektiivisena totuutena, jota voidaan tutkia systemaattisesti. Positivistiseen tutkimukseen soveltuu erityisen hyvin kvantitatiivinen eli määrällinen tutkimus, jolloin tutkija toimii ulkopuolisena tarkkailijana. Positivismia edustavalle tutkimukselle tyypillinen tavoite on kehittää yleispätevä tieteellinen selitys jollekin ilmiölle. Interpretivismi puolestaan painottaa ihmisten subjektiivista kokemusta todellisuudesta. Tässä suuntauksessa pyritään ymmärtämään eri tulkintoja ja näkökulmia etenkin tutkittavien tahojen näkökulmasta. Kriittinen realismi korostaa todellisuuden realiteetteja riippumatta siitä, miten kukin sitä kokee. Se pyrkii syventymään ilmiön syvempiin ja piilossa oleviin rakenteisiin, ja selittämään sitä niiden kautta. Pragmatismi keskittyy nimensä mukaisesti käytännöllisyyteen arvottaen tieteellisiä tuloksia niiden käytettävyyden kautta. Pragmaattisessa lähestymistavassa tutkimusmenetelmät voidaan valita suhteellisen vapaastikin sen pohjalta, että ne palvelisivat mahdollisimman hyvin tutkimuksen tavoitteita. (Saunders ym., 2019, 144–145.)

Tätä tutkielmaa lähestytään etenkin interpretivistisen suuntauksen kautta. Vaikka tutkimuksen kannalta monet asiat ovatkin objektiivisia totuuksia, korostuu silti tutkimusmenetelmien käytössä tulkinnat ja niiden merkitys. Interpretivismin avulla voidaan tutkia ja tulkita sitä, miten vakuuttajat ja toisaalta pk-yritykset ymmärtävät kontrollivaatimusten merkityksen. Myös interpretivismille tyypillinen ajatus tiedon olevan muuttuvaa ja dynaamista sekä suhteellisen pieni analysoitava empiirinen aineistokoko sopivat tähän tutkimukseen hyvin. Toisaalta tutkimus sisältää myös elementtejä pragmatismista. Käytännönläheisyys, todellisten ongelmien tunnistaminen sekä käytännön toimenpidesuosituksen viittaavat interpretivismin lisäksi pragmatismiin suuntaukseen.

Laadullisesta tutkimuksesta käytetään myös termiä ”ymmärtävä tutkimus”, mikä kertoo hyvin sen luonteen; sen tarkoitus on lisätä lukijan ymmärrystä tutkittavasta aiheesta (Tuomi & Sarajärvi, 2018, 28). Valitun tutkimusmenetelmien sekä tutkimuksen lähdeaineiston taustalla on valitut tutkimuskysymykset sekä tutkielman teoreettinen viitekehys. Hirsjärven ym. mukaan laadullinen tutkimus tähtää laajentamaan ymmärrystä tutkittavasta ilmiöstä, joten siksi se soveltuu hyvin tähän tutkielmaan (2009, 161). Kyberriskit, niiden strateginen hallitseminen vakuuttamisen näkökulmasta on tieteellisesti tarkasteltuna suhteellisen uusi ja kompleksinen kokonaisuus, jonka käsittelyyn kvalitatiivinen tutkimus soveltuu mainiosti (Hirsjärvi ym., 2009, 163).

1.5 Tutkimusmenetelmät

Tieteelliset tutkimukset voidaan jakaa tutkimuksen tarkoituksen perusteella neljään kategoriaan: kartoittavaan, kuvailevaan, selittävään ja ennustavaan tutkimukseen. Aiheen uutuuden ja vähäisen aiemman tutkimusaineiston vuoksi tämä tutkielma on selkeimmin kartoittava tutkimus, eli sen tarkoitus on yleisellä tasolla kuvata tutkittavaa ilmiötä, tarkastella sen erityispiirteitä ja etsiä mahdollisesti uusia näkökulmia ja mahdollisuuksia aiheeseen liittyen (Hirsjärvi ym., 2009). Kartoittavassa tutkimuksessa oleellista on tehdä laaja selvitys olemassa olevasta kirjallisuudesta teemaan liittyen, jotta sen pohjalta kyetään taustoittavassa ja empiriaa pohjustavassa teoriaosuudessa kuvata tutkittava ilmiö riittävän hyvin. Tämän päälle voidaan rakentaa kerättyyn aineistoon perustuva empiriaosuus.

Myöskin empiriaosuudessa voidaan aineistoa kerätä neljällä eri tavalla: dokumenteilla, havainnoilla, kyselyillä ja haastatteluilla. Haastattelu on soveltuvin silloin, kun tutkimusaihe on tuntematon, vastaukset vaihtelevat ja tavoitteena on syventää ymmärrystä eli kartoittaa tilannetta (Hirsjärvi & Hurme, 2022). Haastattelut ovat joustava aineistonkeruumenetelmä, jossa haastattelussa itsessään

voidaan syventyä tiettyyn suuntaan riippuen haastateltavan vastauksista. Tämän takia asiantuntijoiden haastattelu soveltuu hyvin tutkimuskysymyksiin aineistoa kerätessä. Tutkimushaastattelut voidaan jakaa kolmeen eri lajiin: strukturoituun (lomakehaastattelu), puolistrukturoituun (teemahaastattelu) ja strukturoimattomaan haastatteluun (avoin haastattelu). Peruseriaate on se, että mitä vähemmän strukturoidumpi haastattelu on, sitä vähemmän käsittely on yhdenmukaista niille (Hirsjärvi & Hurme, 2022). Lomakehaastattelu on yleisin haastattelumuoto, ja se soveltuu parhaiten silloin, kun tiedetään täsmälleen, keneltä kysytään ja mitä halutaan kysyä ja että tarvittava tieto saadaan strukturoidulla haastattelulla. Kvalitatiiviseen tutkimukseen soveltuvat paremmin avoin ja teemahaastattelu, jotka jättävät tilaa vapaammalle ja alkuperäisestä rungosta poikkeavalle keskustelulle haastattelutilanteessa.

Puolistrukturoitu teemahaastattelu perustuu kaikille haastateltaville annettaviin samoihin kysymyksiin, mutta vastausvaihtoehdot ei ole, vaan haastateltavat saavat täysin itsenäisesti vastata. Tällöin verrattuna strukturoituun haastatteluun ei ole vaaraa, että jotain kriittistä tietoa tutkimuksen kannalta jäisi keräämättä. Teemahaastattelussa kysymysten järjestystä on myös mahdollista muuttaa, mikäli se on laadukkaamman keskustelun kannalta järkevää (Hirsjärvi & Hurme, 2022). Teemahaastattelussa, etenkin näin laajassa aihealueessa kuin kybervakuuttamisessa, on oleellista se, että käsiteltävät teemat ovat jäsenneily selkeästi etukäteen. Tällöin myös haastateltava ymmärtävät mihin ilmiöön tutkimuksella pyritään saamaan ymmärrystä ja vastauksia. Tämän takia laadukas esitietojen välittäminen ja tutkimusaiheen läpikäyminen ennen haastattelua on oleellista. Teemahaastattelun yksi suurimmista vahvuuksista on sen joustavuus; vastausten perusteella voidaan tarkentaa ja mahdollisesti syventyä tiettyyn yksityiskohtaan (Tuomi & Sarajärvi, 2018, 75).

Haastateltaviksi tähän tutkimukseen haluttiin vähintään kuusi alan asiantuntijaa, joilla olisi riittävä osaaminen ja ymmärrys aiheesta, jotta vastaukset olisivat riittävän laadukkaita. Laadullisessa tutkimuksessa riittävää haastateltavien määrää on vaikea tietää etukäteen, mikäli sovelletaan niin sanottua saturaation periaatetta. Tällä tarkoitetaan sitä pistettä, jolloin uudet haastattelut eivät tuota enää merkittävää lisähyötyä tutkimuksen lopputuloksen kannalta, vaan vastaukset noudattelevat samansuuntaista kaavaa. Toisin sanoen vastauksista käy ilmi se peruskuvio, joka tutkimusasetelmasta on mahdollista saada (Tuomi & Sarajärvi, 2018, 87). Koska sopivaa tarkkaa määrää haastateltavien määrästä on vaikea tietää ennakolta, lähdettiin aluksi tavoittelemaan 6-8 haastateltavaa, jota voidaan pitää myös opinnäytteelle soveltuvana määränä (Tuomi & Sarajärvi, 2018, 85).

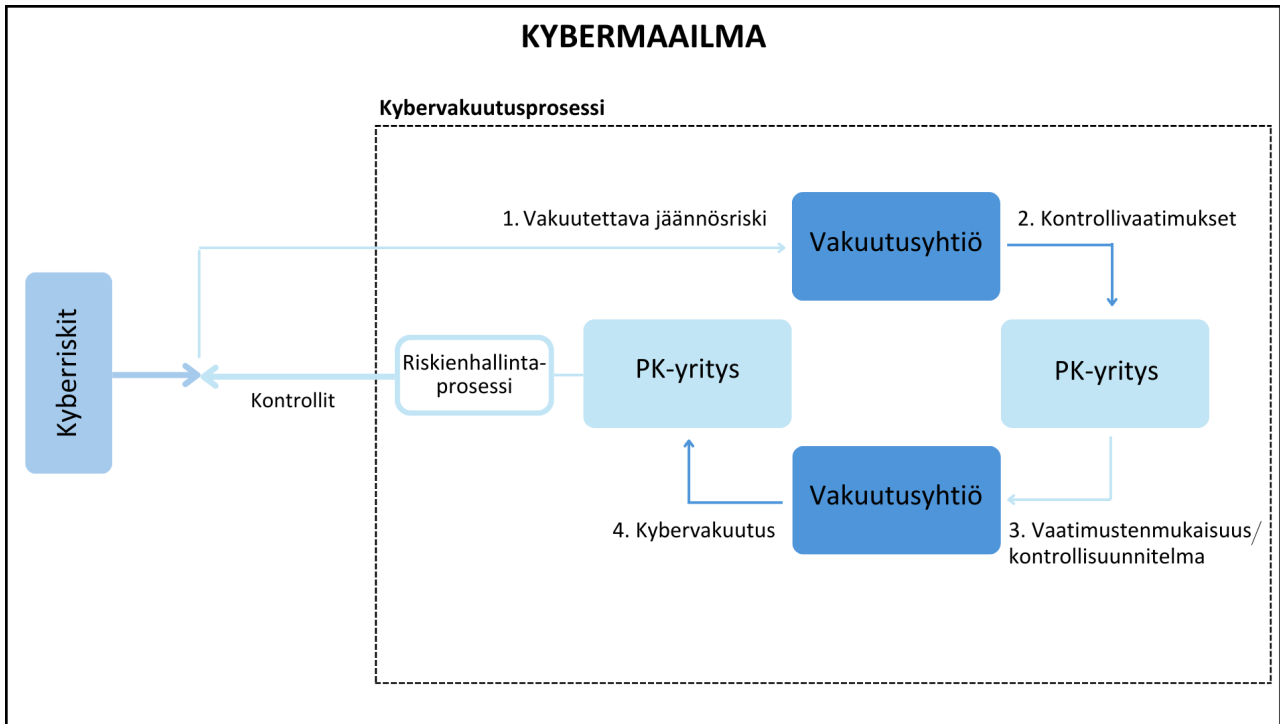
Aineiston keräämisen lisäksi toinen tärkeä metodologinen valinta on analyysimuodon valinta.

Laadullisen tutkimuksen aineiston analysointikeinoja on useita, joista tyypillisimpiä ovat laadullinen sisällönanalyysi, teemoittelu ja tyypittely (Eskola & Suoranta, 2014). Tässä tutkielmassa päädyttiin käyttämään analyysin lähtökohtana laadullista sisällönanalyysia, tarkemmin teoriasidonnaista analyysia. Se pitää sisällään abduktiivista päättelyä, mikä tarkoittaa sitä, että analyysille haetaan vahvistusta sekä teoriasta että aineistosta tehdyistä havainnoista. Tällöin aineistolähtöiset ja teorialähtöiset mallit käyvät dialogia ja vuorottelevat analyysiprosessissa, eli sitä voidaan pitää teorialähtöisen deduktiivisen päättelyn ja aineistolähtöisen induktiivisen päättelyn hybridiversiona (Tuomi & Sarajärvi, 2018, 83). Joustavuuden ja monipuolisuuden takia abduktiivinen päättely sopii hyvin tämän tutkielman aineiston sisällönanalyysin menetelmäksi. Tasapaino on kuitenkin hieman kallellaan deduktiivisen eli teoriapainotteisen analyysin suuntaan, sillä tutkimuksen lähtökohtana on nojaaminen teoriaosuuteen ja sen luomaan viitekehykseen, vaikka induktiivinen päättely onkin oleellista laadullisessa tutkimuksessa (Eskola ja Suoranta, 2014, 83).

Sisällönanalyysi auttaa teoreettisen viitekehyksen ja empiria-aineiston yhdistämisessä (Hirsjärvi ym., 2009). Valintaa teoriasidonnaiseen sisällönanalyysiin tukee myös tutkimuksen tavoite kartoittaa nykytila kybervakuutusten kontrollivaatimuksien osalta ja parantaa ymmärrystä niiden merkityksestä pk-sektorin yrityksille. Tuomen ja Sarajärven mukaan sisällönanalyysi mahdollistaa aineiston läpikäynnin niin, että erityiset merkitykset nousevat esiin joiden avulla ilmiötä voidaan myös selittää paremmin (2018). Analyysivaihe on tutkimuksen onnistumisen kannalta kriittinen vaihe, sillä sen pohjalta vastaukset esitettiin tutkimuskysymyksiin tehdään. Analyysivaihe myös vaikuttaa vahvasti tutkimuksen luotettavuuteen ja merkitykseen.

1.6 Teoreettinen viitekehys ja tutkielman rakenne

Kvalitatiiviselle tutkielmalle tyypillisesti tutkielmaa pohjustetaan aluksi taustateorialla, johon tutkimustuloksia voidaan peilata ja analysoida yhtäläisyyksiä ja eroja. Taustateoriassa käsitellään ensiksi sekä kyberriskin käsitettä ja yleist teoriaa, sekä kybervakuuttamisen käsitteitä ja sen yleist teoriaa. Tämä siksi, että ne antavat perustason ymmärryksen ja luovat hyvän pohjan syventyä kyberriskien vakuuttamisen tärkeään yksityiskohtaan; kontrollivaatimukseen. Etenkin abduktiivista päättelyä käytettäessä myöhemmin analyysivaiheessa korostuu tulkintateorian merkitys ja sen antamat suuntaviivat tutkimuskysymyksiin. Teorioiden välistä suhdetta käsiteltävään aiheeseen kuvaa alla oleva teoreettinen viitekehys (kuvio 1). Viitekehys rakentuu tutkimuksen keskeisten käsitteiden ympärille, ja se luo pohjan tutkielman teoriaosuudelle ja sen myöhemmälle tulkinnalle.



Kuvio 1. Tutkielman teoreettinen viitekehys

Viitekehysten toimijoina ovat pk-yritys ja kybervakuutusta tarjoava vakuutusyhtiö. Kuvion kehikko, kybermaailma, toimii kontekstina, jossa toimiminen muodostaa yritykselle jatkuvasti kehittyviä kyberriskejä. Omassa riskienhallintaprosessissaan yritys analysoi kohtaamiaan riskejä ja asettaa sekä toteuttaa hyväksi näkemänsä kontrollit hallitakseen kyberriskejä riittävällä tasolla. Halutessaan yritys voi myös kontrollien lisäksi vakuuttaa jäännösriskiä. Tämä on usein perusteltua, sillä kyberriskejä ei voi ikinä hallita täydellisesti (Strupczewski, 2021). Vakuutusyhtiön tarkastellessa sille tarjottua riskiä, se lähtökohtaisesti esittää yritykselle tiettyjä kontrollivaatimuksia, jotka yrityksen tulee tai olisi hyvä täyttää vakuuttamista ajatellen. Yritys voi omassa vastauksessaan todeta kontrollien olevan paikallaan tai laatia suunnitelman niiden täytäntöönpanemiseksi. Yritys voi myös kieltäytyä kontrollivaatimuksista, jolloin vakuuttajan vastuulle jää valinta siitä, aikooko se myöntää vakuutuksen siitä huolimatta ja mikäli kyllä, millä ehdoilla se sen tekee. Tutkielman viitekehys pyrkii kiteyttämään ja luomaan johdonmukaisen yhteenvedon käytettävistä keskeisistä käsitteistä, niiden merkityksestä ja niiden välisistä suhteista.

Yksinkertaistettuna voidaan siis sanoa, että kybervakuutusprosessi lähtee liikkeelle siitä, että omat kyberriskikontrollit ovat kunnossa, sen jälkeen jäännösriskiä voidaan hallita vakuuttamalla. Riskin siirto, joka käytännössä pk-yritysten osalta tarkoittaa melkein aina vakuuttamista, on tutkimusten valossa tehokkain tapa hallita jäännösriskiä (Marotta ym., 2017). Kybervakuutus ja organisaation

omat riskikontrollit eivät siis missään nimessä ole vaihtoehtoisia riskienhallinnan menetelmiä, vaan ne täydentävät toisiaan kokonaisvaltaisessa kyberriskien hallinnassa. Kontrollivaatimuksilla voidaan kuitenkin ajatella olevan vahva työntävä vaikutus yrityksille panostaa omaan kyberturvallisuuteen. Kontrollivaatimuksia voi jossain mielessä verrata perinteisten vakuutusten suojeluohjeisiin, eli esimerkkinä jokaiselle tuttu suojeluohje napsauttaa pesukoneen hana pois päältä, kun konetta ei käytetä.

Tutkielma koostuu viidestä pääluvusta; johdannosta, kahdesta teoriakappaleesta, empirialuvusta sekä yhteenvetoluvusta. Ensimmäisenä on johdantokappale, jossa esitellään tutkielman teema, tavoitteet, tutkimuskysymykset ja tutkimuksen toteutustapa. Jokainen pääluku on jaettu useampaan alalukuun. Johdannossa käydään läpi myös tutkimuksen tieteenfilosofiset lähtökohdat ja aineiston keruu- ja analysointitapa. Johdannon tarkoituksena on esitellä lukijalle aihe, sen tausta sekä merkitys tieteellisesti, toisin sanoen se asettaa raamit tutkielmalle. Johdantokappaleen tarkoitus on myös perehdyttää lukija aiheeseen ja aikaisempiin saman teeman tutkimuksiin (Hirsjärvi ym., 2009).

Teoriaosuus on jaettu kahteen; taustateoriaan ja tulkintateoriaan. Teorioiden rakennetta voidaan hahmottaa myös teoreettisen viitekehyksen pohjalta (kuvio 1), josta voidaan nähdä, että käytännössä kaikki muut viitekehyksen käsitteet käsitellään taustateoriassa eli ne taustoittavat käsiteltävää pääteemaa – kontrollivaatimuksia, johon pureudutaan tulkintateoriassa tarkemmin. Taustateorialla tuetaan myös tutkimuskysymysten valintaa ja tutkimuksen rajausta (Hirsjärvi ym., 2009). Taustateoria käsittelee pk-yritysten kohtaamia kyberriskejä ja niiden vakuuttamista yleisesti ilmiönä. Taustateorian tarkoitus on tuoda esille tutkielman kannalta relevantit käsitteet ja faktat. Se luo perustan, jonka varaan tutkimuksen muut osuudet rakentuvat.

Tulkintateoria paneutuu tarkemmin kontrollivaatimukseen, niiden ominaispiirteisiin ja merkitykseen sekä vakuuttajien että asiakasyritysten kannalta. Tulkintateorian tarkoitus on ohjata tutkijan valintoja etsiessään vastauksia tutkimuskysymyksiin aineiston perusteella (Eskola & Suoranta, 2014, 82). Tulkintateoria luo tässä tutkielmassa sen näkökulman, josta aihetta tarkastellaan. On oleellista, että kontrollivaatimukset määritellään alussa riittävän tarkasti; selkeä käsitys niistä auttaa tutkimuksen empiriavaiheessa tekemään oleellisia huomioita tutkimuskysymysten kannalta. Tulkintateoria pyrkii antamaan riittävän laajan perusymmärryksen kaikkiin kolmeen tutkimuskysymykseen, joiden varaan empiriaosuuden tulkintaa voidaan peilata ja analysoida. Tulkintateorian todellinen arvo tulee esiin empirian ja teorian dialogissa tehdessä analyysia.

Tutkielman sinetöi lopussa yhteenveto, jossa esitellään keskeisimmät tehdyt havainnot ja analysoidut päätelmät sekä vastataan tutkimuskysymyksiin eli kirjataan tutkimustulokset. Yhteenvedossa myös arvioidaan tutkimusta retrospektiivisesti kokonaisuudessaan sekä listataan mahdollisia jatkotutkimusehdotuksia. Ehdotusten lisäksi yhteenvedossa on hyvä asettaa tutkimus kontekstiin, eli miten se asemoituu muihin tutkimustuloksiin nähden. Arviointi on tärkeä osa tieteellistä tutkimusta, jossa arvioidaan tutkimuksen validiteettia eli pätevyyttä ja reliabiliteettia eli luotettavuutta. Yhteenvedon tarkoitus on tiivistää tutkimuksen keskeiset tulokset ja johtopäätökset eli kuinka tutkimuskysymyksiin onnistuttiin lopulta vastaamaan.

2 KYBERRISKI JA SEN VAKUUTTAMINEN

2.1 Kybermaailma

Kybermaailma saattaa kuulostaa salamyhkäiseltä ja jopa tieteiselokuvamaiselta, mutta tosiasia on, että se koskettaa meistä jokaista nykypäivänä Suomessa. Vaihtoehtoisia termejä kybermaailmalle voisivat olla kyberavaruus tai hieman maanläheisemmin kybertoimintaympäristö. Yhtä kaikki, sillä tarkoitetaan ympäristöä, joka muodostuu toisiinsa yhteydessä olevista digitaalisista tietojärjestelmistä (Limnell ym., 2014). Kyse on tuoreesta ja voimakkaasti kasvavasta maailmasta, joka tietysti haastaa sen riskienhallintaa. Vaikkakin perinteinen fyysinen maailma on ensisijainen liiketoiminnan toimintaympäristö, ei Suomessa voi nykypäivänä välttyä kyberpuolesta – niin tiiviisti ne ovat kietoutuneet toisiinsa. Digitalisaation tarkoitus on luonnollisesti palvella niin yksilöiden kuin yritystenkin tarpeita ja auttaa saavuttamaan tehokkaammin tavoitteitaan, arkisissa asioissa kuten pankkisiirroissa tai läheisten kanssa kuulumisten vaihtamisessa, kuten myös haastavammissa tehtävissä kuten avaruuslennoissa tai vakuutusteknisen vastuuvelan laskemisessa. Yritykset ovat paljon vartijoina kybermaailmassa, sillä valtaosa digitaalisista palveluista ja niiden kyberriskien hallinnasta toteutetaan Suomessa yrityskentän toimesta (Lehto, 2024).

Kybermaailma on auttanut yrityksiä ottamaan valtavia kehitysloikkia viimeisten vuosikymmenten aikana, etenkin Suomessa. Suomessa on panostettu tällä vuosituhanella merkittävästi digitalisaatioon, josta osoituksena on esimerkiksi viime vuotuinen kansainvälinen ”digimestaruus”. Yritysten osalta digitalisaation hyödyntämisessä Suomi sijoittui toiseksi länsinaapurin jälkeen (Ala-Yrkkö ym., 2023). Kuten viimeiset pari vuosikymmentä liki olematonta talouskasvua todistaa, ei vahva digiosaaminen yksinään varmista yritysten menestystä tai talouskasvua. Toisaalta on myös hyvä muistaa yhdysvaltalaisen tutkijan Roy Amaran laki: ”Teknologian vaikutus yliarvioidaan lyhyellä ja aliarvioidaan pitkällä tähtäimellä” (Ratcliffe, 2016). Vaikka digiloikan elinkaari on vielä pahasti kesken, digitalisaation tarjoama tuottavuusapu on kiistaton. Esimerkiksi rahoitus- ja vakuutustoiminnassa tuottavuus on pelkästään vuosikymmenessä kasvanut 35 prosenttia (ETLA, 2021).

Kuten kaikella, myös kyberympäristöllä on kääntöpuolensa. Yritykset joutuvat investoimaan suuria resursseja päästäkseen hyödyntämään digimaailman etuja ja pysyäkseen mukana kehityksen kelkassa, ilman takuita niistä saatavista tuotoista. Puhutaan siis riskinottamisesta. Riski on kaiken liiketoiminnan ytimessä, eikä kyberympäristössä toimiminen tee tähän poikkeusta. Riski voidaan

määritellä lukemattomilla eri tavoilla myös tieteellisesti, mutta yksi tapa on yleisesti ajatella sitä yksinkertaisesti seikaksi, mikä vaikuttaa yrityksen tavoitteiden saavuttamiseen (Hopkin, 2018, 16). Vaikka liiketoimintaan kuuluukin perusajatus positiivisista riskeistä ja niiden tuomasta mahdollisuudesta tuottoihin, sovelletaan selvyuden nimissä tässä tutkielmassa riskin käsitteeseen sen yleiskielellistä merkitystä eli vaaraa tai uhkaa siitä, että tarkasteltavalle organisaatiolle tapahtuu jotakin epäedullista (Juvonen, ym., 2014, 8). Kyberympäristön osalta positiivisia riskejä voisivat olla esimerkiksi onnistunut uusi ohjelmistopäivitys tai digi-innovaatio, mutta kuten todettua ne eivät ole tämän tutkielman osalta relevantteja. Digitalisaation ja kyberympäristöön liittyvät riskit ovat juuri pk-yrityksille erityisen suuri haaste, sillä niillä usein käytettävät resurssit ovat pienempiä, mutta riskit voivat olla kuitenkin hyvin samankaltaisia kuin isoilla yrityksillä. Yksi syy miksi pk-yritykset panttaavat investointeja on juuri kyberriskit ja valmistautumattomuus niihin (Sommer 2015, 1528). Siksi kyberriskien hallinta olisi erityisen tärkeää juuri pk-sektorille.

2.2. Kyberriskit

Fyysisen maailman rinnalle luotu kybermaailma siis luo valtavan määrän uusia riskejä, joita kutsutaan loogisesti kyberriskeiksi. Kyberriskille ei ole osittain sen uutuuden ja osittain monimutkaisuuden takia selkeää universaalia määritelmää käytössä. Yksi käytetty määritelmä on: *kyberriskillä tarkoitetaan taloudellisen menetyksen, maineen vahingoittumisen tai muun vahingon riskiä, joka liittyy informaatioteknologiaan* (Institute of Risk Management 2014, 10). Laveampi esimerkki: *Kyberriski sisältää kolme eri ominaisuutta: digitaalinen vahinko digitaaliselle omaisuudelle, digitaalinen vahinko fyysiselle omaisuudelle tai fyysinen vahinko digitaaliselle omaisuudelle* (Böhme ym., 2019). Tai kokoavampi: *Kyberriski on operatiivinen riski, joka liittyy kybermaailmassa tapahtuvaan toimintaan, joka uhkaa tieto- ja viestintätekniillisiä resursseja ja joka voi aiheuttaa aineellista vahinkoa, liiketoiminnan keskeytymistä tai maineellista haittaa organisaatiolle* (Strupczewski, 2021). Vaikka eri määritelmät ovat osittain erilaisia, yhteinen nimittäjä on kuitenkin se, että riski aiheutuu kyberympäristöstä ja vaikuttaa negatiivisesti organisaatioon aineellisesti tai aineettomasti. Tässä tutkielmassa kyberriski-termillä tarkoitetaan sellaista uhkaa, joka voi aiheuttaa yritykselle taloudellista tappiota, liiketoiminnan keskeytyksen, mainehaittaa tai oikeudellista vastuuta.

Oleellista on myös muistaa, ettei kyberriskejä yhdistetä ainoastaan kyberrikollisuuteen tai kybersodankäyntiin, sillä esimerkiksi tietovuodoista noin puolet aiheutuu tietotekniikan teknillisistä virheistä tai työntekijöiden inhimillisistä virheistä (IBM, 2024). Moni yritys onkin havahtunut siihen,

että osaamaton tai varomaton henkilöstö voi olla organisaation merkittävin kyberriski. Tämä korostuu etenkin pienemmissä yrityksissä sekä Suomessa, missä kyberturvallisuus on muuten hyvällä tasolla, eikä rikollisuus ole yhtä merkittävä uhka kuin muissa maissa. On kuitenkin hyvä muistaa, että Suomen ollessa kärkimaita kansallisen kyberturvallisuuden osalta, on kyberrikollisuuden määrä ja laatu kasvanut viime vuosina selvästi (Traficom, 2024). Yrityksen pienempi koko ei myöskään yksin suojaa rikollisilta, sillä kuten mainittua haittaohjelmien heijastevaikutukset voivat vaikuttaa kaikenlaisiin organisaatioihin. Pienemmissä yrityksissä kyberturvan taso on alhaisempi, jolloin se tekee siitä helpomman ja sitä kautta houkuttelevamman kohteen. Lisäksi kyberrikolliset eivät usein spesifioi kohdettaan, vaan skannaavat internetiä ja haavoittuvuuden löytyessä iskevät siihen. Ongelma on, etteivät pk-yritykset itse koe tutkimusten valossa olevansa houkutteleva kohde tilastoista huolimatta (Alahmari & Duncan, 2020).

Kyberturvallisuuden voidaan ajatella olevan yrityksen tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa liiketoiminnan jatkuvuus voidaan turvata. Lisäksi siihen lasketaan kuuluvan yritysten toteuttamat toimenpiteet, joilla erilaisia kyberuhkia ja niiden vaikutuksia voidaan ennakoivasti hallita ja tarvittaessa sietää (Turvallisuuskomitea 2018, 25). Tämä tavoitetila saatetaan ottaa helposti yrityksessä automaationa ja perustilana otettavana oletuksena, vaikka sen eteen täytyy nähdä vaivaa, kouluttautua jatkuvasti ja allokoida resursseja. On myös hyvä muistaa, mitä kaikkea kyberturvallisuus pitää nykyään sisällään. Se ei ole pelkästään tekniikkaa ja teknologiaa, vaan siihen liittyy myös sosiaalisia ja organisatorisia aspekteja. Kyberturvallisuus laajentuu digitaalisen omaisuuden lisäksi kattamaan myös muun kybermaailmaan liittyvän informaatioteknologian, sen käyttäjät ja muun kuin tietoon liittyvän omaisuuden (von Solms & van Niekerk, 2013).

Kyberriskien luonteeseen siis kuuluu, että ne muodostuvat kyberympäristöstä käsin, mutta voivat aiheuttaa sekä henkilövahinkoja että aineellisia ja aineettomia vahinkoja digitaalisen toimintaympäristön lisäksi. Lisäksi ne ovat vaikeammin tunnistettavissa kuin perinteisemmät riskit, jatkuvan muutoksen ja riskin verkostoituneisuuden vuoksi. Riskit eivät myöskään rajoitu vain tietyille maantieteelliselle alueelle ja suurten kyberhyökkäysten kuten vuoden 2017 NotPetyan heijastevaikutukset varsinaisen iskukohteen ulkopuolelle voivat aiheuttaa satojen miljoonien eurojen vahinkoja esimerkiksi liiketoiminnan keskeytymisenä (Neary, Steinberg & Stepan, 2021). Muita kyberriskien erityispiirteitä ovat niiden vaikea ennustaminen esimerkiksi verrattuna luonnonkatastrofeihin jatkuvan muutoksen takia ja toisaalta yritysten riippuvuus tietyistä suurista teknologiafirmoista kuten GAF A-yhtiöistä tai muista Big Tech-yrityksistä (Eling & Schnell, 2016). Esimerkki tällaisesta tapauksesta tapahtui tänä kesänä, kun tietoturvaohjelmiston päivitys aiheutti

laajoja häiriöitä Microsoft-käyttäjärjestelmään ja sen myötä lukuisiin yrityksiin (Kyberturvallisuuskeskus, 2024).

Riskejä on käytännössä loputtomasti erilaisia, ja helpottamaan niiden hallintaa ne tyypillisesti luokitellaan eri tasoisiin kategorioihin. Riskien luokittelu helpottaa niiden analysoimista ja hallintaa. Yksi hyvin yleinen tapa yritysmaailmassa on luokitella liiketoiminnan riskit neljään pääkategoriaan: strategisiin riskeihin, taloudellisiin riskeihin, operatiivisiin riskeihin ja vahinkoriskeihin. Operatiiviset riskit liittyvät yritystoiminnan henkilöstöön, päivittäisiin prosesseihin tai järjestelmiin. Operatiivisiin riskeihin sisältyy uhka mainehaitasta, mikä on oleellinen kyberuhkista puhuttaessa. (Ilmonen, ym. 2022, 79). Kyberriskit voidaan kokonaisuudessaan sisällyttää siis pääsääntöisesti tähän luokkaan. Tarkemmin kyberriskit voidaan vielä jakaa niiden syntyperän mukaan, sisällyttäen myös inhimilliset tekijät yhdeksi. Tällainen jako voi olla esimerkiksi: 1) Ihmisten toiminta, 2) järjestelmä- ja teknologiahäiriöt, 3) Organisaation sisäisen prosessin epäonnistuminen ja 4) ulkoiset tapahtumat (Biener ym. 2015).

Vaikka ensimmäisenä saattaa tulla kyberriskeistä puhuttaessa mieleen rikollisjärjestöt ja niiden masinoimat kyberrikokset, niin pk-yrityksistä puhuttaessa suurin uhka on kuitenkin listan ensimmäisenä eli ihmisten toiminta ja inhimilliset riskit (Alahmari & Duncan, 2020). Toki tässä on hyvä muistaa, että usein työntekijöiden tai kolmannen osapuolen virheen seurauksena aiheutuvat kybervahingot sisältävät myös kyberrikollisuutta, tästä esimerkkinä vaikkapa kalasteluviestit tai muu sosiaalisesta manipuloinnista aiheutuva uhka. Huomionarvoista on siis käsitteiden päällekkäisyys, mutta selvää on joka tapauksessa yrityksen henkilöstön rooli kyberturvallisuuden toteuttajana. Tämä korostuu pk-yrityksissä, joissa tietoturvaohjelmat ja -prosessit eivät välttämättä ole kypsyytasoltaan parhaalla mahdollisella tasolla (Toivonen, 2017).

2.3 Kyberriskien hallinta

Kuten edellisessä kappaleessa todettiin, kybermaailmaan liittyy sellaisia erityispiirteitä, joita ei samalla tavalla muista riskilajeista löydy, ja jotka tekevät niiden hallinnasta erityisen haasteellista. Tällaisia piirteitä ovat esimerkiksi riskeistä aiheutuvien vahinkojen kumuloituminen, yleinen puute historiatiedosta ja epäsymmetrinen tieto (Eling, 2020). Näistä syistä kyberriskien realisoituessa kustannukset voivat nousta erittäin suureksi ja muun muassa siksi kyberriskit on arvioitu usein merkittävimmäksi yksittäiseksi riskilajiksi yrityksille. Vaikka kyberuhat tapahtuvat kybermaailmassa, ovat ne pääsääntöisesti ihmisten välisiä konflikteja, joissa voi välissä toki olla

esimerkiksi botteja välineellistetty. Ihmisten välisten konfliktien ennustaminen menneiden tapahtumien perusteella on hyvin vaikeaa, jota voi verrata terrorismin tai sodan todennäköisyyksien ja vahinkojen arviointiin (Coburn, 2019). Alalla paljon käytetyn saksalaisen vakuuttajan Allianz riskibarometrin mukaan kyberriskit ovat nousseet viimeisen kymmenen vuoden aikana sijalta kahdeksan sijalle yksi, johon se on selvällä erolla viime vuodet listattu (Allianz 2014 & 2024). Tämä kertoo selvästi sen, kuinka nopeasta muutoksesta on kyse.

Kyberriskeissä yhdistyy siis yrityksen kannalta kaksi haastavaa elementtiä: kybervahinkojen aiheuttamat korkeat kustannukset sekä niiden haasteellinen hallinta. Korkeista kustannuksista kertoo tutkimustulos, jonka mukaan joka viides pk-yritys, jota on kohdannut kybervahinko, on ollut joko hyvin lähellä maksujärjestelyä tai joutunut konkurssiin (Hiscox, 2022). Tämä on yksi syistä, miksi kyberriskien hallinta on niin tärkeää myös pk-yrityksille. Haaste monille yritysten johtajille on ajatus siitä, että turvallisuusinvestoinnit eivät tue kasvua vaan päinvastoin hidastavat sitä. Tutkimuksen mukaan vain reilu kymmenys pk-yritysten johtajista ajattelee, että he ovat saaneet kyberturvainvestoinneista halutun lisäarvon (Chaput, 2024). Syitä tähän taustalla voi olla monia. Tosiasia on kuitenkin se, että parhaimmillaan hyvä hygieniataso kybermaailmassa voi olla muun muassa kilpailuetua tuova, luottamuksen rakentaja ja tietysti riskienhallitsija; yrityksen kannattaa lähtökohtaisesti välttää pitämästä itsellään yllättäviä suuria riskejä. Oleellista on nähdä puhtaan kulun sijasta kyberturvassa investointi (von Solms & van Niekerk, 2013).

Voisi kuvitella, että Suomi olisi syrjäisenä maana ja harvinaisena kielenä kybermaailman lintukoto, mutta ihan näin ei asia ole. Kybermaailman globaali luonne ja esimerkiksi tekoälykääntäjät ovat mahdollistaneet hyökkäykset myös kaukaisemmista maista Suomeen. Toisaalta myös yhteiskunnan pitkälle edennyt digitalisaatio mahdollistaa laajan kirjon riskejä. Kyberhyökkäysten vuosittaiset kustannukset mitataan Suomessakin miljardeissa (Sjövall, 2018). Laajuudesta pienempienkin yhtiöiden osalta kertoo se, että jo reilu viisi vuotta sitten viisi prosenttia suomalaisista pk-yrityksistä altistui kyberhyökkäyksen kohteeksi vuoden aikana (Toivonen, 2017). Yritykset saattavat toki pimittää tietoja itseensä kohdistuneesta hyökkäyksestä, joten tilastoihin on syytä suhtautua pienellä varauksella. Merkittävä hyppäys, niin maailmalla kuin Suomessa, tapahtui koronapandemian puhkeamisen kanssa miltei samanaikaisesti vuosina 2019–2020. Tällöin Suomessa hyökkäysten määrä kaksinkertaistui, ja arvion mukaan taloudellisten kustannusten määrä kasvoi tätäkin nopeammin. Näinä vuosina Suomi sijoittui kyberturvallisuuden liittyvissä ongelmissa selkeästi EU:n keskiarvon yläpuolelle (Ali-Yrkkö ym., 2020).

Suomesta on usein digitalisaation ohella puhuttu kyberturvallisuuden ykkösmaana, joskin kaikki tutkimustulokset eivät ole sitä täysin vahvistaneet. Esimerkiksi vuonna 2020 tehdyn digibarometrin mukaan Suomi on perässä kaikkia muita Pohjoismaita kyberturvallisuudessa ja jäämässä jälkeen muistakin alan kärkimaista. Esimerkiksi tietovuodot ovat suomalaisissa yrityksissä kolme kertaa yleisempiä kuin muissa EU28-maissa (Ali-Yrkkö ym., 2020). Vaikka Suomen digitalisaatio on edistynyt kiistatta maailman kärkivauhtia, ei alan asiantuntijoita, etenkin turvallisuuden osalta, ole saatu selvästi riittävästi. Päätekijänä taustalla vaikuttaa varmasti asenne, joka näkyy myös yritysten kyberriskien hallinnassa. Merkittävimpiä kehityskohteita ovat tilannekuva, turvallinen ohjelmistokehitys ja henkilöstön riittävä osaaminen. Finanssialalle annetaan kuitenkin erityismaininta kyberkypsyudesta (Sibakov, 2020). Osittain tähän on syynä regulaatio, joka pakottaa finanssialan yritykset panostamaan kokonaisvaltaiseen riskienhallintaan ja turvallisuuteen. Toisaalta selvä korrelaatio näkyy myös siinä, onko yritys integroinut kyberturvallisuusstrategian osaksi omaa kokonaisstrategiaa (Digipooli, 2023). Lisäksi kyberturvallisuus vaatii myös taloudellisia investointeja, ja mikäli kyberriskejä ei koeta aidoksi uhaksi, jää riskienhallinta usein puutteelliseksi.

Nimenomaan pk-yritysten kyberriskien hallinnan tasosta ei ole laajoja tutkimuksia vielä tehty, mutta yksi lähestymiskulma on peilata tilannetta isojen eli pörssiyritysten kautta. Tutkimuksen mukaan 112:sta suomalaisesta pörssiyrityksestä 96 raportoi vähintään jollain tasolla vuosiraportoinnin yhteydessä kyberturvallisuudesta (Haavisto, 2024). Luku on suhteellisen hyvä, mutta kääntöpuolena voidaan ajatella, että vuosiraportoinnissa voidaan helposti syyllistyä tilanteen kaunistelemiseen. Lisäksi jos yli kymmenys pörssiyrityksestä ei mainitse sanallakaan kyberturvallisuudesta, mikä tietoisuuden ja tekemisen taso on pienemmän kokoluokan yrityksissä? Suomen kyberkypsyys-selvityksen mukaan tilannekuva on yrityskentällä parantunut viime vuosina, mutta saadun tiedon hyödyntäminen jää vajavaiseksi osaamisen, tekijöiden tai ajanpuutteen vuoksi. Lisäksi käsitys oman organisaation houkuttelevuudesta kyberhyökkäyksen kohteena voi vaikuttaa varautumisen tasoon (Digipooli, 2023). Usein ongelmana on, ettei yrityksen johdon ja tietoturvaan vastaavan ajatukset halutusta riskitasosta (rik appetite) kohtaa (Chaput, 2024).

2.3.1 Kyberriskien eri hallintakeinot

Riskienhallinnan merkitys on yrityksissä viime vuosina korostunut entisestään, pitkälti globaalien kriisien kuten koronapandemian ja Venäjän hyökkäyssodan sekä niiden lieveilmiöistä johtuen kuten rajuista sähkö- ja korkomarkkinamuutoksista. PWC:n tutkimuksen mukaan kohonnut kiinnostus ei ole kuitenkaan konvertoitunut riittävässä määrin konkreettisiin toimenpiteisiin, vaikka

riskienhallinnan ymmärrys on parantunut; henkilö- ja teknologiaresurssit eivät ole kasvaneet vaatimusten mukana samaa vauhtia (PWC, 2023). Osasyynä tähän on varmasti monen yrityksen kohdalla taloudellisesti tiukat ajat. Nollakasvussa lisäresursointia riskienhallintaan on vaikea tehdä, vaikka selkeä tarve olisi. Monen mielestä Venäjä-maariskin toteutuminen hyökkäyssodan myötä ja merkittävien tappioiden aiheutuminen monelle suomalaisyritykselle oli merkki suomalaisesta riskienhallinnan heikkoudesta suhtautua omiin vaikutusmahdollisuuksiin epärealistisesti (Aspara, 2022). Lisäongelmana on myös se, että kyberturvallisuutta pidetään vahvasti ”pakollisena pahana” eikä sen tuomaa lisäarvoa ja kilpailuetua nähdä, johtuen pitkälti tietotaidon ja ymmärryksen puutteesta (Chaput, 2024).

Keino	Esimerkkejä toimenpiteistä
Välttäminen	<ul style="list-style-type: none"> • Haavoittuvuuden poistaminen tai korjaus • Vanhojen laitteiden poisto tai päivitys • Ulkoisten USB-laitteiden kieltäminen
Pienentäminen	<ul style="list-style-type: none"> • Palomuurien ja virustorjunnan vahvistaminen • Henkilöstön kouluttaminen • Varmuuskopioiden ylläpitäminen
Siirtäminen	<ul style="list-style-type: none"> • Luotettavien alihankkijoiden ja palveluntarjoajien käyttö ja vastuun siirtäminen heille. Esim. pilvipalvelut tai kyberturvallisuuskeskus (CSOC)
Vakuuttaminen	<ul style="list-style-type: none"> • Kybervakuutus esimerkiksi yritysvakuutuksen laajenuksena tai itsenäisenä vakuutus sopimuksena
Pitäminen itsellä	<ul style="list-style-type: none"> • Ei erillisiä toimenpiteitä. Tulee kyseeseen, jos riski on hyvin pieni tai kustannukset liian suuria, eikä muita sopivia vaihtoehtoja ole.

Kuvio 2. Perinteiset riskienhallinnan keinot (Mukaillen Juvonen ym., 2014) ja toimenpide-esimerkit kyberturvallisuuden kontekstissa.

Mahdollisuuksia kyberriskien hallintaan on käytännön tasolla monia. Yksi tapa keinojen esittämiseen on nelijako riskin siirtämiseen, pienentämiseen, välttämiseen ja pitämiseen itsellään (Juvonen ym., 2014). Toki jossain tapauksissa vakuuttaminen eriytetään riskin siirtämisestä omaksi keinokseen (kuten kuviossa 2), mikä tässä tutkielmassa on mielekästä kybervakuuttamisen ollessa keskiössä. Ennen sopivien hallintakeinojen valitsemista on tietysti tunnistettava ja arvioitava riskit prosessin mukaisesti (kuvio 3). Oleellista on myös huomata, ettei hallintakeinot ole poissulkevia. Toisin sanoen

käytännössä paras mahdollinen hallintataso saavutetaan yhdistämällä eri keinoja yrityksen koosta riippumatta (Eling & Schnell, 2016).

Kontrollivaatimukset kyberriskeissä painottuvat hallintakeinoista etenkin välttämiseen ja pienentämiseen. Välttäminen poikkeaa keinona perinteisestä riskienhallinnasta siinä, että kybermaailmassa se on mahdollista tehdä ilman, että itse liiketoimintaa muutetaan, vaan esimerkiksi poistamalla ohjelmistosta haavoittuvuus (Eling & Schnell, 2016). Pienentämistä voidaan pitää yleisimpänä keinona ja sen alle menevät suurin osa riskikontrolleista, kuten monivaiheinen tunnistautuminen, varmuuskopiot ja henkilöstön koulutus. Riskin pienentäminen vaatii jatkuvia toimenpiteitä ja kehittymistä organisaatiolta. Pienentämisen haaste on se, että käytännössä kyberriskejä voi mitigoida loputtomasti niin, että jäännösriski on aina olemassa eli puhutaan niin sanotusta optimointiongelmasta. Lisäksi tietyn vaiheen jälkeen lisätyt kyberriskikontrollit eivät enää paranna yrityksen arjen sujuvuutta. Päinvastoin tilannetta voidaan ajatella fyysisen maailman kautta. Jos työpaikalla on jokaisessa huoneessa lukittava ovi ja jokaisessa nurkassa kamera kuvaamassa, kuinka mielekäs työympäristö silloin olisi. Itsellä riskin pitäminen voi joskus kannattaa, etenkin jos riski on hyvin pieni eikä siihen ole tehokkaita kontrolleja saatavilla. Kyberriskien osalta pk-yrityksen kannattaa kuitenkin olla erityisen tarkkana siinä, mitä se pitää itsellään, sillä pieneltäkin tuntuvista riskeistä voi koitua suuria tappioita pahimman skenaario toteutuessa. (Eling & Schnell, 2016)

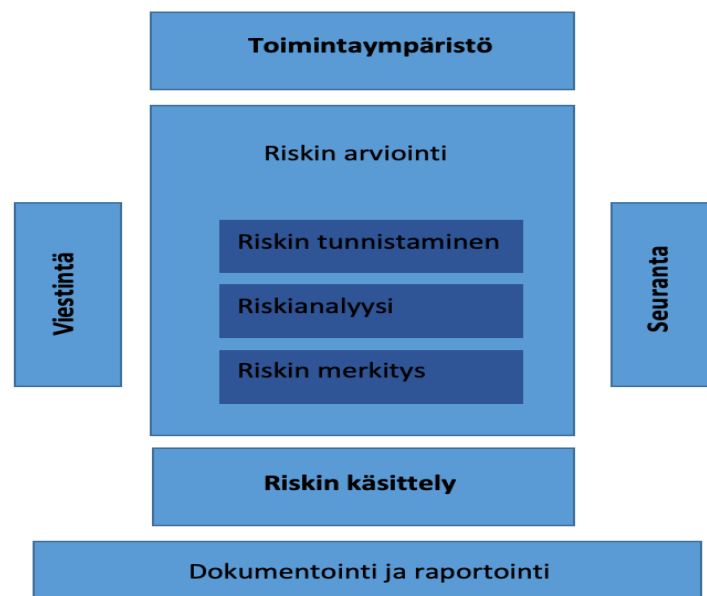
Riskin siirtäminen voi olla pienemmälle yritykselle tehokas tapa ulkoistaa palvelun lisäksi samalla siihen liittyviä kyberriskejä. Tässä on kuitenkin oleellista muistaa, että ulkoistaminen ei poista kuitenkaan kokonaan siihen liittyvä vastuuta yritykseltä (Benaroch & ym., 2020, 318). Kybervakuuttaminen on vielä pk-sektorilla suhteellisen tuntematon keino, etenkin Euroopassa. Pohjois-Euroopassa kybervakuutettujen osuus arvioidaan olevan n. 10%:n luokkaa (Lemnitzer, 2021, 120) ja Suomessa asiantuntijoiden arviot ovat vieläkin maltillisempia (Ollila, 2024). Tietoisuus yleistyy kuitenkin jatkuvasti ja hankintaprosessi helpottuu. Vakuuttaminen ei ole tietysti oikotie onneen riskienhallinnan kokonaisuuden kannalta, vaan jotta kyberriski olisi ylipäättään vakuutettava riski, täytyy sen hallinta olla organisaatiossa tietyllä tasolla (Biener ym., 2015).

2.3.2 Standardeihin perustuva hallinta

Yksi tapa lähestyä kyberriskien hallintaa on erilaisten standardien ja viitekehysten kautta. Nämä auttavat hahmottamaan kyberriskien hallintaa ja riittävää riskienhallinnan tasoa. Pääsääntöisesti ne ovat toimivia työkaluja, vaikkakin niissä on tietysti omat heikkoutensa ja soveltumattomuudet etenkin

pk-yrityksille. Pk-yrityksillä usein heikon tietoturvan taustalla on resurssipula, mikä tarkoittaa sitä, että toiminnan reunaehdoja ja tavoitetasoja määrittelevät standardit saattavat helpottaa riskienhallintatyötä ja konkretisoida mitä kaikkea yrityksen tulisi tehdä kyberturvallisuutensa eteen (Hoppe ym., 2021). Vaikka yleisimpiä viitekehyksiä ei olekaan spesifioitu nimenomaan pk-sektorille, ovat ne silti suhteellisen joustavia organisaation koon suhteen, ja kyberriskien ollessa suhteellisen samoja koosta riippumatta, pätevät yleisesti myös samat standardien käytäntösuositukset ja vaatimukset.

Riskienhallintaprosessi mielletään perinteisesti monivaiheiseksi prosessiksi, josta yksi tunnetuimmista malleista on kansainvälisen standardisoimisjärjestö ISO:n luoma ISO 31000-standardi (kuvio 3). Pääpiirteissään se sisältää riskien arvioinnin, jota seuraa sen pohjalta toteutettava riskin käsittely ja seuranta. Riskien arviointi alkaa riskien tunnistamisella, jatkuu riskianalyysillä ja merkityksen arvioinnilla (ISO, 2018, 15). ISO:n riskienhallintaprosessissa korostuu kyberriskien osalta se, ettei hallinta jää pelkästään IT-osaston tai kyberturvallisuudesta vastaavan harteille, vaan siihen osallistuu kokonaisvaltaisesti koko organisaatio (Antonucci, 2017). Tämä onkin yksi keskeisimmistä haasteista, sillä perinteisempien riskien kuten paloriskien ennaltaehkäisy ovat lapsesta asti juurrutettu ihmisten mieliin ja tulevat useimmilla myös työpaikoilla selkärangasta, toisin kuin kyberturvallisuuteen liittyvät periaatteet.



Kuvio 3. Riskienhallintaprosessi ISO:n standardin mukaisesti (ISO, 2018, 14)

Haastavin vaihe pk-yrityksen kannalta voi olla prosessin aloitus, eli täsmällinen kyberriskien tunnistaminen. Kyberriskejä voi olla vaikea hahmottaa ja tunnistaa konkreettisesti, varsinkin sellaisen, joka ei ole päivittäin tekemisissä kyberturvallisuuden kanssa. Riskit voivat muodostua organisaation sisältä tai ulkoa – joko tarkoituksellisesti tai tahattomasti (Böhme ym. 2019). Toisena seikkana on kustannus. Kyberriskejä on vaikea muuttaa euroiksi eli riskien merkityksen arviointi; millaista taloudellista vahinkoa tietty kyberriski voi aiheuttaa. Kustannusten analysointi voi olla miltei mahdotonta, esimerkiksi jos kyberhyökkäys sisältää henkisten väkivallan elementtejä tai se vaikuttaa voimakkaasti yrityksen maineeseen, jolloin yritysarvoon kohdistuva vaikutusta voi olla pitkällä aikavälillä hyvin vaikea arvioida (Eling & Schnell, 2016). Standardit pyrkivät vastaamaan näihin haasteisiin eli loppupeleissä tekemään riskienhallinnasta tehokkaampaa ja yksinkertaisempaa. ISO:n riskienhallintaprosessissa vakuuttajien vaatimat kontrollivaatimukset kuuluvat lähtökohtaisesti ”riskien käsittely” ja ”raportointi” osioihin (ISO, 2018, 14).

Lisähaasteen tuo vielä tiheä muutostahti, mikä vaikeuttaa historiadatan perusteella tehtävää arviota tulevista riskiskenaarioista (Eling & Schnell, 2016). Riskin muutostahti on näkynyt myös julkaistuissa standardeissa. Esimerkiksi vasta voimaan tullut EU:n NIS2-direktiivi astui voimaan vain muutama vuosi alkuperäisen standardin version jälkeen (EUR-Lex, 2022). Tämä kertoo hyvin sen, kuinka nopeasti riskikenttä muuttuu ja tahti tuskin on hidastumassa. NIS2-direktiivin tarkoitus on parantaa ja harmonisoida etenkin yhteiskunnan tasolla kriittisten yritysten kyberturvallisuuden tasoa. Tämä voi koskea myös pk-yrityksiä, mikäli ne toimivat direktiivissä määritellyllä alueella. Pienemmille yrityksille on kuitenkin annettu joitain helpotuksia raportoinnin ja sakkojen suhteen (EUR-Lex, 2022). Merkittävin ero tässä viitekehyksessä on ISO:n standardeihin tietysti se, että direktiivi asettaa lakisääteiset vaatimukset suositusten sijaan.

Yleisen riskienhallintastandardin lisäksi ISO on julkaissut liudan muitakin standardeja, joista yksi merkittävimmistä on tietoturvastandardi ISO 27001, jonka ensimmäinen versio julkaistiin jo vuonna 2005. Standardi määrittelee vaatimukset riskien arviointiprosessista sekä tietoturvan hallintajärjestelmälle (ISO, 2022). Sen lisäksi, että standardinmukaisesta toiminnasta saatava sertifikaatti lisää luottamusta kumppaniverkostossa ja tietysti parantaa organisaation kyberturvallisuuden kypsyystasoa, sitä voidaan vaatia yhä useammin yhteistyökumppanien toimesta – myös pk-yrityksiltä. Esimerkiksi monet puolustus- ja turvallisuusalan yritykset vaativat jokaiselta alihankkijaltaan tietoturvasertifikaatteja. Sertifikaatit pakottavat yrityksen käymään laajasti läpi omia kyberriskejä ja niihin implementoituja kontroleja, kuten alla olevasta kuviosta voidaan nähdä. Yksi paljon sovellettu viitekehys kontrollien suhteen on myös 18 kontrollin listaus (kuvio 10), johon on

kerätty CIS:n (Center for Internet Security) näkemyksen mukaan oleellimmat kontrollit kyberturvallisuuden kannalta. (CIS, 2017).



Kuvio 4. Päivitetyt ISO 27001:2022-standardin riskikontrollit jaoteltuna riskikategorioittain (Djebbar & Nordström, 2023)

Miten vakuuttaminen sitten asemoituu näihin standardeihin ja viitekehyksiin? Mikäli yritys on hankkinut itselleen sertifikaatin tai on esimerkiksi NIS2-direktiivin alla, kertoo se vakuutusyhtiölle jo vähintään sen, että asioita on käyty läpi ja perusjutut kyberriskien hallinnan osalta ovat todennäköisesti kunnossa (Marotta ym., 2017). Jos katsotaan esimerkiksi kuvion 4 jaottelua, nähdään että kyseisessä ISO-sertifikaatissa on kontroleja hyvin laajasti pk-yritykselle, ja mikäli ne ovat kaikki implementoitu kiitettävästi, ei vakuuttajalla välttämättä ole enää lainkaan lisätoiveita kontrollien osalta (Djebbar & Nordström, 2023).

Useilla vakuutusyhtiöillä kontrollivaatimukset perustuvatkin juuri standardeihin ja historiatiedon valossa kaikista tehokkaimpiin kontroleihin. Erilaiset järjestöjen standardit ja viranomaisten laatima lainsäädäntö ovat entistä tärkeämpää, kun poliittinen ja taloudellinen ympäristö on muuttunut jo pidemmän aikaa epävarmempaan suuntaan, jolloin yritysten riskienhallinnan merkitys korostuu. Standardit, viitekehykset ja niiden noudattaminen pitäisi olla lähtökohtaisesti kaikkien osapuolten etu. Ne luovat osviittaa sille, missä yritysten riskienhallinnan taso olisi standardinmukainen, mutta samalla ne ovat myös neutraali malli ja auktoriteetti vakuuttajien suuntaan sen suhteen, missä menisi riittävän kontrollivaatimustaso. Lisäksi viranomaisten julkaisemat vaatimukset, kuten EU:n vastikään voimaan tullut yleinen tietosuojasetus GDPR sekä NIS2 lisäävät yritysten tietoisuutta kyberriskeistä ja niiden hallinnan tärkeydestä, mikä voi myös osaltaan lisätä kysyntää kybervakuutuksille. (Marotta ym., 2017)

2.4. Kybervakuuttaminen

Vaikka yritykset ovat maailmalla ja Suomessakin hyödyntäneet kyberympäristöä liiketoiminnassaan jo kymmeniä vuosia, on kybervakuuttaminen suhteellisen tuore tulokas. Viimeisen noin kymmenen vuoden aikana kybervakuutuksia on vasta laajemmin saapunut Suomen ja Pohjois-Euroopan markkinoille. Ennen itsenäisten (standalone) kybervakuutusten laajempaa tarjontaa, perinteiset omaisuus- tai vastuuvakuutukset saattoivat sisältää kyberlaajennuksen ehdoissaan. Kolmas vaihtoehto saada riskin siirtoa vakuuttamisella on niin kutsuttu hiljainen vakuutusturva, jossa kybervahinkoja ei olla selkeästi ehdoissa lisätty, mutta ei myöskään rajattu pois (Vogel, 2018). Myöhemmin muiden omaisuusvakuutusten kyberlaajennuksia on niiden suurten kustannusten ja vaikean ennustettavuuden takia purettu pois, ja siirrytty enemmän itsenäisten kybervakuutusten suuntaan (Biener ym., 2015). Tämä on johtunut useasta eri syystä, mutta yhtenä päätekijänä oli vuoden 2017 aikana myllänneet NotPetya ja WannaCry kyberhyökkäykset, jotka aiheuttivat miljardien eurojen vakuutuskorvauksia vakuutusyhtiöille, vaikkei kyseisiä vakuutustuotteita ollut suunniteltu erityisesti kyberriskien varalle (O'Brien & Davis, 2020).

Kybervakuutustuotteet voidaan jakaa karkeasti kahteen: omaisuus-keskeytysvakuutuksen perustuvaa kyberturvaa ja vastuuvakuutuksiin perustuvaa turvaa. Omaisuusvakuutuksen perustuva kybervakuutus kattaa pääosin käyttökelvottomia laitteita ja tietojen palautusta sekä menetettyä katetuottoa liiketoiminnan mahdollisesta keskeytymisestä. Vastuuvakuuttamiseen pohjautuva kybervakuutus kattaa enemmän kolmansille osapuolille aiheutettuja kustannuksia ja mahdollisia vahingonkorvauksia ja oikeudenkäyntikuluja. Tällaisesta tuotteesta esimerkki on techpi-vakuutus (professional indemnity for technology professionals), jossa yhdistyvät sekä ammatillinen vastuuvakuutus ja kybervakuutus. (Kuosmanen & Pitkämäki, 2023). Yleisintä on toki se, että kybervakuutus on jonkinlainen yhdistelmä näitä ominaisuuksia riippuen tuotteen laajuudesta sekä vakuutuksenottajan liiketoiminnasta. Suomalaiset yhtiöt ovat päätyneet pääosin kirjoittamaan suppeampia ehtoja verrattuna kansainvälisiin vakuutustuotteisiin. Näin hinta on pysynyt maltillisempänä, mutta toisaalta ajatus suppeasta kattavuudesta voi aiheuttaa mielikuvaa turhana vakuutuksena kyberriskeihin nähden. Konkreettinen esimerkki tästä on lunnasvaatimukset, joka saattaa kääntää monen yrityksen valinnan kansainväliseen ratkaisuun (Kailio, 2021).

Yhdysvalloissa kybervakuutuksia on yli 30%:lla yrityksistä (Granato & Polacek, 2019), minkä taustalla on osaksi paikallisen lainsäädännön tiukemmat vaatimukset ja suurempi vastuuriiski. Koska mahdolliset kybervahingon kustannukset ovat suuremmat, myös kybervakuutuksen tarjoama suoja

on merkittävämpi. Lisäksi Yhdysvalloissa on ollut Eurooppaa pidempään voimassa lakisääteinen raportointivelvollisuus kaikista kybervahingoista, joka on lisännyt yritysten tietoisuutta ja aktiivisuutta kyberriskien hallinnassa (Eling & Schnell, 2016). Vakuutusliiketoiminnassa volyyymi näkyy väistämättä vakuutusten houkuttelevuudessa. Suomessa on luonnollisesti yrityksiä murto osa Yhdysvaltojen markkinaaan verrattuna, ja vieläkin pienempi määrä maksajia kybervakuutuksen osalta, joka väistämättä näkyy hinnoittelussa ja vakuutussopimusten sisällössä. Suomen vahinkovakuutusmarkkina on pitkälti jakautunut kolmelle suurimmalle yhtiölle: Pohjola vakuutus 32,6%, LähiTapiola-ryhmä 27,8% ja If vahinkovakuutus 21,8% (Finanssiala, 2024). Kaikki Suomen suuret vahinkovakuutusyhtiöt tarjoavat kybervakuutusta. Lisäksi Suomessa toimii useita kansainvälisiä vakuuttajia aktiivisesti kybervakuutusmarkkinoilla, kuten yhdysvaltalaiset vakuuttajat AIG ja Chubb.

Samoin kuin kyberriskien osalta, myös kybervakuuttamista on haastava määritellä yksiselitteisesti, osittain sen markkinoiden uutuuden takia, osittain sen diversiteetin vuoksi. Terminä kybervakuutus saattaa kuulostaa korkealentoiselta, joten kotimaiset vakuuttajat puhuvatkin mieluummin etenkin pienempien yritysten parissa tietoturvakvakuutuksesta, sisällön ollessa kuitenkin hyvin samanlainen. Suomen ja kansainvälisten kybervakuutusten tarjonta poikkeavat toisistaan usein sekä hintatason että vakuutusehtojen osalta, mutta määrittelen tässä yleisen kansainvälisen linjan mukaisesti kybervakuutuksen määritelmän ja sen sisällön. Lähinnä oleellista on huomioida, että etenkin niin dynaamiseen riskiin kuin kyberriskiin on saatavilla hyvin monenlaisia räätälöityjä vakuutusratkaisuja. Pääidea kybervakuutuksessa on kuitenkin korvata nimensä mukaisesti vakuutuksenottajalle niitä taloudellisia menetyksiä, jotka aiheutuvat kybervahingosta. Poikkeuksellisen vakuutusturvan kybervakuutuksista tekee sen nopea muutostahti verrattuna muihin. Hintataso ja ehdot voivat muuttua nopeastikin vahinkokehityksen mukaisesti markkinoiden hakiessa vielä tasapainoa. (Kuosmanen & Pitkämäki, 2023)

Kybervakuutuksella onkin nuoresta iästään huolimatta monivaiheinen historia, joka sai alkunsa ensin 80-luvulla vastuuvakuutusten teknillisenä laajenuksena, mutta kehittyi varsinaiseksi itsenäiseksi vakuutuslajiksi vasta 90-luvulla IT-kuplan kehittyessä ja kysynnän kasvaessa. Usein ensimmäiseksi kybervakuutukseksi tituleerataan keväällä 1997 yhdysvaltalaisyhtiö AIG:n myöntämää vakuutusta nimellä ”internet security liability policy” (Granato & Polacek, 2019). AIG oli myös ensimmäinen, joka lisäsi vakuutukseen kolmannen osapuolen kulut kattavan lisäyksen. Sen jälkeen kysyntä on ollut jatkuvassa kasvussa, ja erilaisten vakuutusratkaisujen määrä on kasvanut huimasti ympäri maailmaa. Kybervakuutusten myynnit ovat olleet koko 2000-luvun selkeässä kasvussa, ja jotain kertoo

markkinasta Euroopan suurimman jälleenvakuutusyhtiö Munich Re:n ennuste, jonka mukaan seuraavan viiden vuoden aikana bruttomaksutulolla mitattuna kybervakuuttamisen markkina tulee yli tuplaantumaan yli 30 miljardiin euroon (Munich Re, 2024). Potentiaalia on kuitenkin vielä valtavasti, sillä samalla kuitenkin vasta alle puolet maailman yrityksistä ovat hankkineet kybervakuutuksen ja pk-sektorista vielä huomattavasti pienempi osa. Vertailun vuoksi perinteisten yritysvarakuutuslajien bruttomaksutulot ovat useita satoja miljardeja euroja (McDonald, 2023).

Kansainvälisen laajemman kybervakuutuksen kattavuuden voi jakaa karkeasti neljään osaan: 1) katteenmenetys sekä ylimääräiset kustannukset, 2) järjestelmien ja tietojen palautuskustannukset, 3) vahingot kolmannelle osapuolelle ja 4) kiristyskustannukset. Tämä on toki hyvin tapauskohtaista ja vain yksi tapa hahmottaa sisältö. Yleisesti voidaan myös jaotella, että kybervakuutuksesta voidaan korvata vahingon sattuessa korvauksia vakuutetulle itselleen sekä kolmannelle osapuolelle kohdistuneisiin kustannuksiin (Biener ym., 2015). Yleensä kybervahingosta aiheutuu jonkinasteista keskeytystä yrityksen liiketoiminnalle, jolloin vahingosta aiheutuu katteenmenetystä. Ylimääräisillä kustannuksilla tarkoitetaan niitä kustannuksia, jotka liittyvät suoraan kybervahinkoon, mutta jotka eivät tulisi muuten maksuun normaaleissa olosuhteissa, esimerkiksi ylityötunnit IT-osastolle tilanteen selvittämisestä. Kiristyskustannukset nostin esiin erikseen, sillä kybervakuutus sopimuksissa on eroja korvaavatko ne lainkaan kiristystilanteisiin liittyviä kustannuksia, mutta yleensä laajemmissa ehdoissa myös lunnasmaksut on katettu. Kotimaiset vakuuttajat eivät niitä pääsääntöisesti kata (Kailio, 2021), ja tästä onkin ollut yhteiskunnallista keskustelua, että onko eettismoraalisesti oikein tukea rikollista toimintaa maksamalla lunnaita.

Vaikka laajemmat kyberehdot tarjoavat yritykselle hyvän ja suhteellisen kattavan turvan kyberriskien varalle, on yritysten johtajilla silti usein virheellinen kuvitelma niiden kattavuudesta. Tutkimuksen mukaan yritysten talousjohtajista yli 70%:a oletti kybervakuutuksen korvaavan yrityksen brändin heikkenemistä, sijoittajien luottamuksen laskua ja myynnin heikkenemistä kybervahingon seurauksena. Mitään näistä tyypillinen vakuutus ei kuitenkaan kata (Granato & Polacek, 2019). Ylipäätään kyberriskeistä seuraavia vahinkoja ei välttämättä kyetä arvioimaan taloudellisesti aina kovin tarkkaan, mikä haastaa omalta osaltaan vakuutusehtojen määrittelyä (Eling & Schnell, 2016). Ja vaikka ne toisaalta voitaisiinkin määritellä, haluaa vakuuttaja lähtökohtaisesti rajata riskin mahdollisimman selkeäksi jo entuudestaan epävarmassa riskilajissa. Sen lisäksi että yritysjohtajat eivät tunne vakuutusten sisältöä kovin tarkasti, on yleisesti ottaen tietoisuus hyvin heikkoa etenkin pk-yritysten joukossa koko vakuutuksen osalta. Tätä vahvistaa se, että vakuutettujen osuus Suomessa

suunnilleen sama kuin kyberhyökkäyksen kohteeksi joutuneiden pk-yritysten (Ollila, 2024 ja Toivonen, 2017).

2.4.1. Vakuuttamiskelpoisuus

Vakuuttaminen perustuu suurten lukujen lain mahdollistamaan taloudelliseen riskienhallintaan; suomeksi idea on varautua ikäviin yllätyksiin. Se on kuitenkin myös tarkkaan laskettua liiketoimintaa, sillä kaikki perustuu riskien arviointiin ja todennäköisyyksien laskemiseen. Jos mietitään isoakin vakuutussalkkua kybervakuutuksia, jonka asiakasyrityksiin kohdistuu muutama isompi kybervahinko, muuttuu portfolion tuotto nopeasti miinusmerkkiseksi. Vakuuttajat eivät luonnollisesti halua kaikkia riskejä vakuuttaa, eikä se ole niiden liiketoiminnan tarkoituskaan. Vakuutusmaksujen ja riskien suhde tulee aina vastata kokonaisuutena, ja jotta tietty riski voitaisiin vakuuttaa, siltä vaaditaan tiettyjä ominaisuuksia ja edellytyksiä (Kivisaari & Rantala, 2020). Siksi on olemassa esimerkiksi kyberriskien osalta kontrollivaatimukset, joilla vakuuttajat pyrkivät hallitsemaan valitsemaansa riskiä.

Voimakkaasti dynaamiset riskit kuuluvat vaikeammin vakuutettavien luokkaan, ja usein sellaisille riskeille, jotka ovat esimerkiksi hyvin suhdanneherkkiä ei löydykään vakuuttajaa. Tästä esimerkki voisi olla poliittisen riskin vakuuttaminen epävakaaassa maassa tai terrorismin vakuuttaminen riskialttiilla alueella. Vakuutuskelpoiselle riskille mielletään olevan yleensä muutama kriittinen ominaisuus. Yksi listaus vakuutettavalla riskille on ennustettavuus, riippumattomuus edunsaajasta, stabiliteetti sekä riskin toteutumisen harvinaisuus. Ennustettavuudella tarkoitetaan sitä, että vakuutettavaa riski tulee olla jollain tasolla ennustettavissa. Mikäli ennustettavuus on heikkoa kuten joissain kyberriskeissä, vakuuttaja joutuu pyytämään sopimuksesta korkeampaa hintaa, ja pyrkiä kasamaan yhteen esimerkiksi erilaisten syndikaattien avulla harvinaisempia riskejä. Riippumattomuus edunsaajasta tarkoittaa sitä, ettei vakuutuksenottaja saa olla suoraan tahallaan tai törkeällä tuottamuksella tuottanut vahinkoa, jotta se olisi korvattavaa. Stabiliteetti kuvaa nimensä mukaan sitä vakuutettavan riskin ominaisuutta, jossa sen vaaditaan olevan riittävän vakaata todennäköisyyksien valossa aikaan suhteutettuna. (Biener, Eling & Wirfs, 2015)

Tämän vuoksi liikeriskit eivät yleensä ole vakuutettavia riskejä (Kivisaari & Rantala, 2020). Riskin toteutumisen harvinaisuus on laveahko vaatimus riskille, mutta toki idea on suhteuttaa harvinaisuus aina vakavuuteen. Eli mitä suurempi vahinko voi olla kyseessä, sitä harvemmin se saa vakuuttajan näkökulmasta tapahtua. Tämä on yksi kybervakuuttamisen ydinhaasteista, harva pystyi ennustamaan

korvausmäärien pomppua tullessa 2020-luvulle, eikä ole mitään syytä epäillä, etteikö niin voisi käydä myös tulevaisuudessa. Pahimmassa hyökkäysaallossa koronapandemian aikaan monet vakuuttajat jopa väläyttelivät mahdollisuutta, että kyberriskiä ei enää kyettäisi vakuuttaa ainakaan samassa mittakaavassa (Smith, 2022). Tämä uhka on kuitenkin suurimmaksi osaksi väistynyt, mutta toki on hyvin mahdollista, että vastaava ilmiö tapahtuisi tulevaisuudessakin.

Tämä nelijakoinen listaus on yksi mahdollinen tapa lähestyä vakuutettavaa riskiä, mutta toki samalla on hyvä muistaa, että suhtautuminen riippuu aina hieman vakuuttajasta, eivätkä edellytykset ole mustavalkoisia, koska kaikki on lopulta enemmän tai vähemmän tulkintaa ja arviointia. (Kivisaari & Rantala, 2020). Teknologian kehitys tuo oman mausteensa vakuutettavuuteen ja sen arviointiin, sillä menetelmät arvioida yrityksen kyberriskiä kehittyvät jatkuvasti ja tuovat uusia mahdollisuuksia vakuutusprosessiin ja vakuutusyhtiön riskienhallintaan (World Economic Forum, 2024).

Vakuutuskelpoisuuden kriteeristö		Arvio vakuutuskelpoisuudesta	Keskeisimmät havainnot
Aktuaariset kriteerit	Vahinkojen sattumanvaraisuus	Ongelmallinen	<ul style="list-style-type: none"> Tiedon puute Kyberriskien muuttuva luonne
	Maksimivahingon suuruus	Ei-ongelmallinen	<ul style="list-style-type: none"> Kyberriskien enimmäistappio on pienempi kuin muiden riskien. Vakuutusyhtiöt suojaavat suurimmilta tappioilta korvausrajoilla
	Keskimääräinen vahinko	Ei-ongelmallinen	<ul style="list-style-type: none"> Kyberriskin keskimääräinen tappio myös pienempi kuin muiden riskien. Riippuu yrityksen koosta, omasuojelusta ja sitoutumisen tasosta.
	Vahinkojen määrä	Ei-ongelmallinen	<ul style="list-style-type: none"> Kybervahinkojen määrän kasvu Riippuvainen tapahtumaluokasta
	Informaation epäsymmetria	Ongelmallinen	<ul style="list-style-type: none"> Moraalikato ja haitallinen valikoituminen ovat merkittäviä uhkia
Markkinakriteerit	Vakuutusmaksu	Vähäinen ongelmallisuus	<ul style="list-style-type: none"> Epävarmuustekijöistä johtuvat korkeat vakuutusmaksut Kilpailun vähäinen määrä toistaiseksi
	Vakuutusturva	Ongelmallinen	<ul style="list-style-type: none"> Korvausrajat eivät välttämättä riitä Rajoitusehdot joskus ongelmallisia Korvattavuus voi olla epäselvää
Yhteiskunnalliset kriteerit	Yhteiskunnalliset periaatteet	Vähäinen ongelmallisuus	<ul style="list-style-type: none"> Moraalikato ja kybermaailman verkottuneisuus lisäävät riskiä Vakuutuspetosten määrä voi kasvaa
	Lainsäädännölliset rajoitteet	Vähäinen ongelmallisuus	<ul style="list-style-type: none"> Sakkoja ei voida usein vakuuttaa Riski uusista lakimuutoksista Oikeudellinen uhka vakuuttajille ja meklareille

Kuvio 5. Kyberriskien vakuutuskelpoisuustaulukko. (Mukaiillen Biener ym. 2015; Berliner 1982)

Toinen esimerkki vakuutuskelpoisuuden kriteeristöstä näkyy yllä olevasta taulukosta (kuvio 5, Biener ym. 2015; Berliner 1982), jossa on listattu kelpoisuuden kriteerejä ylä- ja alatasolla, niiden ongelmallisuuden tasoa ja oikealla keskeisimpiä havaintoja kybervakuuttamiseen liittyen. Berlinerin (1982) alun perin esittelemä jako on yksinkertainen, mutta silti kattava ja nykypäivänakin toimiva työkalu vakuutuskelpoisten ja vakuutuskelvottomien kyberriskien jakamiseen. Jaottelussa on yhdeksään eri kategoriaan, ja ne jakautuvat kolmeen eri pääluokkaan, jotka ovat aktuaariset kriteerit, markkinakriteerit sekä yhteiskunnalliset kriteerit. Näille jokaiselle kriteerille on määritetty omat vaatimuksensa, jotta tarkasteltava riski on luokiteltavissa vakuutuskelpoiseksi (Biener ym. 2015). Arvio ongelmallisuudesta on tietysti subjektiivinen näkemys, ja noin kymmenessä vuodessa esimerkiksi lainsäädännölliset rajoitteet ovat muuttuneet merkittävästi.

Vakuutuskelpoisuus ei ole siis mitenkään yksinkertainen kysymys, etenkin kyberriskien saralla, joka on tunnettu sen heikosta ennustettavuudesta, dynaamisesta luonteesta ja korreloituneisuudesta. Koska kyberriskit kehittyvät jatkuvasti teknologian muuttuessa ja hyökkäystekniikoiden monipuolistuessa, on vakuutusyhtiöiden vaikeaa arvioida näiden riskien todennäköisyyttä ja vaikutuksia tarkasti (Dambra ym., 2020). Harva olisi osannut kuvitella muutama vuosi sitten kuinka paljon tekoäly tulee muuttamaan työelämää, joten samalla tavalla sen aiheuttamia riskejä edes lähitulevaisuudessa on vaikea ennustaa. Se tulee varmasti molempia osapuolia auttamaan (Jada & Mayayise, 2023), mutta kumpaa enemmän ja miten se näkyy vahinkokehityksessä, on avainkysymys vakuuttajille. Kansainvälisen tutkimuksen mukaan tietoturvajohdajista vain noin yhdeksän prosenttia uskoo, että generatiivisesta tekoälystä on enemmän hyötyä puolustajille kuin kyberhyökkääjille (World Economic Forum, 2024). Toisaalta samaan aikaan myös teknologia kehittyy puolustajien näkökulmasta ja tulee uusia mahdollisuuksia suojautua vaikkapa toimitusjohtajahuujauksilta tai haittaohjelmilta, joten voidaan olettaa, että tuo luku tulee hyvin mahdollisesti muuttumaan lähivuosina.

Lisäksi kybervakuuttamiseen liittyy usein epäsymmetristä informaatiota, mistä aiheutuu moraalikatoa ja haitallista valikoitumista (Holmström, 1979, 89). Puutteellinen informaatio tarkoittaa sitä, että vakuutuksenantajalla ei ole täydellistä tietoa vakuutettavien yritysten kyberturvallisuuden tasosta, mikä pakottaa sen nostamaan vakuutuksien hintaa (Eling & Schnell, 2016). Tämä hankaloittaa vakuuttamisprosessia entisestään, etenkin pk-sektorin näkökulmasta, joissa prosessi pitäisi olla kustannustehokas ja julkista tietoa ei ole juuri saatavilla. Haitallinen valikoituminen ilmenee kybervakuuttamisessa siten, että yritys, joka on alttiimpi kybervahingolle, hankkii itselleen ennemmin vakuutuksen toisin kuin sellainen yhtiö, jolla riski on pienempi. Tämä voi pitemmällä

aikavälillä aiheuttaa sen, että vakuutuksenantajat kohtaavat keskimäärin suurempia riskejä kuin on odotettu (Böhme ym. 2019). Moraalikato puolestaan tarkoittaa tilannetta, jossa kybervakuutuksen saaminen voi johtaa siihen, että yritykset eivät investoi riittävästi kyberturvallisuuteen, koska ne luottavat vakuutuksen kattavan mahdolliset vahingot (Biener ym, 2015). Nämä haasteet ovat osasyitä sille, miksi kybervakuuttaminen on haastava vakuutettavuuden näkökulmasta, mutta toisaalta samat lainalaisuudet pätevät muidenkin vakuutuslajien osalta.

Niin kutsuttu knock-on -efekti tai suomennettuna lumipalloefekti on vakuutettavuudesta puhuttaessa oleellista huomioida. Tällainen tilanne voi esimerkiksi tulla kyseeseen, jos suuri ohjelmistotoimittaja joutuu kyberhyökkäyksen kohteeksi ja vaikutukset leviävät globaalisti laajalle sen asiakkaiden keskuudessa, aiheuttaen merkittäviä vahinkoja useissa eri yrityksissä samanaikaisesti ja voi mahdollisesti levitä vielä asiakkaiden asiakkaillekin vahingon kumuloituessa. Yksi esimerkki tällaisesta riskistä realisoitui vuonna 2017 kun Ukrainaan alun perin suunnattu kyberhyökkäys levisi Windowsin haavoittuvuutta pitkin ympäri maailmaa ja esimerkiksi logistiikkajätti Maerskille aiheutui tästä ”sivullisena uhrina” yli 300 miljoonan euron tappiot, kun se joutui asentamaan lähes kaikki työasemat uudelleen (Roth & Wesley, 2024).

Tämänkaltainen riski poikkeaa perinteisistä vakuutusriskien laskentamalleista, joissa riskit pyritään valitsemaan usein suhteellisen itsenäisinä ja sen voidaankin ajatella olevan yksi riskin vakuutuskelpoisuuden periaatteista (Kivisaari & Rantala, 2020). Toki poikkeuksiakin on, esimerkiksi jos mietitään luonnonkatastrofeja, niin riskithän ovat valtavia ja hyvinkin korreloivat keskenään, mutta joita kuitenkin pystytään ennustamaan suhteellisen tarkkoilla ennustusmalleilla ja nykitekniikkaa hyödyntämällä. Lisäksi sääilmiöiden aiheuttamia suurvahinkoja varten vakuuttajat ovat tehneet globaalisti jo pitkään laajamittaista yhteistyötä (Suutari, 2021), toisin kuin kybervakuutusten osalta, jossa vakuutusmarkkinat vielä hakevat asemiaan ja yhtiöt kasvattavat tiimejään.

Kyberriskit ovat pääsääntöisesti riippumattomia edunsaajasta, mikä tarkoittaa, että yrityksen omilla toimilla ei yleensä voida aiheuttaa tahallista kyberhyökkäystä, vaikka tietoturvan taso vaikuttaakin riskin toteutumiseen. Tällainen tilanne voi kuitenkin käydä toteen, mikäli yrityksen oma työntekijä päättäisi esimerkiksi kavaltaa rahaa tai asentaa kiristyshaittaohjelman. Nämä tilanteet ovat kuitenkin usein rajattu kybervakuutuksen ulkopuolelle. Stabiliateetin osalta, vaikka kyberrikosriskit muuttuvat nopeasti, vakuutuksenantajat voivat käyttää lyhyen aikavälin sopimuksia ja säännöllisiä uudelleenarviointeja hallitakseen tätä ongelmaa (Eling & Schnell, 2016). Usein kybervakuutukset

myönnetäänkin vain määräaikaisesti kerralla vain vuodeksi eteenpäin (Kuosmanen & Pitkämäki, 2023).

Biener ym. (2015) soveltavat vakuutuskelpoisuuskriteeristöä kyberriskien analysointiin. Berlinerin kriteerit jakautuvat kolmeen pääluokkaan (kuvio 3): aktuaariset kriteerit, markkinakriteerit ja yhteiskunnalliset kriteerit. Kussakin kategoriassa on omat vaatimuksensa, joiden täytyminen määrittää riskin vakuutuskelpoisuuden. Taulukon uloimmassa sarakkeessa on kuvattu kriteerin mahdollista problematiikkaa kybervakuuttamisen osalta. (Biener ym., 2015)

Aktuaariset kriteerit sisältävät seuraavat vaatimukset: 1) Riskien täytyy olla satunnaisia ja riippumattomia, jotta vakuutusenantajat voivat ennustaa vahinkojen todennäköisyyden ja asettaa vakuutusmaksut sen mukaisesti. Kyberriskien osalta tämä on ongelmallista, sillä riskit eivät ole täysin riippumattomia ja hyökkäykset voivat levitä laajasti. 2) Vahinkojen suuruuden tulee olla rajallinen. Kyberriskien kohdalla suurvahinkojen potentiaali on suuri, mikä voi asettaa rajoituksia vakuutusten tarjoamiselle. 3) Keskimääräisen tappion tulee olla ennustettavissa, joka kyberriskien tapauksessa on haasteellista, koska historiallista dataa on rajallisesti ja riskit muuttuvat nopeasti. Aktuaarisista kriteereistä sattumanvaraisuuden vaatimus on erityisen haastava, koska kyberhyökkäykset voivat olla hyvin suunniteltuja ja kohdistua tiettyihin yrityksiin tai toimialoihin, jolloin niiden riippumattomuus kärsii. (Biener ym., 2015)

Markkinakriteerit sisältävät seuraavat vaatimukset: 1) Vakuutettavien tulee altistua riskille satunnaisesti. Kyberriskien osalta tämä toteutuu vain osittain, koska yritykset voivat olla jatkuvasti alttiina kyberhyökkäyksille. 2) Tietojen epäsymmetria vakuutusenantajan ja vakuutusnottajan välillä tulee minimoida. Tämä on merkittävä ongelma kyberriskien vakuuttamisessa, koska vakuutusenantajat eivät usein tiedä kaikkia yksityiskohtia vakuutettavan yrityksen kyberturvallisuudesta, vaikka perusasiat saataisi selville. Henkilöstön osaamistaso ja tietoisuuden kasvattaminen on esimerkki tällaisesta laadullisesta seikasta, jota on vaikea mitata. 3) Maksujen tulee olla oikeudenmukaisia ja riittäviä kattamaan riskit. Kyberriskien osalta tämä vaatii tarkkaa riskinarviointia ja jatkuvaa seuranta. Markkinakriteereistä epäsymmetrinen informaatio on erityisen merkittävä kyberriskien kohdalla. (Biener ym., 2015).

Näiden taulukon kriteerien valossa kyberriskit ovat teorian osalta osittain vakuutuskelpoisia, mutta monien kriteerien täyttäminen vaatii jatkuvaa kehitystä ja markkinoiden mukautumista. Kyberriskien ennustettavuuden ja hallittavuuden parantaminen on keskeistä vakuutusten onnistumiselle, jossa

teknologinen kehittyminen on isossa roolissa. Biener ym. (2015) korostavat, että vakuutuksenantajien ja -ottajien välinen tiivis yhteistyö ja kommunikaatio ovat olennaisia, jotta voidaan vähentää tiedon asymmetriaa ja siten parantaa vakuutusmarkkinoiden toimivuutta ja hintatason stabiiliteettia. Tätä varmasti tulevaisuuden teknologiat tulevat omalta osaltaan helpottamaan, kun kaikkea tietoa ei tarvitse vaihtaa sähköpostiviestien tai haastattelujen välityksellä.

Kybervakuuttajat ovat jatkuvasti kehittyneet omaa underwriting-prosessia. Markkinat ovat olleet kasvussa, ja vakuutusyhtiöt investoivat yhä enemmän kyberturvallisuuden asiantuntemukseen ja riskienhallintatyökaluihin. Tämä kehitys mahdollistaa entistä tarkemman riskien arvioinnin ja hinnoittelun, mikä parantaa vakuutusten houkuttelevuutta sekä ylipäättään riskien vakuutettavuutta. Tulevaisuudessa myös lainsäädännölliset muutokset ja standardisoinnit voivat helpottaa kyberriskien vakuutusprosessia. Vakuutusten sisältöjen standardisointi ja selkeyttäminen etenkin pienemmille yrityksille, joilla ei ole välttämättä erillisiä riskienhallintatiimiä tai laajaa IT-osastoa tulkaamassa päättävällä johdolle on oleellista, jotta vakuuttajat ja asiakkaat pääsevät lähemmäs ”samalle aaltopituudelle” ja epäsymmetrisen tiedon määrä vähenee. (Granato & Polacek, 2019)

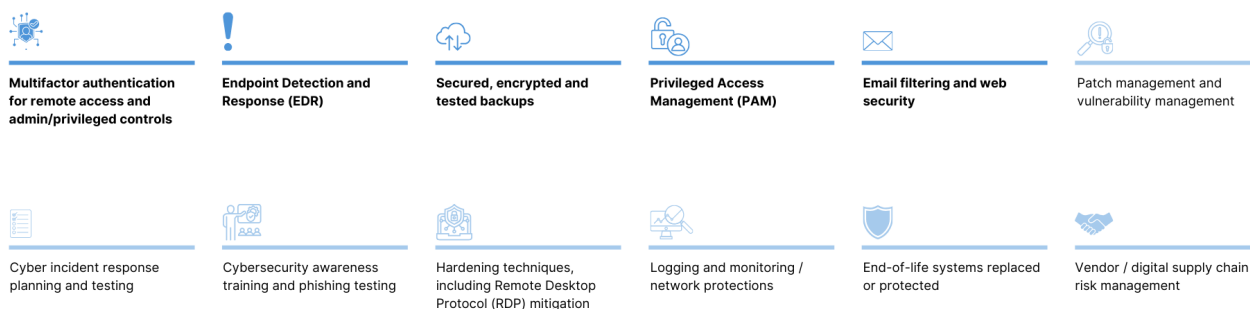
Yhteenvetona vakuutettavuuden osalta voidaan todeta, että vaikka kyberrikosriskien vakuutuskelpoisuuteen liittyy merkittäviä haasteita, kuten riskien vaikea ennustettavuus, niiden dynaaminen luonne ja toisaalta vakuutusliiketoiminnalle tyypilliset ilmiöt kuten haitallinen valikoituminen ja moraalikato, on myös useita tekijöitä, jotka tukevat näiden riskien vakuuttamista ja luovat sille merkittävän kasvupotentiaalin vakuutusosalalla. Suurin on tietysti jatkuva digitalisaatio ja riskitietoisuuden kasvu ja yritysten halu suojautua tältä. Tämä ristiriitaisuus yhdistettynä teknologian jatkuvaan kehitykseen tekee kybervakuuttamisesta mielenkiintoista, mutta riskialttiin ja tuntemattoman tuotteen vakuutusyhtiöille. Jokainen vakuutuskausi lisää kuitenkin valtavat määrät datan ja sen perusteella kasvavan riskiymmärryksen määrää, joten hintatason saattaa stabiloitua tulevina vuosina. (Granato & Polacek, 2019)

3 KONTROLLIVAATIMUKSET

3.1 Vähimmäisvaatimukset

Kyberriskit ovat siis merkittäviä kaikille yrityksille pienistä suuriin. Niitä on myös haastava hallita niiden erityisluonteen vuoksi, mistä syystä myös niiden vakuuttaminen vaatii vakuuttajilta erityistarkkuutta. Miten näitä riskejä ja niiden hallintakeinoja sitten arvioidaan ja analysoidaan yrityksistä? Puhutaan kontrollivaatimuksista tai vakuutettavuuskontrolleista, joita vakuutusyhtiöt asettavat kybervakuutuksen vaatimukseksi (esimerkki kuvio 6). Näiden vaatimusten tehtävänä on nimensä mukaisesti kontrolloida kyberriskejä ja ennen kaikkea niiden hallinnan tasoja, jotta vakuuttaja voi varmistua rahoittamastaan riskistä (Shamma, 2018).

Toisaalta kontrollivaatimukset ovat asiakasyritykselle tilaisuus tarkastaa oma kyberturvallisuustasonsa ja mahdollisesti paikata löytyviä aukkoja. Itse kontrolleilla tarkoitetaan siis käytäntöjä, joilla yritys suojaa itseään kyberriskeiltä. Kontrolli-sana itsessään saattaa olla hieman epäselvä, sillä toisaalta sillä tarkoitetaan niitä teknisiä ratkaisuja, joilla yritys pyrkii hallitsemaan omia kyberriskejä, ja toisaalta se on yleistermi kaikille riskienhallinnan toimille. Tässä tutkielmassa käytän termiä ”kontrollivaatimus” kuvamaan niitä ehtoja ja vaatimuksia, joita vakuutusyhtiö asettaa kybervakuutuksen ehdoiksi sekä joita se lisäksi toivoo asiakkaan täyttävän, mutta jotka eivät ole ehdottomia vakuutuksen myöntämiseksi (If, 2024). Kyseessä on joka tapauksessa elintärkeä osa kybervakuutusprosessia, mutta kuten muutenkin kybermaailmassa, myös kontrollivaatimukset ovat muuttuneet dynaamisesti, mikä on osaltaan ollut syynä markkinan volatilitettiin, sillä niiden muutokset näkyvät väkisin myös vakuutussopimusten sisällössä ja hintatasossa (Howden, 2023).



Kuvio 6. Keskeisimpiä kontrolleja. Tummalla värjättyt ovat vähimmäisvaatimuksia eli jotka tulisi vähintään olla vakuutuksenottajalla kunnossa. (Marsh Inc, 2020).

Käydään läpi vielä tarkemmin yllä olevan taulukon perustason kontrollit eli niin sanotusti vähimmäisvaatimukset, joita yrityksiltä edellytetään, jotta vakuutus voidaan myöntää. Nämä ovat

relevantteja jokaiselle yritykselle maantieteellisestä sijainnista tai liiketoiminnan koosta huolimatta kyberturvallisuuden kannalta. Pelkästään näiden viiden kontrollin käyttö ei tietenkään riitä kokonaisvaltaisen kyberturvallisuuden varmistamiseksi, mutta ne luovat hyvän perustan. Samoin kuin yrityksetkin, myös niille soveltuvat kontrollit ovat tapauskohtaisia ja yksilöllisiä – toimiala ja liiketoimintamalli vaikuttavat kyberriskitasoon merkittävästi, pahimmillaan pk-yrityskin voi vaarantaa ihmisten henkiä, mikäli se toimii kriittisellä toimialalla ja kohtaa vakavan kybervahingon (Marotta ym., 2017). Tämä luo ison haasteen yleispätevien kontrollivaatimuksien mietintään. Myöskään edellä mainitut viisi vähimmäiskontrollia eivät ole kaikille yrityksille pakollisia vakuutuksen saamiseksi, mutta nämä ovat kuitenkin niin perustason käytäntöjä, että niiden puuttuminen hyvin todennäköisesti vaikuttaa vähintään sopimuksen kattavuuteen tai hinnoitteluun (Marsh Inc, 2020).

Monivaiheista tunnistautumista sivuttiin jo aiemmin, ja se lienee nykypäivänä vähintään Suomessa olla jokaiselle internetin käyttäjälle tuttu. Sen tehtävä on varmistaa käyttäjälle turvallinen kirjautuminen laitteelle tai ohjelmistoon ja samalla estää hyökkääjiä kirjautumaan väärälle tilille. Sen toimintaperiaate on vaatia vähintään kahden tai useamman ”todennuksen” käytön ennen kuin kirjautuminen järjestelmään onnistuu. Tämä luonnollisesti tekee kyberrikosten toteuttamisesta huomattavasti vaikeampaa, kun enää pelkästään salasanan hakkerointi ei riitä järjestelmän sisäänkäyntiin (Kyberturvallisuuskeskus, 2020), jonka vuoksi sen käyttöaste organisaatioissa kiinnostaa suuresti vakuuttajia. Tällainen todennus voi olla salasanan lisäksi esimerkiksi sormenjälki, mobiilikoodi tai todennussovelluksen käyttö. Todennusmenetelmät voidaan jakaa kolmeen kategoriaan: 1) tietoon perustuva, esimerkiksi ulkoa muistettava salasana tai PIN-koodi, 2) omistamiseen perustuva, kuten matkapuhelimeen lähetettävä koodi tai viivakoodin luku henkilötodistuksesta ja 3) biometriin tietoihin perustuva, eli sormenjälki, kasvojen piirteet tai sykkeen tunnistus (EKG). Monivaiheisen tunnistuksen käyttö sisäänkirjautumisessa pitäisi aina yrityksen koosta tai toimialasta riippumatta olla laajalti käytössä. Se on tutkimusten valossa kuitenkin käytössä vasta vain reilulla puolella yrityksistä (Andreev ym, 2018).

Päätelaitteiden tunnistus ja käsittely (Endpoint detection & response; EDR) on yksi oleellisimmista hallinnollisista työkaluista kyberturvallisuuden ylläpitämiseksi. Se suojaaa yritystä haittaohjelmilta ja hyökkäyksiltä ja sen avulla valvotaan jatkuvasti päätelaitteita kuten yrityksen palvelimia, tietokoneita ja puhelimia. Tarkoituksena ei ole kuitenkaan vakoilla ja vahtia työntekijöiden omia tekemisiä, vaan suojata laitteita ulkoisilta verkon kyberriskeiltä. Uhan havaitessaan EDR muodostaa hälytyksen ja mahdollistaa nopean reagoinnin. Järjestelmä saattaa myös mahdollistaa tietyn päätelaitteen

eristämisen verkosta tarvittaessa (Adarsh & Greeshma, 2023). Kuvainnollisesti se toimii kuin toimiston automaattinen valvontakamerajärjestelmä; luo näkyvyyttä IT-infraan ja muodostamalla automaattiset hälytykset se mahdollistaa nopean reagoinnin uhkiin.

Varmuuskopiointi tarkoittaa tietojen kopiointia erilliseen paikkaan turvaan, jotta tärkeät tiedot voidaan palauttaa, mikäli alkuperäiset tiedot katoavat tai vahingoittavat. Käytännössä jokaisella yrityksellä on liiketoiminnan kannalta kriittisiä tietoja digitaalisessa muodossa, useissa tilanteissa tietyt tiedot ovat jopa elinehto bisnekselle, ja niiden puuttuminen voi aiheuttaa massiivisia taloudellisia kustannuksia. Siksi varmuuskopiointi on vakuuttajien silmissä kriittistä, ja siksi varmuuskopioinnin automatisointi ja säännöllinen testaaminen on myös tärkeää. Todistettavat varmuuskopiot myös lisäävät yrityksen uskottavuutta (Kyberturvallisuuskeskus, 2020). Varmuuskopiointiin liittyy nyrkkisääntö nimeltä ”3-2-1 -sääntö”, joka tarkoittaa että olisi suositeltavaa kopioida alkuperäisen lisäksi tuplakopio, säilyttää tiedostoja vähintään kahdella eri tallennusvälineellä (esim. pilvipalvelu + kovalevy) ja vähintään yksi kopioista tulisi olla kokonaan erillään verkosta vaikka ulkoisella kovalevyllä. Lisäturvaa tuo varmuuskopion salaus, etenkin jos ne sisältävät yrityksen kannalta arkaluonteista materiaalia (Limnell ym., 2014).

Pääsynhallinnalla tarkoitetaan prosessia, jossa hallitaan käyttäjien pääsyä yrityksen järjestelmiin ja tietoihin. Erityisen oleellista on hallita ja valvoa yrityksen kriittisten IT-resurssien käyttöä eli niin kutsuttuja erityisoikeudellista käyttöä (Privileged access management; PAM). Näihin ei lähtökohtaisesti ole hyvä olla pääsyä kuin vain niillä henkilöillä, joille se on välttämättömyys, sillä järjestelmänvalvojilla on oikeudet muokata koko infrastruktuuria. Mikäli kyberhyökkääjä pääsee käsiksi ylläpito-oikeuksiin, voi lasku olla valtaisa. Myöskään inhimillisten vahinkojen mahdollisuutta ei ole syytä jättää huomiotta, jonka takia niin kutsuttu nollaluottamusmalli (Zero trust - tietoturvamalli) onkin yleistynyt kyberturvallisuuden osalta edistyksellisissä yrityksissä. Tietoturvamallin mukaan kukaan tai mikään ei ole automaattisesti luotettava, vaikka se olisi organisaation sisäinen toimija, vaan kaikki kirjautumiset tunnistetaan ja vahvistetaan (Adarsh & Greeshma, 2023).

Suodatinohjelmat ovat monelle tuttuja jo perustason sähköpostipalveluista. Ilmaisten versioiden laatu tosin vaihtelee, mutta perusideana on suojata organisaatiota haitallisilta viesteiltä tai verkkosivustoilta (Adarsh & Greeshma, 2023). Harva yritys on varmaan tyystin kyennyt välttymään esimerkiksi toimitusjohtaja-huijausviesteiltä, joissa rikolliset pyrkivät esiintymään yrityksen johtajana ja pyytämään esimerkiksi klikkaamaan virallisen näköiseksi naamioitua haitallista linkkiä.

Suodattimien tehtävä olisi pyrkiä tunnistamaan tämänkaltaisia viestejä, linkkejä ja sivustoja. Kuitenkin kyberrikollisetkin ovat ajan saatossa kehittyneet ja esimerkiksi tekoälyn laajempi käyttö on parantanut huijauksien laatua entisestään. Viesteissä saatetaan usein vedota tunteisiin tai kiireeseen, mikä voi lisätä inhimillisen virheen tekemisen riskiä. Lisäksi ulkomailta lähetettyjen suomenkielisten viestien laatu ja uskottavuus on parantunut (Kyberturvallisuuskeskus, 2020). Sähköpostihuijausyriksiä tapahtuu miljoonia vuosittain, ja niiden arvioidut kustannukset ovat miljardeissa. Keskimääräisen onnistuneen huijauksen kustannus oli viime vuonna 2023 globaalisti miltei viisi miljoonaa euroa (IBM, 2024). Koska kustannukset ja volyyymi ovat suuria, kiinnostaa roskaposti- ja verkkosuodatusohjelmiston käyttö tietysti myös kybervakuutusta myöntävää vakuuttajaa.

3.2 Kontrollivaatimusten merkitys

Tavallinen kotivakuutus kuluttajalle tai kiinteistövakuutus yritykselle voidaan myöntää hyvinkin minimaalisilla tiedoilla. Suurten lukujen lain mukaan asiakasmassan ollessa suuri, voidaan vakuutuksia myöntää matalammalla kynnyksellä ja jolloin varmistettuja kontrolleja ei tarvita niin paljon tarjouksen antamiseen. Kybervakuutuksen osalta jonkinlainen kontrollikartoitusta voidaan taas pitää välttämättömänä vakuutusyhtiön näkökulmasta. Kuten tässäkin tutkielmassa on useampaan kertaa käynyt ilmi; kyberriskit ovat haastavia. Ilman minkään taseisia kontrolleja, olisi vakuuttaminen käytännössä erityisen vaikeaa toteuttaa (If, 2024). Ilman kontrolleja vakuutusnottajat voisivat käytännössä saada minkälaisella vahinkohistorialla ja kyberturvallisuuden tasolla tahansa vakuutuksen, mikä tietenkään ei olisi pitkässä juoksussa muiden vakuutettujen etu.

Kuitenkin kyberriskien yhtenä erityispiirteenä voidaan pitää niiden arvaamattomuutta. Kybervahinkoja voi olla miltei mahdotonta ennustaa, vaikka historiatietoa olisikin riittämiin saatavilla. Tällaisia esimerkkejä riittää historiasta, kuten aiemmin mainittu NotPetya-hyökkäys. Vakuutusyhtiöt ovat kuitenkin pyrkineet pienentämään tätä ongelmaa riskikontrolleilla, sillä kiistämätöntä on korrelaatio hyvien kyberriskikontrollien sekä kyberriskien todennäköisyyden välillä. Esimerkiksi teknologiajätti Microsoftin oman datan perusteella jo pelkästään monivaiheinen tunnistus (MFA) vähentää jopa 99 prosenttia tunkeutumisyriksistä käyttäjän tilille (Maynes, 2019). Tästä syystä perusvaatimukset (kuvio 6 tummalla värjätty) ovat pitkälti samoja yhtiöstä riippumatta. Kuitenkin monella suuremmallakin yhtiöllä saattaa olla ongelmia täyttää perusvaatimuksia,

esimerkiksi arvioiden mukaan läheskään kaikissa yrityksissä MFA ei ole kustannustehokkuudestaan ja toimivuudestaan huolimatta aktiivisessa käytössä.

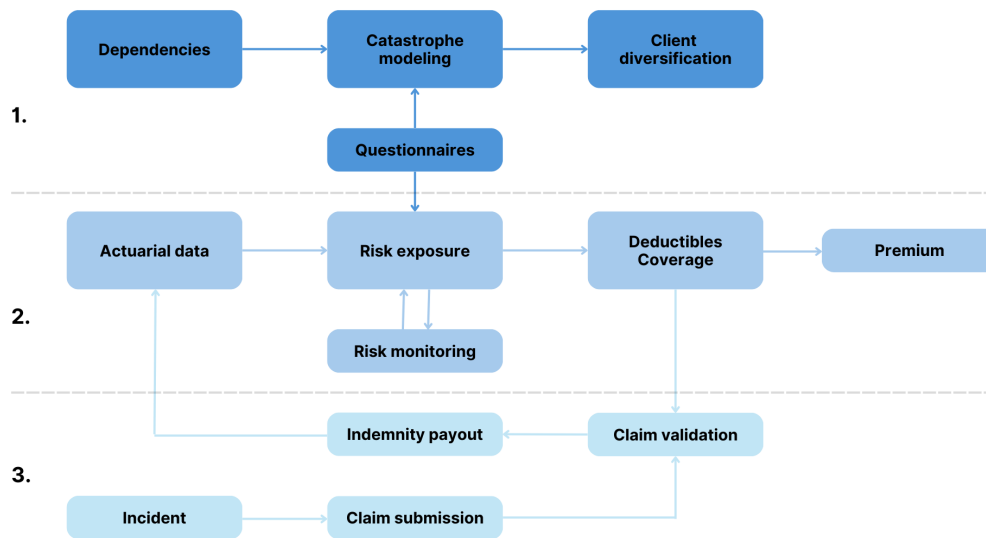
3.2.1 Vakuutusyhtiön näkökulmasta

Jotta vakuuttajan intressejä ja insentiivejä voidaan analysoida tarkemmin kontrollivaatimusten asettamisessa, paneudutaan tässä luvussa vielä kybervakuutusprosessiin vakuuttajan näkökulmasta. Kuvioista 7 on nähtävissä vakuuttamisprosessin eri vaiheita. Prosessi voidaan jakaa karkeasti kolmeen eri vaiheeseen: 1) riskin arviointi, 2) riskin rahoittaminen ja 3) riskin seuranta ja korvauskäsittely. Riskin arviointi liittyy vakuutusyhtiön tarpeeseen valikoida omaan riskiportfolioon oman strategiansa mukaisia riskejä. Vakuutusratkaisut lähtökohtaisesti laaditaan yrityskohtaisen riskiarvion pohjalta (Rantala & Kivisaari 2020, 423). Etenkin pienemmillä ja tiettyyn vakuutuslajiin erikoistuneilla yhtiöillä niin kutsuttu ”risk appetite” eli haluttu riskisegmentti voi olla hyvinkin suppea. Isoimmat yhtiöt taas ovat lähtökohtaisesti hyvinkin kaikkiruokaisia, eikä alkukarsinta perustietojen perusteella näyttele niin suurta roolia prosessissa. Toisaalta pienikin yhtiö voi olla sofistikoitunut tiettyyn riskilajiin ja he saattavat jopa tavoitella riskialttiimpia yrityksiä asiakkaisiksi (Ollila, 2024).

Riskien arviointiin kuuluu siis kokonaisvaltaisesti portfolion hallinta ja riskien seulominen sen perusteella. Vakuutusyhtiöllä on tietty strategia siitä, miten se haluaa omaa portfolioa rakentaa ja millaisia yrityksiä se haluaa sinne asiakkaisiksi. Lopulta kontrollivaatimukset ovat tämän strategian toteutuksen käytännön implementointia. Tekniikan kehittyessä skenaarioiden laskentajärjestelmät ja riskien mallinnus ovat pitkälle kehittyneitä. Kybervakuutuksen osalta tullaan kuitenkin taas sen erikoislaatuisuuteen; asiakkaiden välisiä riippuvuuksia on vaikea ennustaa. Kumuloituva riski ja niin kutsuttu kyberkatastrofiriski, jossa jokin kybervahinko leviää laajalle nopeasti kyberympäristössä ovat niitä pahimpia mahdollisia skenaarioita, joita vakuuttajat joutuvat ottamaan huomioon. Kybervakuutusportfolioa kasattaessa kerrannaisvaikutukset ovat erityisen tärkeitä. (Tsohou ym., 2023)

Kybervahingoissa voi tulla massiivisia vahinkoja yhdellä kertaa kuten vaikka luonnonkatastrofeissa, mutta toisin kuin luonnon kanssa – tuhot eivät korreloi välttämättä mitenkään maantieteellisesti. Arviointivaiheessa vakuuttaja pyrkii keräämään tarvitsemansa tiedot avoimista lähteistä ja asiakkaan täyttämistä hakulomakkeista – sekä tarvittaessa täydentämään täsmentävillä lisäkysymyksillä, esimerkiksi juuri toimialan tai henkilötietorekisterien perusteella (Tsohou ym., 2023). Toimialan lisäksi muita kriittisiä tietoja, mitä vakuuttaja yrityksen koosta riippumatta kaipaa

kybervakuuttamisen osalta, on pääsääntöisesti verkkotunnus, liikevaihto- ja henkilöstömäärä. Avoimista lähteistä saatava tieto voi olla muutakin kuin nettisivuihin päällisin puolin tutustumista. Vakuutusyhtiöt tekevät yhä enenevässä määrin erilaisia haavoittuvuusskannauksia kybervakuutusta hakeville yrityksille, joiden tarkoituksena on hankkia tietoa kriittisimmistä haavoittuvuuksista mihin hyökkääjät saattaisivat iskeä (Dambra ym., 2020).



Kuvio 7. Kybervakuuttamisprosessi jaoteltuna kolmeen osaan. (Dambra ym., 2020).

Riskin rahoittaminen tai underwriting on prosessin seuraava vaihe, jossa kaikkea kerättyä dataa pyritään hyödyntämään määriteltäessä vakuutus sopimuksen ehtoja sekä hintaa. Asiakkaalta kerätty data yhdistetään niin kutsuttuun vakuutusmatemaattiseen tietoon (actuarial data), jonka pohjalta sopimuksen tietoja arvioidaan. Nyrkkisääntö tietysti on, että vakuutusmaksujen avulla pystytään maksamaan tulevat vahingot sekä liiketoiminnasta aiheutuneet kulut ja päälle jää vielä palkkio riskistä eli vakuutustekninen kate (Dambra ym., 2020). Kyberriskeissä yksi haastavimmista asioista on arvioida tulevien vahinkojen määrää. Vaikka isossa kuvassa kybervahingot ovat kasvaneet vuosittain suhteellisen tasaisesti, on yksittäisissä vuosissa suuriakin vaihteluja, mitkä voivat käydä vakuutusyhtiöille kalliiksi. Lisäksi kybervakuutusta varten kerättävät tiedot ja sopiva kontrollien vaatimustaso ovat vaihdelleet paljon niin eri yhtiöiden välillä ja kuin myös yhtiön sisäisesti vuosien mittaa. Syy on yksinkertainen: aktuaarista dataa on hyvin niukasti saatavilla, eikä konsensusta siitä, mikä olisi sopiva taso ole löytynyt (Dambra ym., 2020). Näin ei myöskään tapahdu välttämättä aivan heti, sillä muutos on niin tiuhaa digitalisaation ja sen uusien ilmiöiden myötä, että tasapainoa joudutaan todennäköisesti vielä vuosia etsimään, jos löytämään koskaan. Prosessin lopuksi, kun vakuuttaja on mielestään saanut tarvittavan informaation kerättyä ja on tyytyväinen asiakkaan

kontrollitasoon, se tarjoaa vakuutussopimusta, jonka hyväksytyään asiakkaalle astuu kybervakuutus voimaan.

Kuten yritykset tavallisestikin, myös vakuutusyhtiöt ovat yksilöllisiä ja vaikka niitä koskee finanssialalle tyypillinen tiukat regulaatiot ja riskienhallintavaatimukset (Sibakov, 2020), voivat vakuuttajat pitkälti itse määritellä kontrollitason, jonka se haluaa asiakasyrityksen vahvistavan ennen kybervakuutuksen myöntämistä. Kontrollit ovat kehittyneet läpi kybervakuuttamisen lyhyen historian, ja vakuutusyhtiöt ovat myös käytännön kokeiluillaan pyrkineet löytämään optimitasoa kybervakuutuksille vaadittavista turvallisuuskontrolleista. Tasapaino täytyy löytää sen välille, kuinka paljon kontrolleja voidaan vaatia, ilman että se käy liian raskaaksi tai kalliiksi asiakkaalle ja kiinnostus kybervakuutusta kohtaan ei katoa. Vakuuttajat ovat keskittyneet pk-yritysten osalta teknisiin kontrolleihin. Tämä johtuu etenkin siitä, että hallinnollisia kontrolleja on vaikeampi mitata etenkin kustannustehokkaasti, vaikkakin ne ovat yhtä tärkeitä kuin tekniset kontrollit (Hoppe & ym., 2021).

Vaarana vakuutusyhtiöiden näkökulmasta on se, että potentiaaliset asiakkaat kokevat järkevämmäksi sijoittaa vakuutukseen menevät rahat omaan kyberturvallisuuden tason parantamiseen vakuutuksen sijasta. Tätä on myös tutkittu jonkun verran, ja yksi selvä havainto on se, ettei kybervakuutus toimi aidosti kannustimena panostaa kyberturvallisuuteen, jos sellainen nykyisellä kontrollitasolla myönnetään. Tutkimuksen mukaan insentiivi muodostuu ainoastaan silloin, mikäli kybervakuutusmaksusta on saatavilla alennusta parantamalla omaa kyberturvaa ja se on suorien kustannusten valossa kannattavaa (Marotta ym., 2017). Tämä toki ei ole poissuljettu tilanne, sillä vakuuttaja saattaa alentaa vakuutuksen hintaa, mikäli yritys parantaa omaa kyberturvallisuuden tasoa merkittävästi. Joka tapauksessa vakuuttajien vastuulla on viestiä siitä, miten vakuuttaminen ja muu riskienhallinta kuten omasuoja eivät ole vaihtoehtoisia menetelmiä, vaan ne täydentävät toisiaan, etenkin kyberriskien dynaamisen luonteen vuoksi.

Kysymys siitä, missä menee tasapaino kohtuullisen kontrollivaatimustason kanssa, on tutkimuksen punainen lanka. Helppoa tai suoraa vastausta siihen ei luonnollisesti löydy, mutta vakuuttajien tekemät muutokset markkinavaatimusten mukana antavat jonkinlaista osviittaa. Teknologian jatkuva kehittyminen ja tekoälyn tuleminen mukaan yhtälöön tuo vielä oman mausteensa. Pohjoismaiden suurin vahinkovakuuttaja If arvioi, että CIS:n viisi ensimmäistä (kuvio 10) kyberriskikontrollia pienentää kyberhyökkäyksen todennäköisyyttä jopa 85 %:a. Samalla If kuitenkin myös muistuttaa, etteivät kontrollit ole kertaluonteisia hankintaprojekteja, vaan niitä täytyy olla jatkuvasti parantamassa ja kehittämässä (If, 2024). Sveitsiläinen vakuuttaja Zurich arvioi puolestaan omassa

tutkimuksessaan hieman maltillisemmin, että viiden kontrollin implementointi laskee todennäköisyyttä 66 prosenttia ja kymmenen kriittisintä kontrollia vähentää hyökkäyksiä 70 prosenttia (Zurich, 2023).

Tekoäly ja jatkuvasti kehittyvät työkalut helpottavat vakuuttajien näkökulmasta kokonaisvaltaista kyberriskien arviointia ja tärkeimpien kontrollien analysointia. Etenkin kyberriskien osalta, kun aikaisempaa historiadataa ei ole laajalti käytettävissä nousee tekoälyllä toteutettava mallintamisen merkitys (Giudici & Raffinetti, 2022). Euroopassa saatavilla olevaa dataa on vielä vähemmän saatavilla tiukempien datankäsittelylakien johdosta, kuin vaikkapa Yhdysvalloissa. Tämän taustalla on Yhdysvaltojen markkinan koko: se edustaa yksin miltei puolia koko globaalista kybervakuutusmarkkinasta (Kshetri, 2021). Haasteena on myös tietysti keinoälyn tuottaman arvion luotettava varmentaminen, sekä menneeseen tietoon perustuva arvio tulevasta. Edes edelliset viisi vuotta eivät välttämättä kerro miten kyberriskit käyttäytyvät seuraavan vuonna, jota taas vakuuttajat pyrkivät vakuutuskautta laskelmoitaessa arvioimaan. Joka tapauksessa merkittävää edistystä työkalut ovat tuoneet, joista osoituksena on useampien vakuuttajien siirtyminen kybervakuutusten myöntämisessä suoraviivaistettuun prosessiin, jossa pitkiä paperilomakkeita on korvattu haavoittuvuusskannauksilla ja kehittyneillä analytiikkatyökaluilla (Biener ym. 2015).

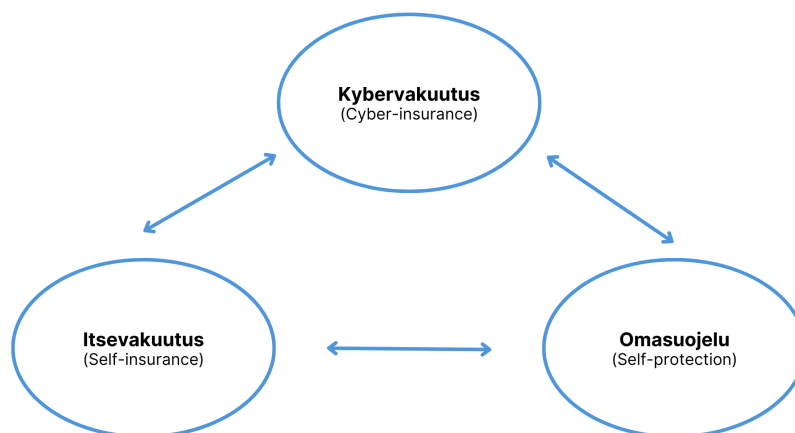
3.2.2 Pk-yrityksen näkökulmasta

Kontrollivaatimuksien kaksiteräinen luonne tarkoittaa sitä, että samalla kun vakuuttaja saa varmuuden tarkemmasta kyberriskitasosta ja mahdollisista voimassa olevista uhista, niin myös asiakkaat joutuvat käymään läpi oman kyberturvallisuustason keskeisiä elementtejä. Asiakkaan näkökulmasta kontrollivaatimukset saattavat mahdollisesti parantamaan näitä keskeisiä elementtejä sekä parhaimmassa tapauksessa lisätä mahdollisista keinoista ja käytännöistä, joilla he voisi vielä parantaa omaa kyberturvaa. Pk-yritykset saattavat kokea vakuutukset riesana ja pelkästään ylimääräisenä liiketoiminnan kuluna, mutta todellisuudessa vakuuttajien asettamat kontrollivaatimuksetkin ajavat parhaillaan molempien osapuolten etua. Molemmilla on halu pienentää kyberriskiä, ja lisäksi vakuuttajalla on tahto selvittää merkittävimmät haavoittuvuudet yrityksen kyberturvassa, mikä on samalla hyvää riskienhallintaa yritykselle (If, 2024).

Vaikka etenkin matalamman riskin alojen yhtiöiden kohdalla puhutaan usein ainoastaan perustason vaatimuksista, voi vakuuttamisprosessi olla monelle yritykselle ensimmäinen kerta, kun se joutuu kunnolla miettimään omia käytössä olevia kontrollejaan kyberriskejä vastaan. Vaikka

ideaalitulanteessa jokainen yritys olisi perillä omista kontroleistaan, todellisuudessa näin ei kuitenkaan ole. Monet suuremmat sekä myös pk-yritykset ovat ulkoistaneet omia tietoturvatehtäviä, eikä tiedonkulku ole IT-osaston ja johtoryhmän välillä välttämättä aukotonta. Toisaalta vakuutusyhtiöt saattavat myös tehdä virheellisiä oletuksia yhtiön liiketoiminnasta ja siihen kohdistuvista riskeistä, jolloin vaaditut kontrollit eivät sovellu täysin asiakasyrityksen liiketoimintaan. Lähtökohtaisesti yritys tuntee aina itse parhaiten oman liiketoiminnan ja siihen liittyvät riskit, jokainen riski kun on kuitenkin yksilöllinen (Juvonen, ym., 2014).

Yrityksellä on kolme pääkeinoa hallita kyberriskejään: omasuojelu, itsevakuuttaminen ja tavallinen vakuuttaminen (kts. kuvio 8). Yrityksen tekemiä parannuksia omaan kyberturvallisuuteensa kutsutaan yleisesti omasuojeluksi (self-protection). Käytännössä ne ovat samoja toimenpiteitä kuin vakuutusyhtiöiden arvioimat kyberriskikontrollit; niiden tarkoitus on parantaa organisaation kyberturvallisuutta ja valmiutta reagoida riskeihin. Varmuuskopioiden salaaminen ja henkilöstön kybertietoisuuden parantaminen ovat esimerkkejä omasuojelusta. Itsevakuuttaminen (self-insurance) ei varsinaisesti ole vakuuttamista, sillä siihen ei liity vakuutussopimusta tai kolmatta osapuolta, joka kantaisi vakuutettavan riskin. Itsevakuuttaminen sisältää kuitenkin elementin riskin rahoittamisesta, sillä siinä yritys itse rahoittaa tiettyä riskiä rahastoimalla sitä varten omaisuutta. Oleellista on kuitenkin tällöin tehdä huolelliset arviot mahdollisista vahingon aiheuttamista kustannuksista, jotta rahastoidut varat varmasti riittävät sen kattamiseen ja liiketoiminnan varmistamiseen. Kolmantena keinona on kybervakuuttamisen hankkiminen vakuutusmarkkinoilta. Nämä kolme vaihtoehtoa eivät toki ole poissulkevia, vaan päinvastoin laajimmissa tapauksissa yritys soveltaa riskienhallinnassaan kaikkia kolmea keinoa (Toregas & Zahn, 2014). Omasuojelu on välttämätöntä vakuuttamisesta huolimatta, ja toki kontrollivaatimusten tehtävä on sitä vaatiakin. Vakuutettavissa olevat riskit voidaan luonnollisesti sitten vakuuttaa kybervakuutuksella.



Kuvio 8. Kyberriskin hallintakeinot kolmijaoteltuna (Toregas & Zahn, 2014).

3.2 Kontrollivaatimukset osana riskienhallintaa

On tärkeää huomioida, että vaikka kybermaailma ja sen riskit saattavat äkkiseltään tuntua erillisiltä muusta todellisuudesta, ovat ne kietoutuneet hyvin tiiviisti toisiinsa. Tämä tarkoittaa sitä, että myöskin kontrollit liittyvät yrityksen muuhun kokonaisvaltaiseen riskienhallintaan. Jos yritys ei tätä aktiivisesti tiedosta, ei integraatio ole varmasti niin hyvällä tasolla kuin se voisi olla. Otetaan esimerkkitapaukseksi henkilöstön säännöllinen koulutus. Toivottavaahan olisi, että henkilöstöä koulutettaisiin muutoinkin säännöllisesti, jolloin kyberturvallisuuteen liittyvät teemat integroituisivat näihin koulutuksiin. Tämä on esimerkki hallinnollisesta kontrollista. Toisena esimerkkinä voimme ottaa säännöllisen varmuuskopioinnin, joka edustaa puolestaan teknistä kontrollia. Mikäli yritys hoitaa ja päivittää muuten tietojansa säännöllisesti ja kurinalaisesti, ei tarvittava varmuuskopiointi varmasti tuota päänvaivaa. Mutta taas toisinpäin ajateltuna, mikäli nämä asiat eivät yrityksen toimintatavoissa, voi vakuuttajan määräämiä kontrolleja olla haastava toteuttaa, sillä kuten todettua, eivät ne ole erillisiä asiakokonaisuuksia. Tässä tullaan siis yrityksen sisäiseen kulttuuriin, mikä onkin ehkä yksi tärkeimmistä seikoista liittyen kyberturvallisuuden ylläpitoon ja kehittämiseen (Roth & Wesley, 2024). Harva yritys on onnistunut nykypäivänä nostamaan kyberturvallisuutta keskeisten teemojen joukkoon, etenkin IT-alan ulkopuolella (Ollila, 2024).

Kontrollien onnistunut implementointi vaatii myös onnistunutta johtamistyötä organisaatiossa. Kuten edellisessä kappaleessa käsiteltiin, kulttuuri ja henkilöstön osallistaminen ovat avainasemassa riskikontrollien johtamisessa ja hallitsemisessa. Johtaminen on jatkuvaa jalkatyötä arjessa, ja kontrollit eivät myöskään toimi ”hanki ja unohda” periaatteella, vaan ne vaativat jatkuvaa aktiivisuutta ja seurantaa. Kontrollien tehtävä ei ole ainoastaan laittaa puolustusta kuntoon ja passiivisesti odottaa riskien mahdollista realisoitumista, vaan toimia aktiivisesti kyberriskien hallitsemiseksi ja estämiseksi (Roth & Wesley, 2024). Selkeä käytännön haaste riskienhallinnan osalta on myös se, että kyberturvallisuuden ollessa monille pk-yrityksille uusi tema ja etenkin kun kybervakuuttaminen on Suomessa noin kymmenen vuotta vanha ilmiö, niin väkisin osaamisvajetta tämän tiimoilta on päätöksiä tekevässä johtajamassassa. Riskikontrollien tärkeys ja niiden onnistunut integrointi osaksi kokonaisvaltaista riskienhallintaa voikin vaatia tulokkausta ja ”myyntityötä” IT-osastolta, jolla on usein paras ymmärrys teknisestä puolesta. Haastetta toki lisää kyberriskien kompleksisuus, eli pelkkä tekninen osaaminen ja riskien kontrollointi ei riitä, vaan yritysten tulee myös arvioida niiden vaikutuksia talouteen ja liiketoiminnan jatkuvuuteen (Hiscox, 2022).

3.3 Resurssi- ja kustannusvaatimukset

Arvioidaan tässä kappaleessa aikaisemmin läpikäytyjen oleellisempien kontrollivaatimusten aiheuttamaa kustannustasoa ja resurssivaadetta yrityksille. Oleellista on se, että riskienhallinnassa otetaan aina huomioon siitä aiheutuvat kustannukset, joita verrataan toimenpiteistä saatavaan hyötyyn. Kustannuslähtöisyys on oleellista sekä budjetoinnin, että resursoinnin kannalta, mutta ennen kaikkea se on tuoton maksimoinnin kannalta oleellista, mikä tietysti on kaiken liiketoiminnan peruseriaate. ROI eli sijoitetun pääoman tuottoaste on laajalti käytetty mittari. Kyberturvallisuuden kontekstissa vastaava mittari olisi turvallisuusinvestoinnin tuottoaste ROSI (return on security investment, kuvio 9). Kaavassa ALE (annual loss expectancy) kuvaa arviota vuosittaisesta kybervahingosta aiheutunutta tappiota ja investoinnin kustannukset kuvaavat sitä rahamäärää, joka kuluu kyseisen kyberturvallisuutta parantavan työkalun tai toimenpiteen käyttöönottoon ja ylläpitoon. (Schatz & Bashroush, 2017).

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

Kuvio 9: Turvallisuusinvestoinnin tuottokaava, jonka avulla yritys voi arvioida investointien kannattavuutta (Schatz & Bashroush, 2017).

Käytännön esimerkkinä voidaan teoreettisesti ajatella, että arvioitu vuosittainen kustannus (ALE) lasketaan vuosittaisen esiintymisasteen ARO:n (Annualized rate of occurrence) ja yksittäisen vahingon odotusarvon SLE:n (Single loss expectancy) tulosta. Eli esimerkkinä Britanniassa on tietojenkalastelun (phishing) osalta arvioitu kustannus kolme tuhatta puntaa eli noin 3500 euroa. Brittiläisten viranomaisten selvityksen mukaan vuonna 2023 22 %:a yrityksistä joutui tietojenkalastelun uhriksi (GOV.UK, 2024). Voidaan pyöristää tämä esiintymisaste (ARO) 0,2 tarkkuuteen, mikä on myös hyvin yleisesti käytetty työluku kyberturvallisuudessa puhuttaessa. Käytännössä tuo luku tarkoittaisi, että todennäköisyyksien valossa yritys joutuu kerran viiteen vuoteen tietojenkalastelun kohteeksi. Valitaan esimerkkilaskelman investoinniksi monivaiheinen tunnistautuminen (MFA), jota pidetään nykypäivänä niin kybervakuuttamisen osalta kuin muutoinkin kyberturvallisuuden osalta perusvaatimuksena yritykselle kuin yritykselle, ja se on hyvin usein kybervakuutuksen pakollisena kontrollivaatimuksena. Lisäksi sitä pidetään tehokkaana kontrollina nimenomaan tietojenkalastelua (phishing) silmällä pitäen. Esimerkkinä Microsoftin Entra MFA maksaa kuusi euroa per käyttäjä, eli kymmenen hengen yrityksessä esimerkiksi noin 60 euron vuosikustannuksesta. Tällöin ALE ilman investointia olisi 700 euroa ja investoinnin kanssa 7 euroa,

joten ROSI olisi 10,55%, mitä voidaan pitää hyvänä tuloksena. Usein yrityksillä on joka tapauksessa Microsoftin tilin ostettuna työntekijälle, jolloin monivaiheinen tunnistus ei aiheuta ylimääräistä suoraa kuluja ja ROSI olisi tietysti korkeampi (Maynes, 2019).

Kyseessä oli tietysti ainoastaan hieman kömpelö ja teoreettinen esimerkkilaskelma, käytännössä arvoja on huomattavasti vaikeampi laskea tietyn yrityksen osalta, ja yhä vaikeammaksi tilanne menee, kun aletaan lisäämään yhtälöön sitä lisävaivaa ja kompleksisuutta, mitä useat päällekkäiset kontrollit voivat työntekijöille aiheuttaa. Haastetta lisää myös kyberriskien väistämätön jäännösriski; vaikka organisaatio varustautuisi kaikilla mahdollisilla kontrolleilla, jää aina mahdollisuus kybervahingolle. Lisäksi kontrollit ensisijaisesti pienentävät riskin tapahtuman todennäköisyyttä, eivät niinkään sen aiheuttamaa vaikuttavuutta organisaatiolle (Uganbayar, ym., 2021). Esimerkiksi: monivaiheinen kirjautuminen (MFA) hankaloittaa kyllä tietojenkalastelijan pääsyä yrityksen järjestelmään, mutta mikäli ohitus onnistuu, ei kyseinen kontrolli pienennä lainkaan vahingon määrää tai vakavuutta. Toki yrityksellä olisi hyvä olla useampi kontrollikerros, mutta ydinhaaste onkin määritellä, missä menee raja, jolloin kontrollit ovat ”riittävällä tasolla” kokonaisvaltaisen riskienhallinnan kannalta. Kontrollien kasaantuessa työntekijöiden käyttömukavuus rajoittuu, jonka lisäksi uusista kontrolleista saatava hyöty saturoituu eli saatava lisähyöty pienenee. Tähän syitä ovat kompleksisuuden lisäksi muun muassa investointien laskeva rajahyöty eli suhteellisesti pienempi tuotto sekä resurssivaje henkilöstön osalta etenkin pienemmän kokoluokan yrityksissä, eli vaikkapa koulutuksen puute voi hukata merkittävästi kontrollin potentiaalia. (Bohara ym., 2023).

Optimitasoa riittävään määrään kontrolleja ja vakuutusuojan välillä on myös tieteellisesti pyritty laskemaan useissa tutkimuksissa. Italialaisten suorittamassa tutkimuksessa rakennettiin algoritmi, jonka avulla voitiin riskiarvoja, tehokkaimpia kontrolleja ja kustannustasoja hyödyntämällä laskea paras mahdollinen optimitaso kontrolleihin satsaamiselle (Uganbayar, ym., 2021). Kärjistetysti tutkimustulos oli, että yksinkertaisessa esimerkkilaskelmassa suunnilleen puolessa välissä kaikkia mahdollisia kontrolleja kulkee optimitaso. Tällaisten algoritmien haaste on pk-yrityksen kannalta se, ettei todellisia resursseja ole arvioida tällaisia lukuja, sillä jokaisen yrityksen täytyy oma analyysi tehdä yksilöllisestä riskipositiostaan. Siksi yksinkertaistavat standarditasot kontrolleille ovat hyviä ja helpottavat yritysten tarttumista käytännön toimiin teorian sijaan. Vakuuttajat voivat helpottaa urakkaa luomalla omia selkeitä vakioituja kontrollivaatimuksia, jolloin hahmottuisi selkeä vähimmäisvaatimustaso (kts. Marsh, 2020 ja If, 2024).

Kansainvälinen ja voittoa tavoittelematon kyberturvallisuuden organisaatio Center for Internet Security (CIS) tarjoaa turvallisuusohjeita ja standardeja tietoturvaraparennusten toteuttamiseksi erikokoisille yrityksille. Sen laskelmien mukaan 10–250 henkeä työllistävälle yritykselle keskimääräinen kustannus viidestä oleellisemmasta kontrollista (kuvio 10) olisi noin 25 tuhatta euroa, mikä on kohtuullinen summa ottaen huomioon ensimmäisten kontrollien merkittävän vaikutuksen (CIS, 2024). Yksittäisilläkin päätöksillä voi olla merkittävä vaikutus; Zurich esimerkiksi mainostaa, että pk-yritys voisi 10 000 dollarin kontrolli-investoinneilla heidän laskelmien mukaan vähentää kokonaisriskiä kiristysyökkäyksen osalta jopa puoleen (Zurich, 2024). Vertailun vuoksi Suomessa on suunnilleen yhteensä 20 tuhatta pk-yritystä, joiden vuosittaisen liikevaihdon keskiarvo on yhdeksän miljoonaa euroa (Suomen Yrittäjät, 2020). Tällöin vastaava investointi olisi siis noin 3%:a kokonaisliikevaihdosta, jota voidaan pitää kohtuullisena. Toisaalta kuten samassa tutkimuksessa ja muissakin lähteissä (kts. Shamma, 2018) todetaan, voi kriittisiä kyberriskikontroleja implementoida myös varsin alhaisella budjetilla. Ongelmaksi usein kuitenkin pk-yrityksen osalta tulee osaamisvaje – monesti yrityksissä ei ole omaa tietoturvaohjaajaa (CISO), ja tarvittava osaaminen esimerkiksi uusien kontrollien implementointiin joudutaan ostamaan ulkoistettuna palveluna, mikä nostaa kustannustasoa (Hoppe & ym., 2021).



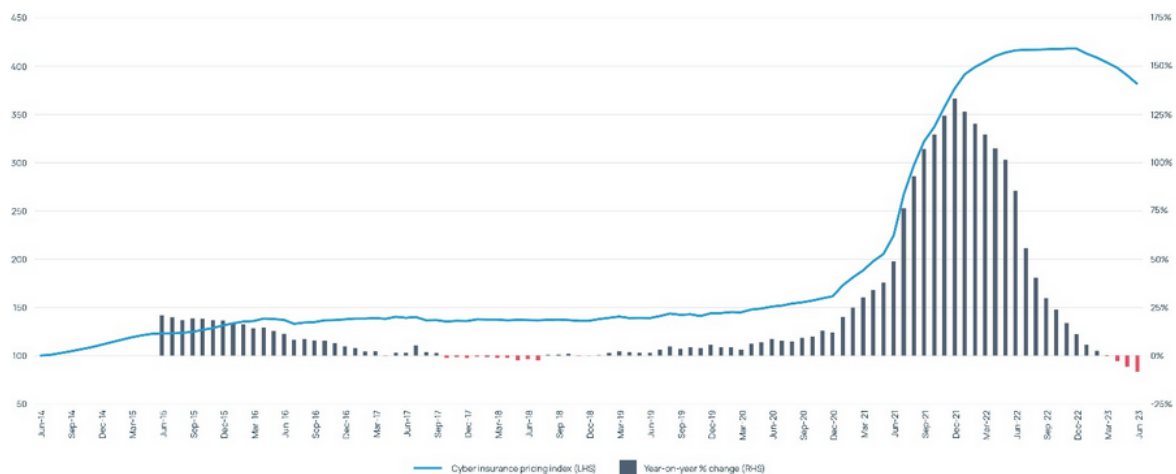
Kuvio 10. Center for Internet Security (CIS) 18 kontrollia kyberturvallisuuden parantamiseksi. (CIS, 2017).

Vaikka riskienhallinnassa on kyse muustakin kuin eurojen optimoinnista, ei niitäkään päätöksiä voi tehdä ilman, että tukena on arvio kustannusvaikutuksista ja mahdollisista vaihtoehtoiskustannuksista.

Riskienhallinnassa on kuitenkin aina huomioitava myös taloudelliset vaikutukset (Juvonen, ym., 2014). Tällaisesta tilanteesta oiva esimerkki on tilanne, jossa pöydällä on kaksi vaihtoehtoa: investointi omaan kyberturvallisuuteen tai saman rahan laittaminen vuosittain kybervakuutukseen. Myös muita vaihtoehtoja on kuten itsevakuuttaminen eli oman ”vakuutuskassan” ylläpito tai captive-yhtiön perustaminen vakuuttamisen näkökulmasta. Nämä ovat kuitenkin hyvin epäkäytännöllisiä ratkaisuja pk-sektorilla suurten pääomavaateiden vuoksi, joten keskitytään tässä tutkielmassa vain omasuojaan eli kyberturvallisuuden parantamiseen ja kybervakuuttamiseen.

3.4 Kontrollivaatimusten historia ja tulevaisuus

Kybervakuuttaminen on vakuutusmaailmassa uusi ilmiö, kymmenen vuotta on hyvin lyhyt aika vakuutusliiketoiminnassa. Euroopassa sitä on ollut laajalti saatavilla vakuutusmarkkinoilta vasta noin hieman yli kymmenen vuoden ajan (Granato & Polacek, 2019), mikä tarkoittaa, ettei ilman lastentauteja ole selvitty – myöskään nyt käsiteltävien kontrollivaatimusten osalta. Kontrollivaatimusten historiaa on mielekästä tarkastella kybervakuutusten markkinaliikkeiden mukaan. Alkuvuosina vakuutusta tarjosivat lähinnä siihen specialisoituneet vakuutusyhtiöt, joiden kontrollivaatimukset olivat suhteellisen minimalistisia, kuten perustason palomuuria ja tärkeimpien tietojen varmuuskopiointia. Kauppa kävi kuitenkin hyvin huonosti alkuvaiheilla, ja samaan aikaan kyberturvallisuus ja teknologia kehittyivät nopeasti, mikä tarkoitti laadukkaampia riskiarvioiteja ja pikkuhiljaa laajennettuja kontrollivaateita. Parantunut kyberturvallisuuden kypsyytaso sai hinnat myös hetkellisesti laskemaan vuosien 2017–2018 paikkeilla (Kuvio 11, Howden 2023), joskin trendi kääntyi rajusti pian sen jälkeen.



Kuvio 11. Kybervakuutusmarkkinan hintakehitystä 2014–2023. (Howden, 2023).

Tultaessa 2020-luvulle kyberrikollisuus oli ilmiönä alkanut ammattimaistumaan ja leviämään voimakkaammin. Koronapandemian puhjetessa loppuvuodesta 2019 myös kyberrikollisuus kiihtyi merkittävästi, mikä johtui osittain ihmisten siirtyessä järjestäen etätyöhön ja IT-infrastruktuurin ollessa siellä alttiimpaa hyökkäyksille. Suomessakin määrä miltei tuplaantui parissa vuodessa (Ali-Yrkkö ym., 2020), ja vakuutusten hinta reilusti yli tuplaantui (kuvio 9). Tahti kiihtyi Suomessa 2021, kun haittaohjelmat levisivät tehokkaasti, ja Kyberturvallisuuskeskukselle ilmoitetut hyökkäykset nelinkertaistuivat edellisvuoteen nähden (Traficom, 2024). Trendi oli vastaavanlainen maailmanlaajuisesti, mikä tarkoitti sitä, että pelkästään hinta ei noussut, vaan kontrollivaatimuksia nostettiin samalla merkittävästi, ja muutamasta perustason vaatimuksesta siirryttiin enimmillään jopa useiden satojen kysymysten hakemuslomakkeisiin. Vaatimukset kovenivat myös pk-sektorille merkittävästi. Kybervakuutusten hinnat lähtivät laskuun vasta vuoden 2023 lopulla, ja se on siitä lähtien tähän päivään tasaisesti laskenut 10–15 % vuodessa, tänä vuonna paikoitellen jopa hieman enemmän (Howden, 2023).

Kontrollivaatimusten kehitys on seurailut pitkälti markkinan kehitystä. Tämä on hyvin luonnollista, sillä mitä enemmän vahinkoja sattuu, sitä enemmän vakuuttajat haluavat pienentää portfolionsa riskitasoa. Iso syy sille, miksi kontrollit ovat höllentyneet aivan viime vuosina on nähtävissä myös vahinkotilastoista. Vuonna 2017–2020 oli pahoja kiristyshyökkäyksiä ympäri maailmaa, mikä aiheutti isoja vahinkopiikkejä ja sitä kautta kustannuspainetta vakuutusyhtiöille. Nyt viimeisen kahden vuoden aikana kiristyshaittaohjelmien takia maksetut korvaukset ovat vähentyneet selvästi, mikä on helpottanut vakuutusyhtiöiden painetta (McIntosh ym., 2024).

Samalla kun hinnat lähtivät laskuun markkinan ”pehmentyessä”, myös kontrollivaatimuksia kevenettiin, etenkin pk-yritysten osalta, joissa riski on helpommin hallittavissa, kun vakuutusmäärät ovat maltillisempia. Nykypäivänä kontrollivaatimukset ovat laskeneet tietyillä vakuuttajilla hyvinkin vähäisiksi, voi esimerkiksi olla, että pelkkä monivaiheinen tunnistus, erilliset varmuuskopiot ja EDR eli päätelaitteiden hallinta ja reagointi riittävät varmistamaan vakuutuksen hankkimisen. Tai kuten maailman suurimmalla vakuutusmeklarilla, yhdysvaltalaisella Marshilla, on näiden lisäksi vielä pakollisina kontrolleina sähköpostisuodatus ja ylläpitokäyttäjien pääsynhallinta (kuvio 4, Marsh Inc., 2020). Lontoosta kotoisin oleva CFC, jota pidetään kybervakuuttamisen edelläkävijänä etenkin pk-yritysten osalta, on siirtynyt jopa pienempien yritysten osalta siihen, että sitovan tarjouksen voi saada heidän tarjoamaltaan alustaltaan pelkästään yrityksen verkkotunnuksen perusteella (CFC, 2024), eli

vieläkin kevyemmin vaatimuksin. Joissain tapauksissa vakuutuksen voi saada myös ehdollisena, eli riittää, että tietyn aikajänteen sisällä huolehtii vakuuttajan vaatimat kontrollit käyttöön.

Kontrollivaatimusten tulevaisuus vaikuttaa mielenkiintoiselta. Toisaalta vakuutuskapasiteetin kasvaessa, uusien toimijoiden tullessa markkinoille ja kybervakuuttamisen tietoisuuden kasvamisen myötä kontrolleja halutaan keventää todennäköisesti entisestään, jotta vakuuttaminen olisi yhä useammalle yritykselle jatkossa mahdollista. Toisaalta kybervakuuttamisen yksi kulmakivistä on ollut vakuutusyhtiön aktiivinen rooli vahingon ehkäisijänä (Tsohou ym., 2023). Se on leimallista kybermaailmassa, sillä apua esimerkiksi poikkeamatilanteen selvittämiseen voidaan tarjota etänä pienemmillä kustannuksilla paljon helpommin kuin vaikkapa paloriskissä.

Vakuuttajien kontrollivaatimukset elävät siis jossain määrin markkinatilanteen kanssa samassa suhteessa ja niiden dynamiikka ei ole tehnyt kybervakuutuksen hankkimisesta pk-yritykselle volatiilin hintatason lisäksi liian yksinkertaista. Tulevaisuus näyttää kuitenkin mielenkiintoiselta; jatkuvasti kehittyvät skannaustyökalut niin ulkoisia kuin sisäisiäkin kyberriskejä varten tuovat vakuuttajille uusia mahdollisuuksia ymmärtää paremmin potentiaalisten asiakkaidensa kyberriskejä ja siten myös räätälöidä kontrollivaatimuksia tarkemmin (Giudici & Raffinetti, 2022). Tällöin etenkin pk-yritysten osalta, joilla ei itsellään yleensä ole paljon resursseja investoida omaan kyberriskien hallintaan, vakuuttaja kykenee omilla tehokkailla prosesseillaan kartoittamaan merkittävimmät riskit ja asettamaan niihin soveltuvat kontrollit. Skannauksessa ja analyysissa on kuitenkin itsessään omat riskinsä; vakuutusyhtiöille annettava data on tietysti äärimmäisen herkkää, sillä sen joutuessa kyberrikollisten käsiin heillä olisi eväät tehdä tarkasti kohdennettuja iskuja. Toisaalta se voi ohjata yritystä tekemään myös virheellisiä päätöksiä vakuuttajan pyytämänä, mikäli esimerkiksi haavoittuvuuksien analysoinnista saatava data ei ole syystä tai toisesta paikkansapitävää tai se perustuu pitkälti esimerkiksi eri toimialan saatavilla olevaan referenssidataan. Tällöin kontrollivaatimuksista voi pahimmillaan olla enemmän vain haittaa.

4 ASIANTUNTIJOIDEN NÄKÖKULMIA KYBERVAKUUTUSTEN KONTROLLIVAATIMUKSIIN

4.1 Aineiston keruu ja käsittely

Tutkielman empiriaosuudessa on tarkoitus syventää ymmärrystä teoriaosuuden pohjalta millaisia kontrollivaatimuksia vakuuttajat asettavat pk-yrityksille, miten ne vaikuttavat yritysten riskienhallintaan ja toisaalta myös millaisia mahdollisuuksia, haasteita ja tulevaisuudennäkymiä tähän liittyy. Empiriaosuutta ei ohjaa pelkästään teoria tai sen yleistettävyyden, päätavoitteena on oppiminen ja ymmärryksen lisääminen. Empiriaosuuden havaintoja ja tuloksia on tarkoitus verrata teoriaosuuden havaintoihin ja pyrkiä vertailun kautta vastaamaan tutkimuskysymyksiin mahdollisimman laadukkaasti. Kuten kvalitatiiviselle tutkimukselle on tyypillistä, tässäkin tutkielmassa on tarkoitus päästä ilmiön ”kuoren” alle kurkistamaan ja ymmärtämään sen toimintaperiaatteita.

Empiirinen aineisto on kerätty hyödyntäen laadullisia teemahaastatteluja. Ne ovat muodoltaan puolistrukturoituja, joten ne jättävät mahdollisuuksia laajentaa keskustelua haastattelun mukaisesti myös kysymysrunгон ulkopuolelle. Etenkin näin monipuolisessa kokonaisuudessa kuin kybervakuuttaminen ja niiden kontrollit, tarjoaa avoimempi haastattelumalli hyvän mahdollisuuden tarttua tutkimuskysymysten kannalta kaikista mielenkiintoisimpiin kohtiin tiettyä haastattelua mukaillen. Teemahaastatteluiden vahvuus tämän tutkielman osalta on myöskin niiden kyky korostaa ihmisten ja asioiden välisiä vuorovaikutussuhteita ja asioiden subjektiivisuuden merkitystä (Tuomi & Sarajärvi, 2018, 74). Haastatteluiden luontevalla dialogilla ja vuorovaikutteisella pyrittiin luomaan luottamusta ja luomaan mahdollisuudet asiantuntijoiden mahdollisimman autenttisille näkemyksille. Hirsjärven ja Hurmeen mukaan, kun tutkimuksen tavoitteena on saada selville ihmisten mielipiteitä ja käsityksiä ja sitä, miksi he ajattelevat tai toimivat juuri tietyllä tavalla, heidän kanssaan keskustelu on luonnollinen lähestymistapa (2022).

Tutkimusta varten haastateltiin kuutta kybervakuuttamisen asiantuntijaa, joilla uskottiin koulutuksen ja ammattinsa puolesta olevan riittävää asiantuntemusta ja näkemyksellisyyttä vastata haastattelurungon kysymyksiin. Laadullisessa tutkimuksessa haastatteluiden määrää tarkasteltaessa on oleellista pyrkiä arvioimaan niin kutsuttua saturaatiopistettä eli sitä tiedon kyllästymisen tasoa, jonka jälkeen uudet haastattelut eivät tuo enää relevanttia lisätietoa tutkimuksen tarkoituksen kannalta (Hirsjärvi & Hurme, 2022). Vaikka kuudessa haastattelussa täydellistä saturaatio ei vielä

luonnollisesti saavuteta, ilmeni tuloksista siitä huolimatta selkeää trendiä ja samankaltaisuuksia näkemyksissä, joiden pohjalta analyysia tutkimustuloksia varten voitiin rakentaa.

Haastattelut toteutettiin syksyn 2024 aikana videotapaamisten muodossa, jonka avulla ne myöskin tallennettiin ja litteroitiin. Haastatteluissa edettiin haastattelurungon mukaisesti (liite 1), mutta teemahaastatteluille ominaisesti osassa haastatteluissa keskustelu syveni tiettyjen aihealueiden osalta syvemmällekin. Kysymykset pyrittiin rakentamaan niin, että ne jättäisivät riittävästi tilaa asiantuntijan omille kokemuksilla ja näkemyksille. Kolmijakoisen haastattelun ensimmäisessä osassa käsiteltiin kontrollivaatimuksia yleisesti ja niiden nykytilaa, toisessa osiossa niiden merkitystä pk-yritysten riskienhallintaan ja viimeisessä osiossa käytiin läpi haasteita ja kehitysnäkymiä. Haastattelun teemat perustuivat suoraan kolmeen tutkimuskysymykseen, jotta tyypittely ja analysointi olisi aineiston pohjalta helpompaa. Haastatteluiden litterointi suoritettiin samana tai seuraavan päivänä haastattelusta, jotta välttyttäisiin mahdollisilta tulkintavirheiltä. Haastattelut kestivät keskimäärin noin 45-60 minuuttia ja jokaisen haastattelun aluksi käytiin lyhyesti käsiteltävää aihealuetta, tutkimuksen viitekehystä sekä asiaankuuluvat tietosuojaseikat läpi.

Asiantuntijoihin viitataan vastauksissa kirjaintunnuksilla A-F, jotta lukijan on helpompi seurata millaisella asiantuntemuksella ja taustalla mahdollisesti nostettu kommentti on annettu. Haastateltavista asiantuntijoista kaksi (A & B) toimii kybervakuutusmeklarina, yksi (C) toimii pk-yritysten kanssa töitä tekevänä kyberturvallisuusasiantuntijana ja loput kolme (D, E & F) suomalaisissa vakuutusyhtiöissä kybervakuuttamiseen erikoistuneina underwritereina. Molemmilla meklareilla on vankka kokemus kybervakuutusmarkkinasta sekä pienempien että suurempien yritysten parissa. Kyberturvallisuusasiantuntija on konsultoinut kyberturvallisuudesta vuosia sekä pk-yrityksiä, että suurempiakin yrityksiä, ja jolle myös kybervakuuttaminen on tuttu ilmiönä asiakastapausten kautta. Kaikilla vakuutusyhtiöiden underwritereilla on vuosien kokemus ja erikoistuminen kybervakuuttamisen osalta.

Aineiston käsittelyn osalta kvalitatiivisessa tutkimuksessa voi olla useita erilaisia lähestymistapoja. Se on kriittinen vaihe työn tieteellisen laadun kannalta, sillä järkevä ja onnistunut aineiston kokoaminen on hyvä tutkimuksen yleistettävyyden kriteeri (Eskola & Suoranta, 2014, 214). Laadullisen tutkimuksen aineiston käsittelyvaihe voidaan jakaa kolmeen osaan: ensiksi koko aineisto järjestetään esimerkiksi teemoittelemalla tai tyypittelemällä jollakin tavoin koherentiksi kokonaisuudeksi. Sen jälkeen aineisto täytyy analysoida (tässä tapauksessa sisällönanalyysillä) ja lopuksi analyysissä saatuja havaintoja tulkitaan ja vedetään yhteen (Eriksson & Koistinen, 2014).

Tässä tutkielmassa hyödynnettiin teoreettista viitekehystä alkuvaiheen aineiston tyypittelyyn. Tyypittely toteutettiin viitekehysten mukaisesti teemoittain, ja sen tarkoituksena on jakaa haastatteluaineistoa ominaisuuksien mukaan hallittavimpiin kokonaisuuksiin (Eskola ja Suoranta, 2014, 182). Samalla on hyvä muistaa, että koska tutkija käyttää empiriaosuuden aineistoa ajattelun ja tulkinnan apuvälineenä, on aineiston poimimisessa kyse aina tutkijan tulkinnoista ja omista päätelmistä (Eskola ja Suoranta, 2014, 147). Tulkintojen tueksi haastatteluista on poimittu sitaatteja. Sitaatit tuovat tekstiin myös moniäänisyyttä ja poistavat riskin näkemysten virheellisestä tulkinnasta.

Tyypittelyn jälkeen tutkielman empiria-aineisto analysoidaan sisällönanalyysin avulla. Sisällönanalyysi on yksi käytetyimmistä laadullisen tutkimuksen analyysimetoodeista, joka soveltuu erilaisiin aineistoihin kuten julkaistuun kirjallisuuteen ja haastatteluihin. Sisällönanalyysin pääpaino on aineiston sisällössä ja teemoissa (Tuomi & Sarajarvi, 2018, 105). Kuten alun tutkimusmenetelmäkappaleessa käytiin läpi, aineistoon käytetyn sisällönanalyysin lähtökohtana käytettiin teoriasidonnaista päättelyä, jossa hyödynnetään sekä teorialähtöistä että aineistolähtöistä päättelyä. Ero aineistolähtöisen ja teorialähtöisen analyysin välillä on se, että aineistolähtöisessä analyysissä teoreettiset käsitteet luodaan aineistosta, kun taas teorialähtöisessä käsitteet tuodaan valmiina olemassa olevasta tieteellisestä kirjallisuudesta. Sisällönanalyysissa tutkimusaineistosta luodaan kehys, jonka sisälle muodostetaan erilaisia kategorioita noudattaen määriteltyjä sisällönanalyysin perusteita (Tuomi & Sarajarvi, 2018, 107). Aineistosta poimitaan asiat, jotka kuuluvat aineiston analyysirunkoon ja tarvittaessa ulkopuolelle jäävistä asioista voidaan muodostaa omia kategorioitaan. Tarkoituksena on saada tutkittavasta ilmiöstä kuvaus tiiviissä ja yleistettävässä muodossa.

Sisällönanalyysin jälkeen on tulosten yhteenvedon aika, eli kerätyt havaintotyyppit ja kategoriat pyritään esittämään mahdollisimman selkeästi ja informatiivisesti. Käytännössä yhteenvedon tarkoituksena on vastata mahdollisimman täsmällisesti esitettyihin tutkimuskysymyksiin. Vertaillen empiriisiä havaintoja ja tuloksia tutkimuskysymyksiin suoritetaan abduktiivista päättelyä eli verrataan niitä myös teoriaosuuden havaintoihin suhteessa tutkimuskysymyksiin. Näiden yhteenvedon tulkintojen jälkeen on mahdollista muodostaa tutkimuksen johtopäätökset. Lisäksi arvioidaan myös analysoitujen tulosten ja muodostettujen johtopäätösten tieteellistä luotettavuutta ja merkityksellisyyttä. Arvioinnin avulla pyritään tarkastelemaan tulosten pätevyyttä ja tarjoamaan perustaa mahdollisille jatkotutkimuksille aiheesta.

4.2 Nykyiset kontrollivaatimukset pk-yrityksille

Asiantuntijoiden haastattelut aloitettiin kartoittamalla vapaamuotoisella keskustelulla haastateltavan taustaa ja kokemusta kyberturvallisuudesta ja kybervakuuttamisesta yleisesti. Alussa ennen varsinaisiin haastattelukysymyksiin siirtymistä kysyttiin jokaiselta haastateltavalta, miten he näkevät kybervakuuttamisen kontrollivaatimusten merkityksen ja miten he määrittelevät ne ylipäätään. Kaikilla vastaukset olivat tämän osalta hyvin samantyyllisiä, eli asiantuntijoiden mielestä niillä tarkoitetaan kybervakuuttajien asettamia vaatimuksia yritykselle, jotta he ovat riittävän tietoisia vakuuttamastaan riskistä ja uskaltavat kyseisen kyberriskin vakuuttaa. Suurin osa asiantuntijoista jakoi myös vaatimukset kahteen pääkategoriaan niiden luonteen perusteella; hallinnollisiin sekä teknisiin kontroleihin. Erot näiden välillä määriteltiin etenkin sen perusteella mihin osa-alueeseen ne kohdistuvat ja millä keinoin niitä käytännössä toteutetaan. Asiantuntijoiden näkökulmasta teknisen kontrollit painottuvat nimensä perusteella enemmän IT-infrastruktuuriin ja helposti mitattavissa oleviin kontroleihin, kuten pääsynhallinta tai monivaiheinen tunnistautuminen. Hallinnolliset kontrollit ovat enemmän johtamiseen ja prosesseihin liittyviä kontroleja. Asiantuntija A nostaa kuitenkin esiin, ettei jako ole selvästi täysin dikotominen, vaan ne menevät myös hieman lomittain. Hänen mukaansa organisaation kyberturvallisuudessa on aina enemmän tai vähemmän kyse prosesseista ja niiden toimivuudesta. Asiantuntija D kuvasi kahtiajakoa näin:

”Mun mielestä tekniset on helpommin kantifioitavia ja siksi myös vakuuttajien suosiossa, vaikka näkisin että hallinnolliset vähintään yhtä tärkeitä. Voi olla paperilla vaikka kuinka hyvät tekniset kontrollit, mutta jos luotettavat prosessit ja riittävä tietoisuus puuttuu niin ei niistä saada hyötyä irti. Hallinnollisissa on vaan juuri se haaste, että niitä ei ole välttämättä kovin helppoa arvioida”

Haastattelurungon ensimmäinen osuus koostui siis taustoittavista kysymyksistä liittyen yleisesti kontrollivaatimuksiin sekä miten ja millä perusteilla vakuuttajat niitä määrittelevät pk-sektorin asiakasyrityksille. Osion tarkoituksena oli kerätä aineistoa ensimmäiseen tutkimuskysymykseen eli millaisia kontrollivaatimuksia vakuuttajat ylipäätään asettavat pk-yrityksille. Teoriaosuuden perusteella lähtökohtainen oletus oli se, että kuten kybervakuutusten ehdot ja hintatasot, myös kontrollivaatimukset ovat pk-yrityksille hyvin standardoidut ja valmiiksi paketoit, eikä sen syvällisempää tai tarkempaa analyysia ja räätälöintiä juuri harjoiteta (Marotta ym., 2017). Vähimmäisvaatimukset ovat kuitenkin vaihdelleet voimakkaasti kybervakuutusten lyhyen historian aikana, joten tavoitteena oli parantaa ymmärrystä nykytilanteesta ja etenkin tulevaisuuden näkemyksistä; mihin vähimmäisvaatimusten taso tulee asettumaan.

4.2.1 Vähimmäisvaatimukset

Seuraavaksi keskusteltiin yleisesti pk-yrityksille asetettavista kontrollivaatimuksista ja samalla asiantuntijoilta kysyttiin, mitkä ovat keskeisimpiä eli niin sanottuja vähittäisvaatimuksia, joita ilman kybervakuutusta ei myönnetä. Tämä oli mielenkiintoinen kysymys, sillä usein esimerkiksi monivaiheista tunnistautumista pidetään vähimmäisvaatimuksena, mutta se on etenkin pk-sektorilla vielä suhteellisen alhaisella tasolla käytössä (Andreev ym, 2018). Yllättävää oli se, ettei kukaan asiantuntija pitänyt mitään kontrollivaatimusta ehdottomana, eli etteikö niitä ilman voitaisi myös arvioida vakuutettavuutta. Tämä oli selvästi poikkeavaa teoriaosuuden pohjalta. Useampi nosti esiin ehdolliset sopimukset, eli vaikei edes perustason vaatimukset olisi kunnossa, voidaan sopimus tehdä, kunhan asiakasyritys sitoutuu implementoimaan tietyt kontrollit sovitussa aikaraamissa.

Asiantuntija B:

”En ehkä sellasia ehdottomia minimivaatimuksia nää, mutta nythän enenevissä määrin näkyy sitä että okei voidaan myöntää vakuutus mutta pitää kuitenkin x ajan sisällä laittaa kontrollit kuntoon. Ja onhan siellä oltava jotain perustasoa, että jos ei yrityksellä ole oikeasti mitään kontrolleja niin vaikeehan sitä on vakuuttaa”.

Kysyttäessä perustason kontrolleja, eli mitä pk-yrityksille nykyisin yleensä esitetään, nousi pääosin vastauksissa samat kontrollit esiin; teknisistä kontrolleista monivaiheinen tunnistauminen, säännölliset varmuuskopiot ja käyttäjien pääsynhallinta sekä hallinnollisella puolella jonkinlainen poikkeamatilanteen suunnitelma (IRP) sekä henkilöstön kouluttaminen. Joitain yksittäisiä lisänostoja myös tuli kuten esimerkiksi Asiantuntija D korosti aktiivista yritystason palomuuria ja sen säännöllistä päivittämistä yrityksen koosta riippumatta. Nousseet vaatimukset olivat tulkintateorian kanssa samoilla linjoilla (kts. kuvio 5), mutta merkittävänä erona tosiaan kokonaistarkastelun korostuminen haastatteluissa. Tällä tarkoitan sitä, ettei mikään kontrolli ole yksittäisenä ehdoton vakuutettavuuden kannalta, vaan vakuutusyhtiötkin pyrkivät tarkastelemaan pk-yritystäkin isomassa kuvassa ja saamaan kontrollivaatimuksilla ja kartoitusvaiheella selville mikä on yleisesti organisaation kyberturvallisuuden kypsyystaso.

Asiantuntija F:

”Kyllä se on aina loppupeleissä kun riskiä arvioidaan niin kokonaisuudesta kyse. Eli mikäli siellä joku osa-alue laahaa perässä niin jos muuten asiat on ok-tasolla niin se kompensoituu. Mutta kokonaisuutta mä ainakin aina pyrin tarkastelemaan ja pyrin olemaan joustava että okei, jos toi

puuttuu niin se ei automaattisesti ole deal-breaker. Toki se kysymyksiä herää jos pienelläkin yrityksellä ei ole MFA:ta ja siellä vaikka tehdään paljon etäyhteyksien kautta töitä, niin ei se hyvää kuvaa anna turvallisuuden tasosta”.

4.2.2 Vakuuttajien painotukset ja muutosajurit

Seuraavaksi asiantuntijoilta kysyttiin kontrollivaatimusten asettamisen perusteita, eli mitä ominaisuuksia otetaan yrityksestä huomioon, kun sen kyberriskejä arvioidaan ja miten ne näkyvät asetettavissa vaatimuksissa. Vaikka lähtökohtaisesti kontrollivaatimukset asetetaan aina yhtiökohtaisesti, ovat pk-sektorin kybervakuutusten vuosimaksut sen verran maltillisia nykyisessä markkinassa, että yhtiöt ovat siirtyneet yhä enemmän standardivaatimukseen. Asiantuntija C toteaa, että jos puhutaan alle 200 miljoonan liikevaihdon yrityksistä, ovat esitettävät kysymykset ja vaateet yleensä hyvin standardeja, ellei liiketoiminnassa ole jotain spesifisti korostunutta kyberriskiä, esimerkiksi ohjelmistokehityksen myötä, jolloin vaatimukset hieman vaihtuvat mutta ovat tällöinkin yleensä vakioituneita. Haastatteluiden perusteella eniten vaatimukseen vaikuttaa juuri toimiala, mutta sen lisäksi arkaluonteisten tietojen määrä ja haettava vakuutusmäärä. Myös aiempi vahinkohistoria saattaa vaikuttaa kontrollivaatimukseen, asiantuntija E:

”Vahingot on tietysti yksi tekijä, ja sanoisin jopa, että pääsääntöisesti ihan hyvä asia. Jos yrityksellä on hyvät tiedot mitä on käynyt ja miten on toimittu sen jälkeen jotta ennaltaehkäistäisiin (vahinkoja) tulevaisuudessa. Toki jos mitään ei ole tehty niin sitten se on huono juttu, mutta sellaista mä en ole kyllä ikinä nähnyt, kyllä ne yritykset pääosin niistä vahingoista oppii ja riski pienenee vahingon myötä”

Kaikki nostivat myös liiketoiminnan piirteiden merkityksen, eli kontrollivaatimuksissa otetaan aina huomioon, vaikka kyseessä olisi pienikin yritys, millaista liiketoimintaa se harjoittaa ja mitä kyberriskejä juuri siihen liittyy. Vaikka yrityksen koko vaikuttaa luonnollisesti kyberriskin määrään, se ei poista sitä mahdollisuutta, että myös pienellä yrityksellä voisi olla suuri ja vaikeasta vakuutettava kyberriski (Marotta ym., 2017). Asiantuntija F esimerkiksi toteaa, että toimiala voi tuoda itsessään jo sellaisia riskejä, mitä on pakko ottaa huomioon asetettaessa kontrollivaatimuksia. Hän nostaa esimerkiksi terapiapalveluita tekevän pk-yrityksen, jolla voi olla valtavat määrät arkaluonteisia henkilötietoja tai vaikkapa pankkipalvelut, joihin saattaa kohdistua myös geopoliittisia kyberriskejä. Tällöin yritykseltä vaaditaan tiukempia kontrolleja.

Kaikki asiantuntijat nostivat esiin myös tuotannolliset yritykset, joissa nykypäivänä teknologian ja IT-järjestelmien rooli korostuu jatkuvasti. On hyvä muistaa, että suomalaisista pk-yrityksistä teollisuuden parissa työskentelee n. 10% yrityksistä (Suomen Yrittäjät, 2020), ja ne eivät ole mitenkään erityisasemassa kyberriskien osalta. Päinvastoin asiantuntija C korostaa, että tällaisissa yrityksissä usein kyberturvallisuuden taso on alhainen, mutta mikäli järjestelmä menee pois käytöstä kyberhyökkäyksen takia, ei tuotanto pyöri ja liiketoiminnan keskeytyksestä johtuva vahinko voi pian olla hyvinkin merkittävä yrityksen likviditeetin kannalta. Asiantuntija D nostaa samassa keskustelussa esiin myös rakennusalan yritykset, joissa liiketoiminta pyörii pitkälti usein nykypäivänä digitaalisen toiminnanohjausjärjestelmän avulla, ja mikäli sen käyttö sakkaa, saattaa tekeminen olla hyvin hidasta, ellei mahdotonta. Tästä syystä useampi asiantuntija korosti informaatioteknologian (IT) ja operatiivisen teknologian (OT) segmentoinnin eli eriyttämisen tärkeyttä, asiantuntija A:

”kyllä yrityksen koosta riippumatta jos siellä tuotantoa on, niin oleellista on IT:n ja OT-verkon eriyttäminen, jotta ei hyökkääjä ei pääse lateraalisesti liikkumaan järjestelmien välillä ja samalla kertaa tekemään vahinkoa molempiin verkkoihin ja pysäyttämään täysin liiketoimintaa”

Seuraavana haastatteluissa käsiteltiin kontrollivaatimusten muutosta viimeisen kymmenen vuoden aikana eli käytännössä sillä ajalla, kun kybervakuutuksia on Suomessa aktiivisesti ollut markkinoilla. Kaikki asiantuntijat korostivat markkinoiden volatilitteettia ja epäkypsyyttä, joka on näkyvissä myös kuviossa 10. Asiantuntijat E ja B korostivat vahinkokehityksen merkitystä vahvana muutosajurina vaatimusten muutoksissa. Muutkin nostivat esiin etenkin muutama vuosi sattuneen hintojen nopean nousun, mikä johtui kyberhyökkäysten ja vahinkojen nopeasta kasvusta. Asiantuntija E:n mukaan samalla myös kontrollivaatimukset tiukentuivat merkittävästi:

”kyllä ne kontrollivaatimukset vaan elää sen markkinan kilpailutilanteen mukaan aikalalla. Kun vakuuttajilla on kapasiteettia vähän ja kilpailua ei juuri ole, niin sitten vakuuttaja pyrkii pitämään sen oman portfolion mahdollisimman terveenä – ainakin niin, että riskitiedot ovat perusteellisia ja hinnoittelu on tarkkaa kontrollien mukaan.”

Tämä on siis nähtävissä käytännössä siten, että kun hieman ennen koronapandemiaa ja vuosikymmenen taitteen jälkeen hyökkäysten määrä räjähti moninkertaiseksi vuositasolla, vakuuttajat pyrkivät nopeasti reagoimaan tähän minimoimalla omaa riskipositiota tiukentamalla ehtorajauksia, nostamalla hintoja ja koventamalla kontrollivaatimuksia. Haastatellut asiantuntijat

nostivat esiin sen, miten vakiintuneet perustason kontrollivaatimuksetkin ovat muodostuneet sattuneiden kybervahinkoilmioiden kautta. Asiantuntija C korosti muun muassa sakkujen korostumisen keskustelussa EU:n tietosuojauudistuksen myötä vuonna 2018, mutta nykypäivänä keskustelun pyörivän enemmän keskeytysriskin ympärillä.

Asiantuntija B:

”Kyllä ne vähimmäisvaatimukset on vahinkojen kautta huomattu oleellisiksi. Esimerkiksi kun ransomware-aalto iski oisko ollut 2017 esim NotPetya ja WannaCry niin huomattiin mikä merkitys on toimivilla varmuuskopioilla ja sitä alettiin enemmän vaatia. Sitten kun esim korona-aikana ihmiset teki etäyhteyksillä töitä ja valvonta oli vähäisempää ja sattuu enemmän tietojenkalastelua niin ymmärrettiin viimeistään aktiivisen monivaiheisen tunnistautumisen kriittinen merkitys siinä”

Vahinkojen lisäksi yksi selvä muutosajuri vaatimuksien osalta on lainsäädäntö ja standardoidut sertifikaatit. Asiantuntija C on ollut mukana useissa auditoinneissa pk-sektorilla ja on huomannut, että ne ovat vaikuttaneet myös vakuutusyhtiöiden vaatimuksiin. Tämä on samassa linjassa teoriaosuudessa tehtyyn havaintoon standardien kuten ISO 27001 -tietoturvastandardin merkityksestä vakuuttajien laatiessa kontrollivaatimuksia (Marotta ym., 2017). Vaikka pk-yrityksille standardivaatimukset ovat harvinaisempia, ovat ne usein erityisesti tietyillä toimialoilla kuten finanssi- tai turvallisuusalalla nykyään yleisiä (Sibakov, 2020). Asiantuntija A huomioi vastauksessa myös lainsäädännön merkityksen muutoksiin:

”Tietyillä toimialoilla etenkin missä on kaikennäköisiä lainsäädännöllisiä vaatimuksia, esimerkiksi kriittisillä toimialoilla olevillehan tuli tänä syksynä NIS2-sääntely, niin kyllä niitä vakuutusyhtiöt tietysti seuraa ja huomioi omissa vaatimuksissa. Se katsotaan tietysti eduksi mutta onhan se välttämättömyydenkin samalla”

Yhteenvedon haastattelun ensimmäisessä osiossa käytiin siis yleisesti läpi kontrollivaatimukset pk-yrityksille sekä vaatimusten vähimmäistaso ja selvitettiin mitä osa-alueita vakuuttajat erityisesti painottavat vaatimuksia laatiessa ja miten ne ovat muuttuneet historian aikana. Muutoin haastatteluissa esiin nousseet vastaukset olivat pitkälti linjassa teoriaosuudessa tehtyjen havaintojen kanssa, mutta yllättävää oli se, ettei kukaan asiantuntijoista nähnyt ehdottomia kontrollivaatimuksia, vaan pk-yrityksiäkin lähestytään kokonaisharkinnan näkökulmasta. Haastatteluista kävi ilmi, että kysytyt kontrollit ovat olleet hyvin dynaamisia läpi historian, ja kaikki uumoilivat saman ilmiön jatkuvan, vaikkakin joitain aikaisemmin mainittuja kriittisimpiä kontrolleja onkin alkanut vakiintua

alalla. Asiantuntijat myös korostivat vuoropuhelua asiakkaiden kanssa riskienhallinnasta ja tietoisuuden kasvattamisesta, jotta kontrollivaatimukset eivät tulisi yllätyksenä ja niiden osalta oltaisiin paremmin varautuneita.

4.3 Vaatimusten merkitys yrityksen kyberturvallisuuden tasoon

Seuraavassa haastattelun vaiheessa siirryttiin tarkastelemaan vaatimusten merkitystä pk-yritysten näkökulmasta – miten ne ovat vaikuttaneet niiden riskienhallintaan ja toisaalta minkälainen rooli vakuutusyhtiöillä ja meklareilla ylipäätään on pk-yritysten kyberriskien hallinnan kehittämisessä ja tietoisuuden parantamisessa. Lisäksi selvitettiin, miten asiantuntijat näkevät vakuutusyhtiöiden roolin vakuutus sopimuksen solmimisen jälkeen ja ylipäätään yhteistyön pk-yrityksen kanssa hallittaessa kyberriskejä. Keskimmäisen osion lopuksi vielä pohdittiin, missä tilanteissa kontrollivaatimukset soveltuvat kaikista heikoiten, eli missä tilanteissa niistä ei ole juuri apua tai pahimmillaan haittaa.

Siitä asiantuntijat olivat kaikki samaa mieltä, että kontrollivaatimuksilla on aito merkitys ja vaikutus pk-luokan yrityksiin. Haastateltavat korostivat, että todellinen vaikutus riippuu paljon toimialasta ja yrityksestä itsestään. Asiantuntija F esimerkiksi nostaa esiin vakuuttajan ja vakuutettavan yhteisen intressin riskienhallinnasta; molemmilla on loppupeleissä halu pienentää yrityksen riskiä ja välttää taloudellisia tappioita. Tämä ei toki poista sitä seikkaa, etteikö näkemys eroja voisi olla siinä, millä tavoilla sitä toteutetaan ja kuinka paljon resursseja riskienhallintaan tulisi panostaa. Hyvä on myös huomioda, että Suomessa arvioiden mukaan ani harvoilla yrityksillä on kybervakuutusta (Ollila, 2024), mutta merkitys voi tulevaisuudessa toki kasvaa. Asiantuntija A näkee merkityksen riskienhallinnan osalta seuraavasti:

”Näkisin että se juuri näiden kontrollivaatimusten kautta se vaikutus tulee. Kyllä mitä itsekkin monien yritysten kanssa on ollut tekemisissä, niin moni joutuu kotiläksyjä tekemään kontrollivaatimuksiin törmätessään. Toisaalta se voi aiheuttaa turhautumista myös yrityksissä, mutta suurin osa on ottanut asian hyvin vastaan ja lähtenyt parantamaan omaa kyberturvaa”

Tätä samaa tukee myös muiden haastateltavien kommentit, eli lähinnä vakuutusyhtiön rooli muodostuu asetettavien kontrollivaatimusten kanssa. Kuitenkin tässä nousi esiin pienet erot eri vakuuttajien ja meklarien välillä. Osa näkee vakuuttajan roolissa mahdollisuuden kasvaa pk-yrityksen sparraajana ja konsulttina yritykselle mahdollisesti vieraassa aiheessa. Riskitiedon tuntemista ja ymmärryksen parantamista kaivataan. Asiantuntija E kuvaa potentiaalia näin:

”Ykkösjuttu on musta se, että jos jokin kontrolli ei ole kunnossa niin vakuuttajalla tai meklarilla olisi valmis ratkaisu ja ohjeistus että hei – näin saat tän homman kuntoon ja sujuvoitetaan sitä prosessia. En nää että se neuvonantajan rooli olisi vakuuttajalla vaan kyllä se lähtökohtaisesti on meklareilla. Toki monilla pk-yrityksillä ei oo meklaria Suomessa ja ne on suoraan vakuutusyhtiöön yhteydessä, niin toki sillon vakuutusyhtiökin voi ottaa isompaa roolia siinä.

Vakuuttajat omaavat toki merkittävän roolin ylipäättään riskienhallinnan edistäjänä, ja yleisesti niiden roolin on ajateltu kasvavan riskien ennaltaehkäisemisessä (Kivisaari & Rantala, 2020). Vaikka riskikartoitukset ja vuosittaiset tarkastukset ovat tutumpaa perinteisissä omaisuusvakuutuslajeissa, voi se hyvin olla myös tulevaisuutta kyberriskien osalta myös. Kyberriskit on arvioitu useissa mittauksissa kaikista merkittävimmäksi riskilajiksi (Allianz, 2024) ja samalla niiden vaikutus koko yhteiskuntaan korostuu, kuten finanssialaan kohdistuneet hyökkäykset ovat viime vuosina osoittaneet. Asiantuntijat C ja F näkevät roolin kasvamisen kulkevan käsi kädessä kybervakuuttamisen kasvun kanssa, eli mitä isommaksi lajiksi se kasvaa, sitä enemmän myös vakuutusyhtiöt tulevat riskienhallinnan edistämiseen panostamaan. Asiantuntija D näkee merkityksen pk-yrityksille näin:

”Se on mielenkiintoista millaiseksi yhteistyö tulevaisuudessa kehkeytyy. Koska kyllä mä oon nähnyt miten nyt vuosien saatossa taso on pk-segmentissä parantunut, ja uskon että yksi tekijä on just ollut vakuuttajien kontrollivaatimukset siinä. Ennen kaikkea musta se vakuuttajan rooli tulee siis sieltä kontrollien kautta. Että ennen joutu paljon useemmin sanomaan yrityksille että ei voida ollenkaa myöntää, koska kontrollit ei ollut kunnossa, mutta ei sitä enää samalla tavalla nää.”

Vakuuttajilla on pitkään ollut riskienhallinnan soihdunkantajan rooli, ja kyberriskien kontrollivaatimukset ovat yksi osoitus tästä. Pk-yritysten osalta erityistä on se, ettei organisaatioissa usein ole erityisesti kyberturvallisuuteen puhtaasti erikoistunutta työntekijää, vaan vastuu saattaa jakaantua ja usein kyberturvasta ja sen budjetista vastaavat henkilöt voivat olla eri henkilö. Tämä saattaa aiheuttaa omaa haastetta riskienhallinnan päätöksiä tehdessä suhteessa vakuutusyhtiön kontrollivaatimuksiin. Asiantuntija A kuvaa tilannetta näin:

”Välillä huomannut, että kun talousjohtajalle lyödään vaatimukset eteen ja sanotaan että hei näiden implementointi maksaa x tuhatta euroa ja sen jälkeen vakuutusmaksu on y tuhatta euroa, niin IT:stä vaaditaan että 'hei antakaa toi raha meille suoraan niin parannetaan kyberturvaa eikä tarvita

vakuutusta'. Ihan näinhän se ei tietysti mee, koska et sä pysty ikinä täysin sitä riskiä kontrolloimaan vaan aina on mahdollisuus hyökkäykselle, ja sitten jos ei ollakaan valmistauduttu siihen että hyökkäys tulee niin vahingot voi olla mittavat eikä vakuutusta ole.”

4.3.1 Kontrollien soveltuvuus ja tarkastus

Seuraavaksi haastatteluissa käytiin läpi kontrollien soveltumista ja niiden tarkastusprosessia. Kuten mainittua kaikkia kyberriskejä ei voida täysin kontrolloida ja kaikkiin skenaarioihin kontrollivaatimukset eivät sovellu. Yksittäisenä riskilajina kyberriskeistä nousee eniten esiin ihmisten toiminta eli inhimilliset virheet ja niistä aiheutuvat vahingot (Alahmari & Duncan, 2020). Haastatteluiden tulokset olivat linjassa tämän teorian kanssa, eli kaikki haastateltavat mainitsivat tätä kysyttäessä inhimillisen aspektin; ihmistä voi kontrolloida kaikista heikoiten ja samalla se on suurin yksittäinen riski organisaatiolle. Asiantuntijoiden näkemyksen mukaan kontrollit voivat olla kuinka hyviä ja kattavia tahansa, mutta mikäli prosessit eivät ole kunnossa ja kyberturvallisuus ei ole osa pk-yrityksen sisäistä kulttuuria, eivät ne lopulta hyödytä yritystä läheskään niin kuin pitäisi. Asiantuntija F kiteyttää asiaa seuraavasti:

”Se on vähä sama kun laitat surkeen kuskin Ferrarin rattiin niin ethän sä saa siitä autosta tehoja irti, kyllä se vaatii koulutusta, selkeen frameworkin ja systeemit miten toimitaan.”

Asiantuntija A:n mukaan haaste on myös siinä, että toisaalta mitä enemmän kontrolleja otetaan käyttöön, sen haastavammaksi se järjestelmien käytön yleensä tekee käyttäjien kannalta. Asiantuntija C nostaa esiin sen, että laadulliset kontrollit ovat kaikista oleellisimpia, mutta niitä on myös työläintä mitata, jolloin pk-yrityksille tyydytään pääosin tekemään ulkoisia haavoittuvuusskannauksia ja kysymään peruskysymyksiä. Lisäksi useassa haastattelussa herätti keskustelua se, kuinka paljon kontrollit aidosti vaikuttavat riskin todennäköisyyteen ja mikä todellinen vaikutus on, sillä historiatietoa on vielä kyseisistä riskeistä niin vähän saatavilla. Asiantuntija B näki tilanteen näin:

”Jos mietitään pk-sektoria ja sitä että sinne nyt lähinnä asetetaan teknisiä vaatimuksia, niin paljonko se aidosti vaikuttaa riskiin? Okei jos se tietty riski nyt sitten toteutuu kerran sadassa vuodessa viidenkymmenen sijaan niin mikä on aito merkitys yritykselle? Että kyllä musta tuntuu että enemmän ollaan alettu ymmärtää ja tunnistaa se ihminen ja työntekijän vaikutus siihen riskiin. Että okei, vaikka me kuinka suojauduttais riskiltä niin oleellista on miettiä miten me ollaan varauduttu siihen kun jotain sattuu ja tässä tietysti vakuuttajilla on iso rooli myös”

”Peruskysymykset” toteutetaan nykypäivänä vielä pitkälti sähköpostitse lähetettävillä lomakkeilla, vaikka tulevaisuuden osalta myös muita vaihtoehtoja on jo nähtävissä. Pari haastateltavaa nostaa esiin tavoitteen tehdä underwriting-prosessista mahdollisimman sujuvaa ja vaivatonta pk-yritykselle, jossa toiminnan pitää olla tehokasta ja dialogin kansantajuisista pk-yritysten päättäjien kanssa. Asiantuntija C nostaa esiin myös terminologian merkityksen, eli monille yrityksille kybermaailma ja kybervakuutus kuulostavat liian teknisiltä tai muuten korkealentoiselta, jolloin tietyt vakuuttajat ovatkin alkaneet puhumaan enemmän tietoturvakatuuksesta ja tulkkamaan muutenkin vaikeaselkoisia vakuutusehtoja ja niiden korvattavuuksia kansantajuisemmin. Tässä useampi asiantuntija korosti meklarin kasvavaa roolia, vakuutusmeklarien yleistyessä myös pk-sektorissa. Perinteisille pdf-lomakkeille esitetään vaihtoehdoksi esimerkiksi verkkoportaaleja, joihin yritys pystyy mahdollisimman helposti täyttämään tarvittavat tiedot ja jota kautta se saa lähes reaaliaikaisesti sitovan tarjouksen kybervakuutuksesta. Asiantuntija A näkee kehityskulun selkeänä ja johdonmukaisena:

”Kyllä se on koko ajan ollut nähtävissä, että vakuuttajilla on ollut halu yksinkertaistaa ja tehdä kontrolli-prosessista mahdollisimman käyttäjäystävällistä. Toisaalta se on näkynyt näinä teknisinä ratkaisuin mutta kyllä toisaalta myös on näkynyt sitä, että vaatimuksia on kevennetty, ja ehkä on ajateltu, että saataisiin näin isompi massa asiakkaita, jolloin joukkoon saa tullakin heikommilla kontrollitasoilla.”

Tämä oli yksi oleellisimmista trendeistä, mistä heräsi keskustelua useamman eri haastateltavan kanssa, josta vielä tarkempi läpikäynti seuraavassa kappaleessa. Kaikki haastateltavat vahvistivat, että tarkastusprosessi suoritetaan lähtökohtaisesti vakuutuksen alkuvaiheessa tai vuosittaisessa uudistusprosessissa, koska kybervakuutukset ovat lähes poikkeuksetta vuoden määräaikaista sopimuksia. Kuitenkaan uudistusprosessissa ei yleensä tehdä sen tarkempaa analyysia tai tarkastuksia, vaan asiakas kirjallisesti vahvistaa, että sovitut kontrollit ovat paikallaan. Mikäli asiakasyritys on ottanut käyttöön uusia kontrolleja ja parantanut merkittävästi kyberturvallisuutensa tasoa, voidaan tämä ottaa huomioon vakuutusmaksussa alennuksena. Lähtökohtaisesti vakuutusyhtiö ei halua sen tarkemmin tarkastaa, että kerrotut kontrollit on implementoitu, sillä vakuutuslainsäädäntö velvoittaa luonnollisesti asiakasta olemaan totuudenmukainen, mikäli haluaa korvausta saada. Asiantuntija E kiteyttää asiaa näin:

”Sinänsähän asia on lainsäädännön kannalta simppelempi, ja me ainakin nojaututaan vahvasti vakuutuslakia, eli ei lähdetä sen tarkemmin kontrolleja tarkastamaan. Eli jos yritys väittää että MFA on kunnossa ja vahinkotilanteessa forensiikkayhtiö selvittää, että vaikkapa se MFA ei ollut kunnolla käytössä, niin se sitten vaikuttaa maksettaviin korvauksiin tai ylittäään vahingon korvattavuuteen.”

Myös asiantuntija B vahvistaa saman ja korostaa forensiikkayhtiöiden eli tietoturvaolosuhteiden selvittämiseen ja analysointiin erikoistuneiden yritysten roolia yrityksen käytössä olleista kontrolleista ja millä tasolla ne olivat suhteessa siihen, mitä on alun perin ilmoitettu. Forensiikkayhtiöt toimivat usein tiiviissä yhteistyössä vakuuttajien kanssa ja ne ovat usein ennalta määrättyjä tai yhdessä sovittuja asiakasorganisaation kanssa.

Tästä osiosta kiteytyksenä voidaan nostaa, että kontrollivaatimukset vaikuttavat hieman yrityksen koosta ja toimialasta riippuen aidosti riskienhallintaan ja kyberturvallisuuden tasoon, mutta vakuuttajilla on siinä vielä isossa kuvassa suhteellisen pieni rooli kybervakuuttamisen ollessa marginaalinen vakuutuslaji. Joskin roolilla on hyvät edellytykset kasvaa vakuutuslajin mukana tulevana vuosina. Lisäksi vastauksista kävi ilmi, että ihmisiä ja yritysten henkilöstöä voidaan pitää kaikista haasteellisimpana kontrolloitavana seikkana, joskin tämä haaste on tiedostettu ja siihen pyritty löytämään ratkaisuja. Lisäksi kontrollivaatimusten tarkastusprosessi elää muutosten aikakautta, kun kybervakuuttamista pyritään tekemään yhä helpommaksi pk-sektorin yrityksille.

4.4 Kontrollivaatimusten haasteet

Viimeisessä haastattelun osassa paneuduttiin kontrollivaatimukseen liittyviin haasteisiin sekä niissä piileviin tulevaisuuden näkymiin ja mahdollisuuksiin. Tavoitteena oli selvittää etenkin viimeiseen tutkimuskysymykseen vastauksia, eli millaisia haasteita ja kehittymismahdollisuuksia kontrollivaatimukseen liittyy. Aluksi haastateltavilta kysyttiin tämänhetkisistä keskeisimmistä haasteista, joissa nousi esiin jo edellisessä osiossa mainittu henkilöstön kontrollointi sekä laadullisten kontrollien haastava analysointi. Toki kontrollivaatimukseen liittyy paljon myös muita haasteita, joista asiantuntijat nostivat esiin riskin jatkuvan muutoksen, vakuutuslajin uutuuden ja teknologian kehityksen tuoman epävarmuuden. Nämä olivat hyvin pitkälti samoja havaintoja kuin teoriaosuudessa tehtiin (Eling & Schnell, 2016). Myös pk-yrityksistä puhuttaessa useampi nosti esiin tietoisuuden vähäisyyden niin kybervakuuttamisessa kuin ylittäään kyberturvallisuuden saralla.

Asiantuntija B:

”Kyllä se mun mielestä lähtee siitä, että yrityksen itse täytyy tuntea parhaiten se oma kyberriski. Kyllä vakuuttaja tai meklari voi olla tukena, mutta jotta niitä päätöksiä käyttöön otettavista kontrolleista siitä rajallisesta IT-budjetista voidaan tehdä oikeesti järkevillä perusteilla niin kyllä kyllä ensisijaisesti mitä täytyy parantaa on kybertietoisuus yrityksissä”

Asiantuntijoiden A ja C mielestä tietoisuudessa on tapahtunut merkittävää parannusta viime vuosina sattuneiden vahinkojen myötä, mutta parannettavaa riittää vielä reilusti. He myös nostavat esiin ulkoiset vaatimukset esimerkiksi sopimuskumppaneilta, jolloin ”pakon edessä” myös pk-yritysten tietoisuus lisääntyy kybervakuuttamisen mahdollisuuksista. Asiantuntija C sanoo huomanneensa, kuinka pk-sektorissa saattaa herättää ihmetystä ja turhautumista, mikäli vertaa kybervakuuttamisen hintaa perinteisiin lajeihin suhteessa liikevaihtoon. Ja toisaalta, vaikka kontrollit olisivat kuinka laadukkaat, siltikään vakuutusta ei välttämättä saada, jos riski on hyvin haastava (Ollila, 2024). Useammassa haastattelussa tuli esiin myös se, kuinka muutama vuosi takaperin tapahtunut äkillinen hintojen nousu aiheutti yrityksissä epätietoisuutta, mikä on haastanut vakuutusten myyntiä. Moni toivoi, että nyt markkina olisi löytänyt tasapainonsa ja hintataso pysyisi suhteellisen vakiintuneena. Tätä kukaan ei tosin pitänyt varmuutena ottaen huomioon dynaamisen kybermaailman huomioon.

Tasapainosta puheen ollen miltei kaikki asiantuntijat nostivat haasteista puhuttaessa esiin pk-yritysten osalta yhdeksi suurimmaksi haasteeksi tasapainon löytämisen sen suhteen, kuinka paljon yrityksiltä halutaan tietoa kysyä ja kontrolleja vaatia. Vaikka vakuuttajille lähtökohtaisesti on sitä parempi mitä paremmat kontrollit asiakkailta on käytössä, on kilpailu kiristynyt markkinassa ja ottaen huomioon pk-yritysten suuren määrän Suomessa ja niiden keskimääräisen suhteellisen heikon kyberturvallisuuden tason (Hoppe & ym., 2021), on kyse aina tasapainottelusta ja kompromissien tekemisestä portfolioita rakentaessa. Asiantuntijat E ja D korostavat, että kovan markkinan aikaan vakuuttajilla oli paljon enemmän varaa valita ja seuloa tarkkaan sisään otettavia asiakkuuksia, kun taas nykyään kilpailu on kovempaa ja on hieman joustettu tavoitellusta hygieniatasosta, jota pyritään paikkaamaan isommalla massalla yrityksiä mikä tasapainottaisi riskejä.

Asiantuntija F:

”Nään että pk-yritykset ovat juuri sieltä haastavimmasta päästä tässä mielessä, koska tiedetään että siellä suojan taso voi olla aika alhainen, mutta samalla se on se väylä mistä kasvua voidaan saada, niin se on pallottelua sen välillä että mihin se taso asettuu vaatimusten osalta ja kuinka paljon me (vakuutusyhtiö) sitten halutaan sitä riskiä ottaa siinä”

Asiantuntijat näkevät haasteen myös siinä, kuinka pk-yrityksiä saatetaan kohdella kontrollivaatimusten osalta samoilla periaatteilla kuin isompia yrityksiä, mikä aiheuttaa turhautumista ja epärealistisia odotuksia. Asiantuntija A ja F ovat huomanneet edelleen markkinoilla, että välillä vakuuttajat asettavat aivan liian korkeita kontrollivaatimuksia, jolloin prosessi pysähtyy siihen ja pk-yritys saattaa laittaa hanskat tiskiinkin kokonaan kyberturvallisuuden parantamisen suhteen. Mikäli vaatimustenmukaisuus vaatii liian suuria panostuksia yritykseltä, se ei palvele ketään osapuolta.

Haastatteluiden perusteella haasteista voidaan vetää yhteenvedona, että esiin nousivat erityisesti muuttuvat riskit, pk-yritysten vähäiset resurssit ja tietotaito sekä tasapainon löytyminen asetettaviin kontrolleihin. Perustason kontrolleihin on alkanut löytymään tietty standardi, mutta toimialasta riippuen ne voivat vaihdella paljonkin. Yksi keskeinen haaste onkin se, onko olemassa jokin tietty riski, jota ei tällä hetkellä nähdä, mutta joka vaatisi uuden ”peruskontrollin” lisäämistä samalla tavalla kuin MFA:n tai varmuuskopioiden tärkeys on huomattu. Asiantuntija C nostaa tästä keskustellessa esimerkiksi pilvipalveluiden käytön yleistymisen myös pk-yrityksissä ja sen mukana tulevat riskit. Asiantuntija D korostaa toimitusketjuriskiä, johon pilvipalvelut voidaan ajatella sisältyvän. Pk-yrityksille kannattavampaa on ulkoistaa omia IT-palveluja, mutta riippuvuus palveluntarjoajista nostaa keskeytysriskiä. Tätä on myös haastavampi kontrolloida vaatimuksilla. Sama ilmiö huomioitiin myös teoriaosuudessa (Marotta ym., 2017).

4.4.1 Tulevaisuuden kehitysmahdollisuudet

Lopuksi haastatteluissa kysyttiin asiantuntijoiden näkemyksiä kehitysmahdollisuuksiin, joita he näkevät tällä hetkellä kybervakuuttamisessa erityisesti kontrollivaatimusten näkökulmasta. Tässä vastaukseksi saatiin osittain eriäviä näkemyksiä, mutta toki joitain yhteneväisiä trendejä oli myös havaittavissa. Näistä yksittäisenä merkittävimpänä havaintona oli vakuuttajien tahtotila kasvattaa presenssiä pk-sektorissa sekä samalla tehdä prosessista kokonaisuudessaan sujuvampaa yritysten näkökulmasta. Leimaavaa vastauksille oli myös ajatukset siitä, kuinka kybervakuutusmarkkina hakee vielä vahvasti jalansijaansa, ja tulevaisuudessa on odotettavissa vielä muutoksia myös kontrollivaatimuksiin.

Keskustellessa prosessin sujuvoittamisesta asiantuntija B ja F nostivat yhdeksi oleelliseksi tekijäksi kontrollivaatimusten standardoinnin, eli markkinoille löytyisi pk-yrityksille vakio- tai vakiomuotoiset

vaatimukset, jotka täyttämällä voisi olla varma, että saa vakuutuksista tarjouksia. Tämän päälle tulevat muut lisäkontrollit voitaisiin ottaa huomioon ehtolaajennuksina tai hinnanalennuksina. Asiantuntija C näki tämän osalta haasteeksi sen, että hallinnollisia kontroleja olisi tärkeä seurata, mutta mikäli prosessista haluttaisiin tehdä mahdollisimman automaattista ja tehokasta, olisi paras tapa tähän seuloa vain teknisiä vaatimuksia. Asiantuntija D korostaa standardoinnissa ja prosessin kehittämisessä meklarilla olevan tärkeä rooli:

”kyllä ne on alkanut vakiintua tässä pikkuhiljaa, kun on alettu huomata millaisia vahinkoja sattuu ja miten niitä voidaan hallita. Mutta näkisin että meklarilla olisi isoin rooli siinä mielessä, että kaikilla isoilla kansainvälisillä meklareilla on omat hakemuslomakkeet, joita vakuuttajat sitten hyväksyvät ja käyttävät.”

Vastausten perusteella yksi kehityskulku liittyy myös reaaliaikaisuuteen ja teknologisen kehityksen hyödyntämiseen. Useampi nosti haavoittuvuusskannausten ja muiden analytiikkatyökalujen käytön yleistymisen ja niiden hyödyntämisen kontrollivaatimusten asettamisessa. Myös tekoälyn nähtiin tulevan apuun etenkin pienempien yritysten osalta, jossa vakuutusprosessi halutaan optimoida mahdollisimman tehokkaaksi ja suoraviivaiseksi. Asiantuntija D:n mielestä vakuutusmaksut alkavat olla niin pieniä pk-kokoluokan yrityksille, että manuaalista työtä ei voida juurikaan käyttää, jotta asiakkuudet säilyvät kannattavina. Myös muiden kyberturvallisuuden palveluntarjoajien käyttöä ja yhteistyön lisääntymistä moni odotti tulevaisuudelta. Asiantuntija A ja D näkemyksen mukaan koska pk-yrityksillä on itsellä pienet resurssit ja ulkoistaminen on usein järkevää, nousee palveluntarjoajien rooli suuremmaksi, jolloin vakuuttajilla on tahtotila myös vaikuttaa näihin kumppaneihin ja olla mukana valinnoissa. Asiantuntijoiden mukaan monet vakuuttajat pyrkivät vähentämään manuaalisesti kysyttäviä kontroleja ja hakemaan tarvittavaa tietoa riskistä eri väyliä pitkin.

Asiantuntija A:

”En usko että vakuuttajat haluaa kokonaan luopua kontrollivaatimuksista ja alkaa vakuuttaa laput silmillä, mutta totta kai koko ajan kysyttäviä tietoja pyritään keventämään ja hakemaan tietoja eri kautta kun on saatavilla työkaluja ja varmati tekoälyä tullaan myös niihin yhdistämään. Tällöin poistetaan sitä manuaalista työtä asiakkaan päästä ja hyväksikäytetään hankittua dataa vaikkapa just skannausten tai toimialalta saatavan vertailudatan avulla”

Vastauksista voidaan päätellä, että selkeä trendi on keventää asiakkaalle asetettavia teknillisiä ja hallinnollisia vaatimuksia ja paikata tätä riskienhallintaa muilla keinoilla, esimerkiksi hankkimalla

isompi asiakaskanta ja hyödyntämällä skannauksilla saatavaa kuvaa asiakasyrityksen kyberturvallisuuden tasosta. Tämä on kuitenkin hyvin tuore ilmiö alalla ja vielä on epäselvää, millaisia seurauksia tällä on vaikkapa vahinkokehitykseen, ja kuinka taas esimerkiksi skannausten perusteella saatavan datan pohjalta voidaan päätellä riskien todennäköisyyksiä.

Lisäksi vastauksista voidaan tehdä synteesiä, että tulevaisuudessa meklarin roolin odotetaan kasvavan tulkkina yritysten suuntaan ja riskienhallinnan asiantuntijana. Myös joistain paljon resursseja vaativista kontrollivaatimuksista on alettu luopumaan ja siirtymään suoraviivaisiin skannauksiin ja automatisoituihin työkaluihin, joiden avulla riskiä pyritään hallitsemaan mutta tietoa saadaan vain eri kautta. Teknologian ja tekoälyn hyödyntämiseen liittyy varmasti suuria mahdollisuuksia, mutta myös uhkia, koska kuten todettua ihminen on usein kuitenkin se merkittävin riskitekijä, ja vielä on hyvin epävarmaa, kuinka tekoäly osaa tällaista analysoida ja ottaa riskiprofiilia muodostaessa huomioon. Selvää on kuitenkin se, että vakuuttajat pyrkivät kasvattamaan rooliaan vahinkojen ehkäisyssä ja kyberturvallisuuden parantamisessa, samalla kun tietoisuus pk-yritysten keskuudessa kasvaa.

Haastatteluissa nousi myös yhdeksi kasvavaksi teemaksi se, miten yritys varautuu kyberhyökkäykseen ja vaikkapa järjestelmien lamaantumiseen ja siitä palautumiseen. Suomeksi käytännössä puhutaan esimerkiksi poikkeamatilanteen suunnitelmasta (incident response plan) ja liiketoiminnan jatkuvuussuunnitelmasta (business continuity plan). Ideana olisi, että kontrollivaatimuksetkin keskittyisivät tulevaisuudessa enemmän dynaamiseen resilienssiin kuin pelkästään koventamaan kyberturvaa teknillisillä ratkaisuilla. Asiantuntijan D:n mainitsema toimitusketjuriski ja siihen varautuminen on hyvä esimerkki tällaisesta. Näin vaaditut toimenpiteet saataisiin integroitua paremmin kokonaisvaltaiseen riskienhallintaan ja palvelemaan liiketoiminnan tavoitteita.

5 YHTEENVETO

5.1 Tutkimuskysymyksiin vastaaminen ja johtopäätökset

Tutkielmassa selvitettiin vastauksia kolmeen tutkimuskysymykseen. Ensimmäinen kysymys käsitteli yleisesti mitä kontrollivaatimuksia nykypäivänä vakuutusyhtiöt asettavat pk-yrityksille. Tarkemmin tavoitteena oli selvittää, mitä aiheen tuore kirjallisuus ja haastatellut asiantuntijat sanovat nykyisistä kontrollivaatimuksista, mitä ovat niin sanotut vähimmäisvaatimukset ja miten ne ovat kehittyneet nykyisenlaisiksi. Teoriaosuuden pohjalta ennako-oletus oli se, että vakuutusyhtiöt pitäisivät vähintään joitain vaatimuksia vähimmäistasona, jolloin vakuutettavuus olisi ylipäätään mahdollista. Lisäksi oli myös oleellista määritellä riittävän tarkasti mitä kontrolleilla tarkoitetaan, jotta kaikki ymmärtäisivät ne samalla tavalla. Haastatteluiden pohjalta tehdyn analyysin havainnot kuitenkin korostivat kokonaistarkastelun merkitystä, eikä niinkään mitään yksittäisten kontrollivaatimusten ehdottomuutta kybervakuutuksen edellytyksenä. Asiantuntijoiden näkemykset olivat tämän osalta hyvin yhdensuuntaiset ja selvät.

Empiriaosuuden luvussa 4.2 käsiteltiin laajemmin vastauksia ensimmäiseen tutkimuskysymykseen, mutta tiivistyksenä voidaan todeta, että pk-yrityksille asetettavat kyberkontrollivaatimukset sisältävät sekä teknisiä että hallinnollisia vaatimuksia, jotka tähtäävät vakuutettavan riskin parempaan hallintaan, riskitietoisuuden lisäämiseen ja tietysti toimenpiteisiin riskin pienentämiseksi. Teknisiin kontrollivaatimuksiin voidaan ajatella kuuluvan erityisesti IT-infrastruktuuriin liittyvät toimenpiteet, kuten pääsynhallinta, varmuuskopiot ja monivaiheinen tunnistautuminen, jotka ovat helpommin mitattavia ja dokumentoitavia. Näitä vakuuttajat ovat perinteisesti vaatineet, joskaan eivät lähtökohtaisesti ehdottomina vakuutettavuudelle. Hallinnolliset kontrollit taas painottuvat johtamis- ja prosessikäytäntöihin, kuten työntekijöiden kouluttamiseen ja tietoturvaprosessien johdonmukaiseen noudattamiseen. Nämä ovat vakuuttajien näkökulmasta vähintään yhtä tärkeitä kuin tekniset kontrollit, mutta ongelma piilee siinä, että niitä on haastavampi arvioida ja tarkastaa vahingon sattuessa. Tärkeys johtuu siitä, että ilman hallinnollista tukea ja prosessien toimivuutta, teknisten kontrollien tehokkuus jää helposti heikoksi.

Lisäksi ensimmäisen tutkimusongelman kohdalla selvitettiin sitä, miten kontrollivaatimukset näyttäytyvät pk-yrityksille ja kuinka prosessi käytännössä toimii asiantuntijoiden näkökulmasta. Tavoitteena oli selvittää, miten vakuuttajat ja meklarit kokevat prosessin ja miten he arvioivat sen

toimivuutta pk-yritysten kontekstissa. Haastatteluiden perusteella alalla toimitaan vielä suhteellisen perinteisin keinoin vaatimusten osalta eli lomakkeita manuaalisesti täyttämällä toistaiseksi, mutta muutos on kuitenkin käynnissä ja jatkuvasti nähdään enemmän teknologian hyödyntämistä ja prosessin sujuvoittamista. Tuloksista voidaan myös päätellä, että pk-yritykset toivoisivat vakiintuneempia vaatimuksia, mikä onkin historian saatossa edistynyt, mutta toisaalta riskin jatkuva muuttuminen aiheuttaa merkittävää haastetta siihen.

Haastatteluista kävi siis ilmi, että kyberriskin dynaamisuus ja tulevaisuuden lähes mahdoton ennustaminen tekee vaikeaksi määritellä vakioituja vaatimuksia – edes pk-yrityksille. Teoriaosuus oli tämän näkemyksen kanssa yhtäläinen (esim. Eling & Schnell, 2016). Vaikka aluksi monet vakuuttajat ajattelivat, ettei kyberriski ole sen muutostahdin vuoksi edes vakuutettava riski, etenkin pienemmän päässä yritysten koska niiltä ei voida vaatia samaa kontrollitasoa kuin isommilta yrityksiltä, on vuosien saatossa näkemys vahvistunut sen suhteen, että kybervakuuttamisesta tulee yksi keskeisimmistä vakuutuslajeista pitkällä aikavälillä, ja kontrollivaatimukset tulevat aina olemaan tavalla tai toisella merkittävä osa niitä. Asiantuntijat vahvistivat, että kybervakuutusmarkkinat ja kybervahinkojen kehitys ovat olleet kaksi eniten vaikuttanutta tekijää kontrollivaatimusten laadinnassa. Tämän koin tutkielman tekijänä itse hyvin mielenkiintoiseksi, sillä arvauksien varaan jää, tuleeko lähivuosina vielä jokin sellainen vahinkorypäs, joka luo uuden vakiintuneen kontrollivaatimuksiin markkinoille.

Toisessa tutkimuskysymyksessä paneuduttiin kontrollivaatimusten merkitykseen. Selvää oli se, että ne ovat vakuuttajille välttämättömyys riskien arviointiin ja sopivan riskitason ylläpitämiseen, mutta tutkimuksella haluttiin myös lisätä ymmärrystä sen osalta, millainen merkitys niillä on vakuuttajien näkökulmasta asiakasyrityksiin, ja kuinka tehokkaita vaaditut kontrollit aidosti ovat. Eli miten paljon ne vaikuttavat riskeihin todellisuudessa ja palvelevatko ne myös yrityksen liiketoiminnallisia tavoitteita, vai voivatko ne olla tietyissä tilanteissa myös ylikuormittavia, epätehokkaita ja soveltumattomia. Lähtökohtaisesti kontrollivaatimuksienhan pitäisi palvella molempia osapuolia; kyberriskejä saadaan mitigoitua ja vakuutuksesta saadaan jäännösriskiä varten turvaa.

Teoriaosuuden pohjalta ajatus oli se, että kontrollivaatimuksilla on merkittävä vaikutus pk-yritysten kyberriskien hallintatasoon. Toki on samalla hyvä muistaa, että vain n. 5%:lla suomalaisista yrityksistä on tällä hetkellä kybervakuutus eli kovin merkittävästä ilmiöstä ei isossa kuvassa vielä puhuta (Ollila, 2024). Tämän osalta tulokset empiriaosuudesta olivat hieman eriäviä, sillä asiantuntijat eivät nähneet merkitystä ainakaan toistaiseksi niin merkittävänä. Lisäksi teorian pohjalta oletettiin, että kontrolleilla on erityisen heikko vaikutus inhimillisiin virheisiin ja niihin liittyviin

kybervahinkoihin (Alahmari & Duncan, 2020). Toregas ja Zahnin mukaan myös pk-yritysten tulisi lähestyä kyberturvallisuutta kokonaisvaltaisesta näkökulmasta, jossa eri riskienhallinnan keinot eivät ole vaihtoehtoisia (2014). Käytännössä se voisi tarkoittaa, että yrityksellä on sekä hyvä omasuoja, jota kontrollivaatimuksilla pyritään varmistamaan, että kybervakuutus, jolla suojataan tasetta äkillisiltä taloudellisilta tappioilta.

Asiantuntijahaastattelujen perusteella kontrollivaatimusten vaikuttavuus vaihtelee etenkin yrityksen koosta, toimialasta ja kyberturvallisuuden tasosta riippuen. Mikäli kyse on pienemmästä yrityksestä, jonka lähtökohtainen asiantuntemus ja käytettävissä olevat resurssit ovat hyvin rajalliset, on vakuuttajan asettamilla kontrollivaatimuksilla tällöin tietysti suurempi merkitys. Jos taas yrityksellä on käytössä jo vaikkapa tietoturvasertifikaatteja ja vaatimukset ovat tulleet tutuksi sitä kautta, ei kontrollivaatimukset näyttele niin suurta roolia. Usein kuitenkin pk-yrityksistä puhuttaessa kontrollivaatimukset pakottavat yritykset arvioimaan ja parantamaan omaa kyberturvallisuustasoaan, mikä johtaa parempaan resilienssiin kyberuhkia vastaan. Haastatteluissa ilmeni, että etenkin kontrollivaatimusten kehittyessä enemmän ennaltaehkäisevämpään suuntaan, niiden merkitys kasvaa. Tällöin puhutaan enemmän siitä, miten kontrollivaatimukset integroitaisiin paremmin kokonaisvaltaiseen riskienhallintaan ja palvelemaan liiketoiminnan tavoitteita. Tämä oli keskeinen havainto myös teoriaosuudessa (Digipooli, 2023).

Asiantuntijat näkevät vakuutusyhtiöiden roolin tärkeänä paitsi riskienhallinnan edistäjänä pelkkien vaatimusten myötä, myös potentiaalisena neuvonantajana etenkin siinä, miten yritys pääsisi sujuvasti eteenpäin kehittäessä kyberturvallisuuden tasoa ja esimerkiksi implementoitaessa uutta kontrollia. Kontrollivaatimukset ovat vakuutusyhtiöille mahdollisuus ohjata asiakkaita kohti tehokkaampaa omasuojaa ja lisätä samalla kyberturvallisuuden tietoisuutta. Tämä havaittiin oleelliseksi etenkin pk-yrityksissä, joilla ei usein ole omaa kyberturvallisuusasiantuntijaa tai tietoturvapääällikköä. Toisaalta jos yrityksellä on käytössä vakuutusmeklari, vakuutusyhtiöiden ja meklarien välinen työnjako on kriittistä, ja erityisesti ohjauksen ja konsultaation osalta merkittävä pk-sektorilla, missä neuvontaa ja tukea kaivataan usein enemmän kuin isomman kokoluokan yrityksissä.

Haastatteluissa nousi myös esiin, ettei kontrollivaatimukseen pidä nojautua liikaa, sillä niiden avulla ei kaikkia riskejä voida kattaa eikä kontrolloida, ja vaikka ne pyrittäisiin räätälöimään asiakasyrityksen toimialaan ja koko huomioiden, on niissä silti usein aukkoja ja puutteita. Asiantuntijat olivat kuitenkin siitä yksimielisiä, että koska perustason kontrollivaatimukset perustuvat pitkälti vahinkohistoriaan ja sen pohjalta huomattuihin tehokkaisiin kontrolleihin, on yrityksellä aina

lähtökohtaisesti perusteet ottaa vaaditut kontrollit käyttöön. Koska yritysten tarpeet ja kyberturvallisuustasot vaihtelevat suuresti, kontrollivaatimukset eivät välttämättä sovi kaikille yrityksille samalla tavalla. Kritiikkiä haastateltavat antoivatkin siitä, että joskus kontrollivaatimukset ovat liian tiukkoja tai liikaa resursseja vaativia, jolloin yritys saattaa todeta prosessin turhaksi ja jättää kybervakuutuksen hankkimatta. Tällöin voidaan ajatella, että kontrollivaatimukset eivät edistä kyberriskien hallintaa – vaan päinvastoin heikentävät sitä. Tämän takia kontrollivaatimusten räätälöinti ja kytkeminen kokonaisvaltaiseen riskienhallintaan on myös tärkeää.

Yhteenvedona vastauksista toiseen tutkimuskysymykseen voidaan todeta, että kontrollivaatimukset vaikuttavat hieman yrityksen koosta ja toimialasta riippuen aidosti riskienhallintaan ja kyberturvallisuuden tasoon, mutta vakuuttajilla on siinä vielä isossa kuvassa suhteellisen pieni rooli kybervakuuttamisen ollessa marginaalinen vakuutuslaji ja koko kybervakuutusmarkkinan vielä hakiessa muotoaan. Joskin sekä teoria- että empiriaosuus vahvistivat sitä mahdollisuutta, että tulevaisuudessa kontrollivaatimusten roolilla on hyvät edellytykset kasvaa vakuutuslajin mukana ja vaikuttaa enemmän myös yhteiskunnallisesti yritysten kyberturvallisuuden tasoon.

Kolmas ja viimeinen tutkimuskysymys koskee kontrollivaatimukseen liittyviä haasteita sekä tulevaisuuden kehittymismahdollisuuksia. Tavoitteena oli selvittää ja laajentaa ymmärrystä sen osalta, mitkä ovat merkittävimpiä kipukohtia tällä hetkellä niiden saralla, ja toisaalta miltä tulevaisuus näyttää; onko merkittäviä muutoksia tulossa ja missä suurin potentiaali piilee. Haasteiden osalta tutkimustulokset voitaisiin jakaa kolmeen merkittävimpään havaintoon; jatkuvaan muutokseen, resurssi- ja osaamispulaan ja tasapainottelun haastavuuteen. Myös muita haasteita ilmeni, esimerkiksi teoriaosuudessa ylipäättään kyberriskien vakuuttamiskelpoisuus (Biener ym., 2015) ja toisaalta kyberriskien vaikea kontrolloitavuus (Strupczewski, 2021), mutta yhteisenä johtopäätöksenä voitaisiin nostaa keskeisimpinä nuo kolme.

Jatkuva muutos on tullut jo aiemmin esiin ja se on varmasti kyberriskeihin niin leimallinen piirre ettei se varmasti tule poistumaan myöskään niistä puhuttaessa koskaan. Jos miettii, miten paljon kymmenessä vuodessa kybervakuutusmarkkina on ehtinyt muuttua ja kehittyä, tuskin tarvitsee kristallipalloa arvioidakseen, että seuraavat kymmenen vuotta olisi täysin stabiilia muutoksen suhteen. Sen lisäksi, että kyberriskit ovat itsessään kytköksissä megatrendeihin kuten teknologiseen kehitykseen ja digitalisaation kasvamiseen, lisää haastekerrointa myös geopoliittisen tilanteen muutokset ja taloudellinen kehityskulku. Valtiolliset ja rikolliset toimijat ovat aktivoituneet yhä enenevässä määrin kybermaailmassa, mikä tarkoittaa, että se muodostaa yhä uusia kyberriskejä myös tavallisille pk-yrityksille, joilta suojautuminen on entistä vaikeampaa. Asiantuntijat korostavat

dynaamisiin riskeihin vastaamista dynaamisuudella. Miten nämä suuren mittaluokan haasteet sitten liittyvät kontrollivaatimuksiin? Luonnollisesti ne aiheuttavat haasteita siihen, millä perusteilla vakuutusyhtiöt määrittelevät kontrollivaatimukset. Vaikka niissä nojataan vahvasti kerättyyn historiatietoon ja vahinkokehitykseen, olisi oleellista pyrkiä pitämään katse samalla tulevaisuudessa ja reagoida mahdollisimman pian, kun selkeä muutos tapahtuu.

Tasapainon hakeminen liittyy vahvasti jatkuvaan muutokseen. Tiedetään, että vakuuttajien vaatimilla kontrolleilla on yleisellä tasolla selvä vaikutus kyberriskien tapahtumisen todennäköisyyteen (Dambra ym, 2020), mutta täyttä varmuutta siitä, kuinka paljon ne oikeasti vaikuttavat juuri tiettyyn yritykseen ja missä kulkee se veteen piirretty raja kontrollien implementoinnin ja muiden riskienhallinnan keinojen hyödyntämisen välillä tuskin on mahdollistakaan saada. Tasapainon hakua se on siis molemmille osapuolille, sekä pk-yritykselle että vakuutusyhtiölle. Mutta koska tämä tutkielma keskittyy kontrollivaatimuksiin, on järkevintä tarkastella asiaa vakuuttajan näkökulmasta. Sekä teoria- että empiriaosuudet korostivat juuri tätä vakuuttajan haastetta; mihin vetää raja siinä, kuinka paljon tietoja yrityksestä halutaan hankkia, mitä kontrolleja halutaan vaatia ja kuinka paljon jätetään pimentoon ja omalle riskille. Tähän ei tietysti ole olemassa yhtä oikeaa vastausta, eikä se ollutkaan tutkielman tavoite, vaan lähinnä pyrkiä ymmärtämään mitkä seikat vaikuttavat tähän dilemmaan ja miten vakuuttajat ovat pyrkineet sitä ratkaisemaan.

Resurssi- ja osaajapula on tietysti hyvin yleinen haaste etenkin kyberturvallisuuden taustalla. Usein pk-yritysten tietoturvaongelmien taustalla onkin juuri resurssien niukkuus (Hoppe & ym., 2021). Asiantuntijat näkivät asian niin, että pk-yritysten osalta vakuutusyhtiöiden ja mahdollisten meklarien rooli tulkkajana korostuu, kun terminologia voi olla vierasta ja ymmärrys vähäistä siitä, miksi vakuutusyhtiö ylipäättään esittää kontrollivaatimuksia ja miten niitä voidaan ottaa tehokkaasti käyttöön. Toisaalta juuri pk-yrityksissä voi korostua ilmiönä teknisten kontrollien käyttöönotto vakuutuksen tai sertifiointin toivossa, mutta hallinnolliset kontrollit ja niiden jalkauttaminen yrityksen kulttuuriin jää monesti puutteelliseksi. Lisääntynyt kustannuspaine ja haastava taloustilanne etenkin Suomessa on myös omalta osaltaan vaikeuttanut pk-yritysten sitoutumista enemmän resursseja vaativien kontrollien ylläpitämiseen.

Kehitysmahdollisuuksista nousi esiin myös kolme tekijää: teknologian tuomat mahdollisuudet, prosessin yksinkertaistaminen ja integrointi kokonaisvaltaiseen riskienhallintaan. Teknologisen kehityksen tuomat mahdollisuudet ja tietysti kuumana puheenaiheena tällä hetkellä oleva tekoälyn hyödyntäminen nousivat useammassa haastattelussa esiin. Tokihan se myös yleisesti on koko

vakuutusliiketoimintaa mullistava seikka, mutta koskettaa erityisesti kyberturvallisuutta johtuen sen digitaalisesta luonteesta ja datakeskeisyydestä (Jada & Mayayise, 2023). Pidän jopa hieman yllättävänä sitä seikkaa, että useampi asiantuntija nosti uudet työkalut ja esimerkiksi niillä tehtävät skannaukset niin merkittävään rooliin kehitysnäkymien osalta. On selvää, että ne tulevat helpottamaan vakuutusyhtiöiden työtä analysoidessa ja kvantifioidessa yritysten kyberriskejä, mutta on silti vaikea nähdä, että ne korvaisivat kokonaan manuaalisen työn ja ihmiseltä ihmiselle tehtävän kyselyn, jolla voidaan tulkita paremmin etenkin hallinnollisten kontrollien tasoa. Nähtäväksi jää, kuinka iso osa potentiaalista pystytään valjastamaan underwriting-prosessiin ja kuinka nopeasti se tapahtuu.

Toinen kehitysnäkymä liittyy koko kybervakuutus-prosessin (kuvio 7) suoraviivaistamiseen ja keventämiseen pk-yritysten osalta. Haasteissa esiin nostettu tasapaino on kääntymässä tällä hetkellä kybervakuutusmarkkinan ollessa pehmeämpi ja kilpailun ollessa vakuutusyhtiöiden keskuudessa kovempaa siihen, että tietoja kysytään yhä vähemmän ja kybervakuutusta pyritään saamaan myytyä entistä voimakkaammin etenkin pk-sektorille. Tämä näkyy tietysti yhdessä lainsäädännön kehittyessä tietoisuuden kasvamisena ja yleisen kyberturvallisuustason kehittymisenä. Asiantuntijat nostivat esiin myös reaaliaikaisuuden lisääntymisen riskienhallinnassa, joka näkyy esimerkiksi siten, että jotkin kansainväliset vakuuttajat ovat alkaneet tarjoamaan välitöntä hinnan laskua käyttöön otetusta kontrollista.

Kokonaisvaltainen riskienhallinta on laaja kokonaisuus, mutta myös kontrollivaatimukset liittyvät niihin yhtenä osatekijänä. Asiantuntijoiden mukaan tulevaisuuden kontrollivaatimukset voisivat keskittyä enemmän siihen, että yrityksillä on valmius palautua kyberhyökkäyksistä ja jatkaa toimintaa mahdollisimman pian, jos sellainen sattuu kohdalle. Tämä lähestymistapa parantaisi kontrollivaatimusten arvoa myös pk-yrityksille, ja tällöin kyberriskit ja niiden hallinta ei jäisi niin helposti omaksi erilliseksi osa-alueeksi vaan se otettaisiin paremmin huomioon keskeisenä tekijänä kokonaisuudessa. Tämä parantaisi yrityksen resilienssiä ja auttaisi hallitsemaan riskejä ennaltaehkäisevästi, mutta samalla myös toipumaan poikkeamatilanteesta mahdollisimman sujuvasti.

Haasteista ja kehitysnäkymistä haastatteluissa tuli esiin hyvin monenlaisia versioita ja mahdollisia skenaarioita, mutta myös trendejä kyettiin erottamaan, joista edellä on mainittu keskeisimmät. Huomionarvoista on myös se, että etenkin epäkypsemät pk-yritykset ovat enenevässä määrin vakuuttajien kiikarissa, isompien yritysten markkinan ollessa saturoituneempi. Tämä tietysti luo omat liiketoimintamahdollisuudet, mutta samalla mukana tulee riskit, joissa kontrollivaatimukset ja niiden

onnistunut määrittely saattaa nousta suureen arvoon tulevina vuosina. Ristiriita muodostuu siitä, että kyberhyökkäjille pk-yritys on kohde muiden joukossa, ja se valikoituu jopa suuremmalla todennäköisyydellä haavoittuvuuksien johdosta. Vakuutusyhtiön näkökulmasta taas pk-yritykseltä ei voida vaatia yhtä laajoja kontroleja johtuen yrityksen resursseista. Lisäksi mikäli kybervakuutukset yleistyvät merkittävästi pk-yritysten keskuudessa, voivat ne olla entistä enemmän iskujen kohteena, rikollisten tietäessä mahdollisille kustannuksille ”varman” maksajan.

Kontrollivaatimukset	Vaikutus pk-yrityksiin	Haasteet	Kehitysnäkymät
<ul style="list-style-type: none"> • Vakiintuneet perusvaatimukset • Muodostuneet vahinkojen kautta • Seuraavat markkinakehitystä • Kokonaistarkastelu ratkaisee 	<ul style="list-style-type: none"> • Tietoisuus lisääntynyt • Asettaa "vähimmäistason" • Ohjaa yritystä päätöksissä • Parantanut kyberturvan tasoa 	<ul style="list-style-type: none"> • Tasapaino vaatimustasoon • Jatkuva muutos riskeissä • Inhimillisten tekijöiden kontrollointi • Resurssi- ja osaamispuute 	<ul style="list-style-type: none"> • Työkalut ja automatisointi • Yhteistyön lisääntyminen • Prosessin tehostaminen • Rääätälöinti ja integrointi kokonaisvaltaiseen riskienhallintaan

Kuvio 12. Yhteenveto tutkielman tuloksista.

Yllä olevaan taulukkoon (kuvio 12) on koostettu keskeisimmät nostot tutkielman tuloksista. Otsikkorivillä tulokset on jaettu neljään kategoriaan pitkälti tutkimuskysymysten pohjalta, ja alle on kategorioittain listattu merkittävimmät tulokset. Tulosten analysointia selkeytti ja helpotti se, että haastatellut asiantuntijat olivat pääosin hyvin yksimielisiä ja johdonmukaisia vastauksissa, ja ne olivat useimmiten vielä linjassa aiemmin tehdyn teoriaosuuden kanssa, jonka jälkeen kyettiin vertaamaan havaintoja osioiden välillä ja päätellä niiden pohjalta vastauksia tutkimuskysymyksiin. Kokonaisuudessaan tutkimuskysymyksiin saatiin riittävästi vastausaineistoa ja niistä kyettiin analysoimaan perustellut johtopäätökset.

Tulosten perusteella voidaan päätellä, että juuri nyt eletään mielenkiintoista muutosvaihetta kybervakuuttamisen saralla. Vakuutusmaksut kasvavat ja yhtiöt hakevat kasvua myös pk-yrityksistä, ja tämän laajenemisen yhtenä portinvartijana toimivat kontrollivaatimukset. Tuloksista on

pääteltävissä etenkin kaksi isompaa trendiä: kyberriskit ovat koko lyhyen historiansa aikana olleet erityisen vaikeita riskejä hallita, eikä tähän ole näkyvissä muutosta. Muutosvauhti ei ole hidastumassa, ja yritysten ulkoistaessa tehtäviä enenevissä määrin, kyberriskit komplisoituvat samalla entisestään. Mielenkiintoista on seurata, miten kontrollivaatimukset muuttuvat ja minkälaisen tavoitetasen eri vakuutusyhtiöt päättävät pk-yritysten osalta valita.

Ei niin pahaa, ettei jotain hyvääkin. Toinen aineistosta havaittu trendi on myönteisempi; pk-yritysten parjattu kybertietoisuus ja osaaminen on kehittynyt ja tietoturva-asiat ovat entistä enemmän esillä päätöksiä tehdessä. Kehitettävää toki riittää, mutta suunta on oikea. Yksi avaintekijä kehityksen taustalla on varmasti ollut vakuutusyhtiöt kontrollivaatimuksineen. Vakuuttajat kantavat taloudellista riskiä muuttuvassa riskikentässä, mikä vaatii myös tarkkaa harkintaa ja tasapainoilua kontrollien valitsemisessa. Äkillinen muutos vahinko-olosuhteissa tuskin enää vaikuttaisi kyberriskien vakuutettavuuteen kokonaisuutena, mutta kontrollivaatimuksia ne voivat hyvin muokata. Kyberriski pysyy siis vakuutettavana riskinä, mutta millä ehdoilla – jää nähtäväksi.

5.2 Tutkielman arviointi

Oleellinen osaa tutkielmaa on sen kriittinen arviointi. Ei pelkästään lopuksi työn valmistuttua vaan myös jatkuvasti tutkimuksen edetessä. Eskola ja Suoranta korostavat etenkin tämän olevan laadullisessa tutkimuksessa ei ainoastaan tärkeää vaan suorastaan välttämätöntä (2014, 210). Kriittinen tarkastelu on oleellista, sillä sen avulla voidaan löytää sokeita pisteitä ja mahdollisia heikkouksia tutkielman johdonmukaisuudesta, tarkoituksenmukaisuudesta, luotettavuudesta tai pätevydestä. Ne ovat kaikki tieteelliselle tutkimukselle ominaisia piirteitä, ja ilman itsekriittistä reflektointia tärkeät havainnot saattavat jäädä huomioimatta ja oleelliset opit keräämättä.

Tutkimuksen laadun arvioinnissa tärkeitä käsitteitä ovat pätevyys, merkityksellisyys ja luotettavuus. Tutkimuksen pätevyys tai validiteetti kuvaa sitä, kuinka hyvin onnistuttiin tutkimaan ja analysoimaan sitä, mitä oli tarkoituskin. Sitä voidaan toki mitata monella eri tapaa, mutta kaikilla on sama päämäärä; validiteetti kuvaa tulosten pätevyyttä tutkimusongelmaan ja tutkimuksen tavoitteisiin (Hirsjärvi ym., 2009). Validiteetin voi jakaa kahteen pääkategoriaan: mittausvalidius ja tutkimusasetelmavalidius. Mittausvalidius tarkoittaa sitä, voiko tietyn tutkimuksen tuloksista ennustaa toisten tutkimusten tuloksia. Tutkimusasetelmavalidius kertoo siitä, onko tutkittu ylipäätään haluttua ilmiötä, esimerkiksi käyttämällä oikeita käsitteitä (Hirsjärvi & Hurme, 2022, 186).

Tässä tutkielmassa validiteettia pyrittiin huomioimaan valitsemalla selkeä tutkimusasetelma, laatimalla riittävän laaja tausta- ja tulkintateoria sekä tietysti pyrkimällä vahvaan reliabiliteettiin. Tutkimusasetelma pyrittiin rakentamaan niin, että läpi koko tutkielman tutkimuskysymykset säilyivät taustalla ja mahdollistaisivat relevantin tarkastelun aiheeseen. Validiteetin kannalta oli myös oleellista määritellä ja käsitellä tutkimuksen keskeiset käsitteet ennen teoreettisen viitekehyksen läpikäyntiä. Käytetyt käsitteet ja niiden tulkinta pyrittiin harkitsemaan tarkkaan ennen teoriaosuutta. Koska aihe on suhteellisen tuore ja tieteellistä tutkimuskirjallisuutta ei ole kovin paljon saatavilla, pyrittiin teoriapohjasta luomaan riittävän laaja ja perusteltu, jotta empiriaosuuden haastatteluita voitiin peilata niitä vasten lopuksi. Teoriaosuudessa pyrittiin käyttämään kyberturvallisuudessa ja vakuutustieteessä laadukkaiksi ja luotettaviksi tiedettyjä lähteitä.

Validiteetin kanssa arvioinnissa kulkee käsi kädessä tutkimuksen luotettavuus eli reliabiliteetti. Yksinkertaisuudessaan se tarkoittaa saatujen tutkimuksen mittaustulosten toistettavuutta (Hirsjärvi ym., 2009, 226). Usein siitä käytetään myös termiä luotettavuus, joka kertoo itsessään hyvin sen tarkoituksen; kuinka luotettavina tutkimustuloksia voidaan pitää. Yksi oleellinen osatekijä luotettavuudessa on sen stabiliteetti (Hirsjärvi & Hurme, 2022, 186), mikä kertoo kuinka luotettavia tulokset ovat riippumatta ajasta. Tämän tutkielman tulokset ovat vahvasti aikasidonnaisia, ja voidaan pitää todennäköisenä, että muutaman vuoden päästä samasta teemasta tehtävän tutkimuksen tulokset poikkeaisivat vähintään jollain tasolla. On kuitenkin tärkeää huomata, että laadullisessa tutkimuksessa kaikista oleellisinta ei ole löytää ajallisesti kestäviä ja toistettavia tuloksia, kuten kvantitatiivisessa tutkimuksessa (Hirsjärvi & Hurme, 2014, 186). Kvalitatiivisessa tutkimuksessa korostuu ymmärryksen syveneminen ja aineiston pohjalta tehtävät validit tulkinnat (Tuomi & Sarajärvi, 2018, 28).

Tässä tutkielmassa aineisto kerättiin teemahaastatteluilla, jotka toteutettiin kybervakuuttamisen asiantuntijoille. Lisäksi vastaukset olivat hyvin samansuuntaisia, jolloin vahvistui käsitys siitä, että riittävä saturaatiopiste saavutettaisiin ja kerättyä aineistoa voitaisiin pitää luotettavana. Koska tutkija on laadullisessa tutkimuksessa keskeinen subjektiviteetti ja tutkimusväline (Eskola & Suoranta, 2014, 22), on syytä arvioida myös tutkijan tekemiä analyyseja ja tulkintoja. Analyysia voidaan arvioida muun muassa kattavuuden kautta, eli kuinka laajasti ja läpinäkyvästi aineistoa on esitelty. Kattava analysointi ei perustu satunnaisiin kohdepoimintoihin aineistoista. Luokittelun osalta on myös tärkeää esitellä perusteet mahdollisimman yksiselitteisesti (Eskola & Suoranta, 2014, 216). Aineiston keruu ja siihen käytettävät analysointimenetelmät liittyvät myös luotettavuuden arviointiin.

Tutkielman merkityksellisyydestä on kerrottu enemmän johdantoluvussa, mutta kiteytetysti voidaan todeta aiheen olevan uusi, vähän aiemmin tutkittu ja etenkin ajankohtainen. Pk-yritysten kyberkontrolleja ja niiden merkitystä on tutkittu vähän, ja erityisesti vakuuttamisen ja kauppatieteellisestä näkökulmasta aihetta ei ole juuri tutkittu. Tätä informaatiota ala kuitenkin kaipaa, sen hakiessa tasapainoa ja vahvempaa jalansijaa vakuutusmarkkinoilta. Tutkielmassa pyrittiin myös lähestymään aihetta poikkitieteellisesti, yhdistämällä liiketoiminnallisia, teknillisiä ja lainsäädännöllisiä näkökulmia yhteen tuomaan lisämerkitystä. Näillä perusteilla tutkimusta voidaan pitää kokonaisuutena luotettavana, relevanttina ja validina tutkimuksena. Sen tavoitteena oli tarjota ajankohtaista ja monipuolista katsausta kybervakuutusten kontrollivaatimuksista pk-yrityksille, ja siinä sen voidaan nähdä onnistuneen.

5.3 Lopuksi

Tämä tutkielma käsitteli pk-yrityksille asetettuja kontrollivaatimuksia kybervakuuttamisen näkökulmasta. Sen yhtenä tarkoituksena oli korostaa ehkä hieman pimentoon jääneen kybervakuuttamisen osa-alueen merkitystä. Juuri nyt aihe on ajankohtainen, kun suurin osa vakuutusyhtiöistä on ottanut kybervakuuttamisen vähintään jollain tasolla osaksi liiketoimintaa, mutta strategioita vasta viilailtaan ja tasapainoa haetaan siinä, millaisia yrityksiä, millä ehdoilla ja vaatimuksilla vakuutusportfolioihin halutaan. Rajausta oli spesifi ja tiukka, mutta kontrollivaatimusten suuren merkityksen vuoksi perusteltu. Vaikka vakuuttajatkin hakevat vielä askelmerkkejään kyberriskien osalta, on niiden rooli kyberriskien hallinnassa kasvanut vuosi vuodelta, ja suuntana voi olla samanlainen riskienhallinnan puolesta puhuja kuin omaisuusvakuuttamisessa nykypäivänä.

Kyberriskien historia on lyhyt mutta värikäs. Vakuuttamisen satojen vuosien pituisesta historiasta moni saattaisi sanoa toista. Peruseriaatteet ja liiketoiminnalliset lähtökohdat eivät ole muuttuneet mihinkään. Kun nämä kaksi maailmaa yhdistää, saadaan mielenkiintoinen ilmiö nimeltä kybervakuuttaminen. Kontrollivaatimukset voivat vaikuttaa tekniseltä ja pieneltä yksityiskohdalta tässä kokonaisuudessa, mutta todellisuudessa ne ilmentävät koko ajan reaaliaikaisemmin vahinkojen ja teknologisen kehityksen kulkua, eli erittäin keskeisiä tekijöitä vakuuttamisen kannalta. Kontrollivaatimuksilla on myös suuri mahdollisuus olla keskeinen tekijä kyberriskien hallinnan kehittymisessä. Vaikka on käytännössä mahdotonta ennustaa miten kontrollivaatimukset tuleva kehittymään, tämä tutkielma pyrki lisäämään ymmärrystä niistä, koska riskienhallinnassa kyse on kuitenkin loppupeleissä aina tasapainottelusta ja adaptaatiokyvystä.

Koska aihetta on tutkittu niin vähän, olisi mielenkiintoisia jatkotutkimuksia useita. Lisäksi tutkielman aihe oli rajattu tiiviisti kontrollivaatimusten ympärille, mikä tarkoittaa, että se jättää hyvin tilaa muille aihealueen tutkimuksille, kuten esimerkiksi suuryritysten kontrollivaatimuksille tai muiden vakuutuslajien kuin kybervakuutusten kontrolleille. Yksi mielenkiintoinen vaihtoehto olisi tutkia kontrollivaatimuksia asiakaslähtöisemmin. Nyt ne tulevat pitkälti annettuina suoraan vakuutusyhtiöiltä, mutta syvempi asiakkaan osallistaminen ja kokonaisvaltaisemman riskienhallinnan yhdistäminen voisi tehdä kontrolleista vieläkin tehokkaampia. Kvantitatiivinen vaihtoehto jatkotutkimukselle olisi aihe mitä käsiteltiin tarkemmin kappaleessa 3.3 eli tutkia tarkemmin, miten tehokkaita nykyiset kontrollit ovat, minkälainen investointi ne ovat yrityksille ja onko olemassa jotain kontrollia vaikkapa riippuvuusriskeihin liittyen, mitä ei tällä hetkellä yrityksiltä osata vaatia.

LÄHTEET

Kirjallisuuslähteet

Adarsh, N. & Greeshma M. 2023. *Mastering Information Security Compliance Management*. Packt Publishing.

Alahmari, A., & Duncan, B. (2020). Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence. *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment*, s. 1–5.

Andreev, S., Ometov, A., Bezzateev, S., Koucheryavy, Y, Mäkitalo, N. & Mikkonen, T. 2018. Multi-Factor Authentication: A Survey. *Cryptography* 2, no. 1: 1.

Antonucci, D. 2017. *The cyber risk handbook: creating and measuring effective cybersecurity capabilities*. 1st edition. Hoboken, New Jersey: John Wiley and Sons, Inc.

Benaroch, M. (n.d.). Cybersecurity Risk in IT Outsourcing—Challenges and Emerging Realities. In *Information Systems Outsourcing*. Springer International Publishing. s. 313–334.

Berliner, Baruch. 1982. Limits of insurability of risks.

Biener, C., Eling, M. & Wirfs, J. 2015. *Insurability of cyber risk: An empirical analysis*. Geneva Papers on Risk and Insurance. Issues and Practice, 40, s. 131–158)

Bohara, R., Kranenburg, R., Ross, M. & Yahalom, R. 2023. "Cyber Resilience, Societal Situational Awareness for SME," *2023 IEEE International Conference on Cyber Security and Resilience (CSR)*, Venice, Italy, s. 458-463

Böhme, R., Laube, S., & Riek, M. 2019. A fundamental approach to cyber risk analysis. *Variance*, 12(2), s. 161-185.

Chaput, B. 2024. *Enterprise Cyber Risk Management As a Value Creator: Leverage Cybersecurity for Competitive Advantage*. Apress L. P.

Coburn, A. (Andrew W.) et al. 2019. *Solving cyber risk : protecting your company and society*. 1st edition. Hoboken, New Jersey: Wiley.

Dambra, S., Bilge, L., & Balzarotti, D. 2020. SoK: Cyber Insurance - Technical Challenges and a System Security Roadmap. *2020 IEEE Symposium on Security and Privacy*. s. 1367–1383

Eling, M. 2020. Cyber risk research in business and actuarial science. *European actuarial journal*. 10 (2), s. 303–333.

Eling, M. & Schnell, W. 2016. *What do we know about cyber risk and cyber risk insurance?* Journal of Risk Finance.17 (5), s. 474–491.

Eskola, J. & Suoranta, J.. *Johdatus laadulliseen tutkimukseen*. Vastapaino.

- Evans, A. 2019. *Managing Cyber Risk*. 1st edition. Routledge.
- Giudici, P., & Raffinetti, E. 2022. Explainable AI methods in cyber risk management. *Quality and reliability engineering international*, 38(3), s. 1318-1326.
- Hirsjärvi, S., Remes, P. & Sajavaara, P. 2009. Tutki ja kirjoita. Keuruu: Otavan kirjapaino Oy.
- Hirsjärvi, S. & Hurme, H. 2022. Tutkimushaastattelu, teemahaastattelun teoria ja käytäntö. Helsinki: Gaudeamus.
- Holmström, B. 1979. Moral Hazard and Observability. *The Bell Journal of Economics*, 10(1), 74–91.
- Hopkin, P. 2018. *Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management*. 5. painos. Lontoo: Kogan Page
- Hoppe, F., Gatzert, N., & Gruner, P. 2021. *Cyber risk management in SMEs: insights from industry surveys*. *The Journal of Risk Finance*, 22(3/4), s. 240–260.
- Ilmonen, I., Kallio, J., Koskinen, J., Rajamäki, M., & Koskinen, J. 2022. *Johda riskejä: käytännön opas yrityksen riskienhallintaan* (4. päivitetty painos). Helsinki: Finanssi ja vakuutuskustannus FINVA.
- Jada, I., & Mayayise, T. O. 2023. The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. *Data and Information Management*, 100063
- Juvonen, M., Koskensyrjä, M., Kuhanen, L., Ojala, V., Pentti, A., Porvari, P. & Talala, T. 2014. *Yrityksen riskienhallinta*. Helsinki: Finanssi ja vakuutuskustannus FINVA.
- Kshetri, N. 2021. *The Economics of Cyber-Insurance*. *IT Professional*, 20 (6), s. 9–14.
- Kuosmanen, O.P. & Pitkämäki, P. 2023. Taloudelliset erikois- ja vastuuvakuutukset. Finva.
- Lehto M. *Kybermaailman ilmiöitä ja määrittelyjä*. V 20.0. 1.8.2024. Informaatioteknologian tiedekunta, Jyväskylän yliopisto; 2024.
- Lemnitzer, J. M. 2021. *Why cybersecurity insurance should be regulated and compulsory*. *Journal of Cyber Policy*, 6(2), s. 118–136
- Limnäll, J., Majewski, K., & Salminen, M. 2014. *Kyberturvallisuus*. Docendo.
- McIntosh, T., Susnjak, T., Liu, T., Xu, D., Watters, P., Liu, D. & Halgamuge, M. 2024. Ransomware reloaded: Re-examining its trend, research and mitigation in the era of data exfiltration. *ACM Computing Surveys*
- Rantala, J., Kivisaari, E., Ellibs., & Ellibs. 2020. *Vakuutusoppi* (13. uudistettu painos.). FINVA.
- Roth, A. & Wesley, D. T. A. 2024. Developing a culture of cybersecurity. *International Journal of Technology, Knowledge and Society*, 21(1), s. 29-48.

Saunders, M., Lewis P., & Thornhil, A. 2019, *Research methods for business students* (8th edition.). Pearson Education.

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

Sommer, L. 2015. Industrial revolution -industry 4.0: Are German manufacturing SMEs the first victims of this revolution? *Journal of Industrial Engineering and Management*, 8(5), s. 1512–1532.

Strupczewski, G. 2021. *Defining cyber risk*. *Safety science*, 135: 105143.

Toregas, C. & Zahn, N. 2014. Insurance for Cyber Attacks: The Issue of Setting Premiums in Context. *Cyber Security Policy and Research Institute, The George Washington University*.

Tsohou, A., Diamantopoulou, V., Gritzalis, S., & Lambrinoudakis, C. 2023. Cyber insurance: state of the art, trends and future directions. *International Journal of Information Security*, 22(3), s. 737-748.

Tuomi, J. & Sarajärvi, A. 2018. *Laadullinen tutkimus ja sisällönanalyysi*. Helsinki: Tammi.

von Solms, R., & van Niekerk, J. 2013. From information security to cyber security. *Computers & Security*, 38, s. 97–102.

Verkkolähteet

Ali-Yrkkö, J., Kässi, O., Pajarinen M. & Rouvinen P. 2023. *Digibarometri 2023: Data, tekoäly ja talouskasvu*. Elinkeinoelämän tutkimuslaitos. (Viitattu 31.7.2024). Saatavilla: <https://www.etla.fi/julkaisut/muut-julkaisut/digibarometri-2023-data-tekoaly-ja-talouskasvu/>

Ali-Yrkkö, J., Mattila, J., Mäkäraänen, K. & Seppälä, T. 2020. Kyberuhat yleistyvät – Miten Suomen yritykset pärjäävät? Elinkeinoelämän tutkimuslaitos. (Viitattu 10.8.2024). Saatavilla: <https://www.etla.fi/wp-content/uploads/ETLA-Muistio-Brief-93.pdf>

Allianz. 2014. Allianz Risk Barometer on Business Risks 2014. (Viitattu 20.8.2024). Saatavilla: <https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2014.pdf>

Allianz. 2024. Allianz Risk Barometer 2024: The top business risks for 2024. (Viitattu 20.8.2024). Saatavilla: https://www.allianz.com/en/economic_research/insights/publications/specials_fmo/2024_01_16-Allianz-Risk-Barometer.html

Aspara, J. *Suomalaisten yritysten riskienhallintaa pitää parantaa*. Helsingin Sanomat. (Viitattu 20.8.2024). Saatavilla: <https://www.hs.fi/mielipide/art-2000009088455.html>

Center for Internet Security (CIS), 2017. *Implementation Guide for Small- and Medium-Sized Enterprises*. (Viitattu 10.8.2024). Saatavilla: <https://www.cisecurity.org/wp-content/uploads/2017/09/CIS-Controls-Guide-for-SMEs.pdf>

Center for Internet Security (CIS), 2024. The Cost of Cyber Defense: CIS Controls IG1. (Viitattu 1.10.2024). Saatavilla: https://learn.cisecurity.org/l/799323/2023-08-02/4t3qkj/799323/1694810927NC0iZQGR/CIS_Controls__Cost_of_Cyber_Defense__2023_08.pdf

CFC. 2024. Streamline insurance quoting. (Viitattu 10.9.2024). Saatavilla: <https://connect.cfcunderwriting.com/>

COSO. 2016. Committee of Sponsoring Organizations of the Treadway Commission. Enterprise Risk Management – Aligning Risk with Strategy and Performance. Executive Summary. Viitattu (18.8.2024). Saatavilla: https://www.coso.org/_files/ugd/3059fc_61ea5985b03c4293960642fdce408eaa.pdf

Digibarometri 2020: Kyberturvan tilannekuva Suomessa. Elinkeinoelämän tutkimuslaitos. (Viitattu 31.7.2024). Saatavilla: <https://www.etla.fi/julkaisut/digibarometri-2020-kyberturvan-tilannekuva-suomessa/>

Djebbar, F., & Nordström, K. 2023. *A comparative analysis of industrial cybersecurity standards.* (Viitattu 10.10.2024). Saatavilla: <https://ieeexplore.ieee.org/abstract/document/10210561>

Digipooli, 2023. *Toimialojen kyberkypsyys selvitys 2022: Kansallinen koosteraportti.* Huoltovarmuuskeskus. (Viitattu 20.8.2024). Saatavilla: https://www.digipooli.fi/sites/digipooli/files/inline-files/HVK_Toimialojen%20kyberkypsyys%20selvitys%202022.pdf

ETLA. 2021. *Digitalisaatio ei lisännyt tuottavuutta odotetusti – tutkijat esittävät ratkaisuja tuottavuuden nostoon.* (Viitattu 3.8.2024). Saatavilla: <https://www.etla.fi/ajankohtaista/digitalisaatio-ei-lisannyt-tuottavuutta-odotetusti-tutkijat-esittavat-ratkaisuja-tuottavuuden-nostoon/>

Euroopan unioni. 2017. *EU:n pienyritysten määritelmä.* (Viitattu 30.8.2024). Saatavilla: http://publications.europa.eu/resource/cellar/79c0ce87-f4dc-11e6-8a35-01aa75ed71a1.0007.01/DOC_1

Finanssialalle. 2024. Vakuutusalan tulevaisuus. (Viitattu 12.9.2024). Saatavilla: <https://www.finanssialalle.fi/opintomateriaalit/finanssialan-perusteet/vakuuttaminen/vakuutusalan-tulevaisuus.html>

Finanssiala. 2024. Julkaisut ja tutkimukset: *Vakuutusvuosi 2023.* (Viitattu 22.8.2024). Saatavilla: https://www.finanssiala.fi/wp-content/uploads/2024/05/fa_vakuutusvuosi_2023.pdf

GOV.UK. 2024. Official Statistics: Cyber security breaches survey 2024. Department for Science, Innovation & Technology. (Viitattu 12.9.2024). Saatavilla: <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024#chapter-4-prevalence-and-impact-of-breaches-or-attacks>

Granato, A. & Polacek, A. 2019. The Growth and Challenges of Cyber Insurance. Federal reserve bank of Chicago. (Viitattu 21.8.2024). Saatavilla: <https://www.chicagofed.org/publications/chicago-fed-letter/2019/426>

- Haavisto, L. 2024. *Kyberturvallisuus osana suomalaisten yritysten vuosiraportointia*. Pro gradu - tutkielma. Turun yliopisto. (Viitattu 19.8.2024). Saatavilla: https://www.utupub.fi/bitstream/handle/10024/178801/Laura_Haavisto_opinnayte.pdf?sequence=1&isAllowed=y
- Hiscox. 2022. Cyber attacks strike insolvency fear into businesses. (Viitattu 22.8.2024). Saatavilla: <https://www.hiscoxgroup.com/news/press-releases/2022/16-05-22>
- Howden. 2023. Howden predicts global cyber insurance premiums could exceed USD 50 billion by 2030. (Viitattu 20.8.2024). Saatavilla: <https://www.howdengroup.com/news-insights/howden-predicts-global-cyber-insurance-premiums-could-exceed-usd-50-billion-by-2030>
- IBM. 2024. Cost of a Data Breach Report 2024. (Viitattu 20.8.2024). Saatavilla: <https://www.ibm.com/reports/data-breach>
- If vahinkovakuutus Oyj. 2024. Cyber risk controls. (Viitattu 20.9.2024). Saatavilla: <https://www.if-insurance.com/large-enterprises/insight/risk-consulting-magazine/risk-consulting-2017-2/cyber-risk-controls>
- Institute of Risk Management. 2014. Cyber Risk: Resources for Practitioners. (Viitattu 11.8.2024). Saatavilla: <https://www.theirm.org/media/7237/irm-cyber-risk-resources-for-practitioners.pdf>
- ISO. 2018. ISO 31000 - Risk Management - Guidelines. (Viitattu 19.8.2024). Saatavilla: <https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en>
- ISO. 2022. ISO/IEC 27001:2022. (Viitattu 31.9.2024). Saatavilla: <https://www.iso.org/standard/27001>
- Karhunen, R. 2014. Sammutusjärjestelmä takaa sahan työpaikat. (Viitattu 12.8.2024). Saatavilla: <https://www.finanssiala.fi/kolumni/sammutusjarjestelma-takaa-sahan-tyopaikat/>
- Kyberturvallisuuskeskus. 2020. Pienyritysten kyberturvallisuusopas. (Viitattu 29.8.2024). Saatavilla: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Pienyritysten_kyberturvallisuusopas_9_2020.pdf
- Kyberturvallisuuskeskus. 2024. CrowdStriken päivitys aiheuttanut häiriöitä Windows-laitteissa. (Viitattu 12.9.2024). Saatavilla: <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/crowdstriken-paivitys-aiheuttanut-hairioita-windows-laitteissa>
- Marotta, A., Martinelli, F., Nanni, S., Orlando, A., & Yautsiukhin, A. (2017). *Cyber-insurance survey*. *Computer Science Review*, 24, 35–61. (Viitattu 30.8.2024). Saatavilla: <https://doi.org/10.1016/j.cosrev.2017.01.001>
- Marsh Inc. 2020. Cyber resilience: twelve key controls to strengthen your security. (Viitattu 20.8.2024). Saatavilla: <https://www.marsh.com/us/services/cyber-risk/insights/cyber-resilience-twelve-key-controls-to-strengthen-your-security.html>

- Maynes, 2019. *One simple action you can take to prevent 99.9 percent of attacks on your accounts*. Viitattu 28.8.2024. Saatavilla: <https://www.microsoft.com/en-us/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/>
- McDonald, A. 2023. Leveraging Cyber Insurance In A High-Risk Digital Landscape. Forbes. (Viitattu 31.7.2024). Saatavilla: <https://www.forbes.com/sites/forbesbusinesscouncil/2023/03/09/leveraging-cyber-insurance-in-a-high-risk-digital-landscape/>
- Munich Re. 2024. *Cyber Insurance Risks and Trends 2024*. (Viitattu 31.7.2024). Saatavilla: <https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2024.html>
- Neary, K., Steinberg, S. & Stepan, A. 2021. *NotPetya: A Columbia University Case Study*. (Viitattu 10.8.2024). Saatavilla: <https://www.sipa.columbia.edu/sites/default/files/2022-11/NotPetya%20Final.pdf>
- O'Brien, Siobhan & Davis, Erica. 2020. Silent cyber – no longer silent? (Viitattu 20.10.2024). Saatavilla: <https://www.proquest.com/docview/2424854547?pq-origsite=primo&accountid=14242&sourcetype=Trade%20Journals>
- Ollila, K. 2024. Tietoevryyn kohdistunut hyökkäys nosti kybervakuutukset pinnalle – tällaisia vahinkoja ne korvaavat. Tivi. (Viitattu 20.8.2024). Saatavilla: <https://www.tivi.fi/uutiset/tietoevryyn-kohdistunut-hyokkays-nosti-kybervakuutukset-pinnalle-tallaisia-vahinkoja-ne-korvaavat/be1ac8e2-942e-4ea2-ab09-08fe70bd8ad5>
- PWC. 2023. PwC:n katsaus suomalaisyrityksiin: Riskienhallinnan merkitys korostunut. (Viitattu 18.8.2024). Saatavilla: <https://uutishuone.pwc.fi/pwcn-katsaus-suomalaisyrityksiin-riskienhallinnan-merkitys-korostunut>
- Railio, A. 2021. Kybervakuutuksella voi maksaa lunnaat – maksaminen kuitenkin tukee rikollista toimintaa. (Viitattu 10.9.2024). Saatavilla: <https://www.kauppalehti.fi/uutiset/kybervakuutuksella-voi-maksaa-lunnaat-maksaminen-kuitenkin-tukee-rikollista-toimintaa/af9e8c77-2242-4eb0-b868-2509fa01479d>
- Ratcliffe, S. 2016. *Oxford Essential Quotations*, Amara Roy Quotation, Oxford University Press, Oxford. (Viitattu 8.8.2024). Saatavilla: <http://www.oxfordreference.com/view/10.1093/acref/9780191826719.001.0001/q-oro-ed4-00018679>.
- Shamma, B. 2018. *Implementing CIS Critical Security Controls for Organizations on a Low-Budget*. Master's thesis, University of Houston.
- Sibakov, J. 2020. *Suomessa yksi ala on kyberturvallisuuden edelläkävijä – ”On hyvä päästä reaktiivisesta toiminnasta ennakoivaan tekemiseen”* Kauppalehti. (Viitattu 1.8.2024). Saatavilla: <https://www.kauppalehti.fi/uutiset/suomessa-yksi-ala-on-kyberturvallisuuden-edellakavija-on-hyva-paasta-reaktiivisesta-toiminnasta-ennakoivaan-tekemiseen/7092379b-ee3b-4a2f-ab8a-bb7778a2a6d5>
- Sjövall, M. 2018. *Cyberspionage kostar de finska företagen miljardbelopp*. Hufvudstadsbladet. (Viitattu 28.7.2024). Saatavilla: <https://www.hbl.fi/artikel/cyberspionage-kostar-de-finska-foretagen-miljardbelopp/>

Smith, I. 2022. Cyber attacks set to become ‘uninsurable’, says Zurich chief. (Viitattu 29.9.2024). Saatavilla: <https://www.ft.com/content/63ea94fa-c6fc-449f-b2b8-ea29cc83637d>

Suomen Yrittäjät. 2020. Yrittäjyystilastot. (Viitattu 20.9.2024). Saatavilla: <https://www.yrittajat.fi/wp-content/uploads/2022/08/Yrittajyystilastot-2020.pdf>

Suutari, E. 2021. Kun Saksassa tulvii, se näkyy Suomen vakuutusmarkkinoilla. (Viitattu 30.9.2024). Saatavilla: <https://www.aamulehti.fi/talous/art-2000008412294.html>

Toivonen, J. 2017. Viisi prosenttia pk-yrityksistä on joutunut kyberhyökkäysten kohteeksi. (Viitattu 28.7.2024). Saatavilla: <https://yle.fi/a/3-9510341>

Traficom. 2024. Tietoturvan vuosi 2023: kyberturvallisuuden vuosikatsaus. (Viitattu 22.7.2024). Saatavilla: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/TRAFICOM_Tietoturvan_vuosi-2023_web.pdf

World Economic Forum .2024. Global cybersecurity outlook 2024. (Viitattu 1.10.2024). Saatavilla: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf

Zurich. 2023. Study highlights 10 Cyber controls reducing 70% most frequent attacks. (Viitattu 30.9.2024). Saatavilla: <https://www.zurich.com/commercial-insurance/sustainability-and-insights/commercial-insurance-risk-insights/study-highlights-10-cyber-controls-reducing-70-most-frequent-attacks>

Henkilölähteet

Asiantuntija A. Kybervakuutusmeklari. Haastattelu 15.10.2024.

Asiantuntija B. Kybervakuutusmeklari. Haastattelu 18.10.2024.

Asiantuntija C. Kyberturvallisuusasiantuntija. Haastattelu 23.10.2024.

Asiantuntija D. Underwriter, kybervakuutukset. Haastattelu 21.10.2024.

Asiantuntija E. Underwriter, kybervakuutukset. Haastattelu 16.10.2024.

Asiantuntija F. Underwriter, kybervakuutukset. Haastattelu 17.10.2024

LIITTEET

Liite 1: Asiantuntijoiden haastattelurunko

Kyberriskien kontrollivaatimukset

1. Miten määrittelet kyberriskien kontrollit ja millaisena näet niiden merkityksen?
2. Millaisia kontrollivaatimuksia kybervakuuttajat esittävät pk-yrityksille, mitkä ovat niistä keskeisimpiä?
3. Mitkä ovat oleellisimpia seikkoja, joita vakuuttajat arvioivat pk-yritysten kyberriskien osalta ennen kontrollivaatimusten asettamista?
4. Miten kontrollivaatimustasot ovat muuttuneet kybervakuuttamisen lyhyessä historiassa ja mitkä ovat olleet vahvimpia muutosajureita?

Kyberkontrollit osana pk-yrityksen riskienhallintaa

5. Millaisena näet vakuutusyhtiön roolin kyberriskien hallinnan osalta?
6. Entä kuinka merkittävä osatekijä asetetut kontrollivaatimukset ovat yrityksen riskienhallinnan näkökulmasta?
7. Miten kontrollivaatimusten täytyminen varmistetaan ja seurataanko niitä vakuutuksen myöntämisen jälkeen?
8. Miten kontrollivaatimukset ovat vaikuttaneet mielestäsi pk-yritysten kyberturvallisuuden yleiseen tasoon?
9. Millaisiin kyberriskeihin kontrollit vaikuttavat kaikista heikoiten tai ei sovellu lainkaan?

Haasteet ja kehitysmahdollisuudet

10. Mitkä ovat tällä hetkellä keskeisimpiä haasteita kyberriskien kontrolleissa vakuuttamisen näkökulmasta?
11. Voiko kontrollivaatimukset vaatia liikaa resursseja pk-yritykseltä?
12. Miten kontrollivaatimusten prosessia voitaisiin mielestäsi käytännön tasolla kehittää?
13. Millaisena näet yleisen kehityksen kontrollivaatimusten osalta vakuuttamisen kontekstissa?
14. Mitkä ovat suurimmat mahdollisuudet liittyen teknologiseen kehitykseen?