Huoltovarmuusorganisaatio
Digipooli

Turvallisuudenhallinnan painopisteet

Huoltovarmuusorganisaation Digipoolin kokonaisturvallisuudenhallinnan selvitys 2024

Antti Nyqvist

Huoltovarmuusorganisaation Digipooli

Teknologiateollisuus ry

Tiivistelmä

Huoltovarmuusorganisaation Digipoolin yritysten kokonaisturvallisuuden tilaa on selvitetty, koska alan yritysten turvallisuudenhallinta on keskittynyt kyberturvallisuuteen ja kokonaisturvallisuuden aiheiden tilaa ei tunneta. Tietoa tarvitaan alan yritysten tukemiseksi.

Työn pohjaksi tehtiin kysely ja haastatteluita. Niiden avulla selvitettiin turvallisuudenhallinnan organisoitumista, strategista ohjausta, sovellettuja standardeja ja osa-alueiden kypsyyttä. Pohjatyö tarjosi tietoa yritysten tilanteesta ja turvallisuudenhallinnan kehityksen vaikuttimista.

Työssä avataan kirjallisuustutkimuksen keinoin huoltovarmuuden kontekstia, yritysturvallisuuden malleja ja nostetaan esiin kontekstissa oleellisia riskejä sekä pohditaan EU:n direktiivien vaikutuksia yritysten turvallisuudenhallintaan.

Työn keskeisinä tuloksina ovat kyselyn ja haastatteluiden perusteella tuotettu riskikartta sekä priorisoitu lista kehitettävistä yritysturvallisuuden osa-alueista ja erittely osa-alueittain tärkeiksi koetuista kehitysaiheista sekä visiotila tarvittavista muutoksista. Muina tuloksina on havaintoja strategian ohjaavasta vaikutuksesta ja organisoitumisen vaikutuksista turvallisuudenhallintaan.

Johtopäätöksinä on mm. tarve määritellä hyvä turvallisuuden taso ja tarve keskustella riskienhallinnan mallien laajemmasta soveltamisesta alalla.

Abstract

The state of comprehensive security of companies in the National emergency Suppy Organization Digipool network is being investigated because the security management of companies in the field is focused on cyber security and the state of other comprehensive security topics is not known. Information is needed to support companies in the field.

A survey and interviews were conducted as the basis for the work. They were used to investigate security management organization, strategic guidance, applied standards, and the maturity of sub-areas. The basis provided information on maturity of companies and the drivers of security management development.

The work presents the context of security of supply, models of corporate security, and highlights risks relevant in the context through literature research, and briefly touches the effects of EU directives on security management.

The main results are a produced risk map and a prioritized list of corporate security sub-areas to be developed and a breakdown of development topics considered important by sub-area, as well as a vision state of the necessary changes. Other results include observations on the guiding effect of strategy and the effects of organization on security management.

The conclusions include the need to define a good level of security and the need to discuss the wider application of risk management models in the field.

Sisältö

1 Johdanto

1.1 Työn tausta

Tämä työ liittyy Huoltovarmuusorganisaation pooleille asetettuun tavoitteeseen, jolla kehitetään verkoston yritysten kokonaisturvallisuuden hallintaa. Tässä työssä keskitytään Huoltovarmuusorganisaation Digipoolin ICT-alan yrityksiin.

Digipoolin kannalta voidaan tämän työn tuottaman tiedon perusteella paremmin suunnitella ja kohdistaa yrityksille koulutuksia, harjoituksia ja huoltovarmuusorganisaatiossa tuotettua materiaalia. Ja toisaalta voidaan paremmin tunnistaa niitä aiheita, joihin tulee tuottaa tukea (lisää materiaaleja, koulutusta ja harjoituksia).

Huoltovarmuuskeskuksen näkökulmasta edellä mainittu pätee kaikkiin pooleihin eri toimialoilla, ja kokonaisuutena huoltovarmuus paranee, kun turvallisuudenhallinnan painotukset tunnetaan paremmin ja voidaan ohjata toimenpiteitä tiedon perusteella.

Huoltovarmuuskeskuksen hallituksen linjaukset pooleille (vuodelle 2023) edellyttävät myös seuraavia toimenpiteitä, mihin tällä työllä tuotetulla tiedolla on merkittävä vaikutus:

- Kannustaa laatimaan ja päivittämään poikkeusolojen sekä niihin verrattavissa olevien vakavien häiriöiden varalta toimintoja koskevat yleissuunnitelmat.
- Sektorit, poolit ja toimikunnat kehittävät huoltovarmuustoiminnan yhdenmukaisuutta yhdessä Huoltovarmuuskeskuksen kanssa.

Tällä työllä tuotetaan tietoa kyseisten suunnitelmien tekemiseksi ja kehitetään erityisesti Digipoolin toimintaa huomioimaan paremmin kokonaisturvallisuutta.

1.2 Työn tavoitteet

Työn keskeisenä tavoitteena on tuntea Huoltovarmuusorganisaation Digipoolin yritysten kokonaisturvallisuuden ohjauksen ja hallinnan nykytila ja kehitystarpeet. Kuinka esim. fyysisen suojauksen toimenpiteet ja kyberturvallisuuden toimenpiteet ovat suhteessa toisiinsa, ja missä aiheissa on syytä parantaa. Lisäksi työ pyrkii tuottamaan tietoa siitä, mihin aiheisiin riskiperusteisesti painottamalla ja nykytilaa arvioimalla tulisi kiinnittää alalla huomiota.

Tavoitteeseen kuuluu myös tavoitetason tai kehitysaiheiden suosittelu ja tulosten käsittely Digipoolin työryhmissä. Käsittelyn avulla pyritään (tähän työhön kuulumattomasti) löytämään toimenpiteitä, joiden avulla yritykset lähtisivät kehittämään toimintaansa työn esittämissä aiheissa.

Tutkimusongelmaan päädyttiin, sillä etsittäessä tietoa yritysten kokonaisturvallisuuden hallinnan tilanteesta, aiheesta ei löydetty kotimaisia tutkimuksia.

1.3 Tutkimusmenetelmä

Tuntemusta, eli tietoa yritysten tilanteesta kerättiin kyselyllä ja haastatteluilla. Kysely toimi EK yritysturvallisuusmallin[1] osa-alueiden kypsyyden itsearviointina ja tarjosi tietoa muista kokonaisturvallisuuden hallintaan vaikuttavista aiheista. Haastattelulla kerättiin tietoa kypsyydestä, mutta saatiin myös syventävää tietoa yritysten tilanteeseen vaikuttavista päätöksistä ja painotuksista.

Perusteluita toimenpiteille, riskipeilausta ja painotusta haettiin ns. kirjallisuustutkimuksella, joka keräsi tietoa olemassa olevista alaa koskevista tavoitteita asettavista tietolähteistä ja riskikokoelmista. Tärkeimpinä lähteinä mainittakoon Yhteiskunnan turvallisuusstrategia vuodelta 2017, Suomen kyberturvallisuusstrategia vuodelta 2019 ja Valtioneuvoston päätös huoltovarmuuden tavoitteista vuodelta 2018. Tieto koostettiin osaksi työtä, jotta sen avulla voitiin painottaa kokonaisturvallisuuden aiheita yhdessä kypsyystiedon kanssa.

Lopulta turvallisuuden osa-alueiden kypsyys suhteutettiin tunnettuihin riskiaiheisiin. Riskien oleellisuus alan yrityksille arvioitiin ja annettiin sille suhdeluku, jolla painotettiin osa-alueiden suhteellista kypsyyttä. Näin saatiin riskien ja kypsyyden perusteella painotettu prioriteettijärjestys turvallisuuden osa-alueille ICT-alalla huomioitavaksi.

1.4 Tavoitteiden painotus

Työn tavoitteista voidaan tunnistaa ensisijainen tietotarve ja useita toissijaisia tietotarpeita. Toissijaiset aiheet tuottavat tietoa, joka selittää sitä miksi ensisijainen selvitettävä asia on kuten väitetään.

Ensisijaisesti selvitetään:

- Turvallisuudenhallinnan osa-alueiden kypsyys eli varautumisen taso kokonaisturvallisuuden hallinnan aiheissa

Täydentävää tietoa haetaan seuraavista aiheista:

- Kuinka turvallisuus on organisoitu tai ohjattu yrityksessä?
- Paljonko eri aiheiden (erit. tietoturvallisuuden) varautumiseen käytetään resursseja suhteessa muihin kokonaisturvallisuuden aiheisiin?
- Mitkä ovat turvallisuuden raportoinnin tai tilannekuvan painopisteet organisaatioissa?
- Mitä kokonaisturvallisuuden aiheita näkyy yrityksen strategiassa?

[1] Lähde [5] Yritysturvallisuusmalli, Elinkeinoelämän keskusliitto, 1987, päivitetty 2020

- Mitä aiheita käsitellään vastuullisuus otsikon alla?
- Yritysten valmius NIS2 ja CER direktiiveistä poikiviin vaatimuksiin?

1.5 Tutkimuksen rajaukset

Kysely ja haastattelut rajattiin koskemaan yrityksen Suomessa toteutettavia toimintoja, jotka ovat oleellisia huoltovarmuusorganisaation toiminnalle. Rajaus eliminoi samalla eri maissa erilaisiksi tunnetut painotukset ja niiden vaikutukset tuloksiin.

Kysely ja haastattelut ja siten koko tutkimus rajattiin Huoltovarmuusorganisaation Digipoolin yrityksiin eli ICT-, tele-, ohjelmisto- ja kyberalan yrityksiin. Tuloksena on siis tietoa alan yritysten kokonaisturvallisuudenhallinnan tilasta.

1.6 Tutkimuksen aineisto

Aineistona on aihepiiriin kuuluvat ja tunnetut tietolähteet elinkeinoelämää koskevista riskeistä.

1.7 Terminologia

Taulukko 1 Työn terminologiaa

Termi	Selite
direktiivi	Ohjailevassa tehtävässä käytetty lausuma. Direktiivisellä lausumalla puhuja käskee, kehottaa, pyytää, ehdottaa tai neuvoo puhuteltavaa toimimaan tai kieltää tai varoittaa häntä toimimasta tietyllä tavalla.
huoltovarmuus	Yleisesti huoltovarmuudella tarkoitetaan kykyä sellaisten yhteiskunnan taloudellisten perustoimintojen ylläpitämiseen, jotka ovat välttämättömiä väestön elinmahdollisuuksien, yhteiskunnan toimivuuden ja turvallisuuden sekä maanpuolustuksen materiaalisten edellytysten turvaamiseksi vakavissa häiriöissä ja poikkeusoloissa.
huoltovarmuusorganisaatio	Huoltovarmuusorganisaatio (HVO) on verkosto, joka työskentelee yhdessä Suomen toimintakyvyn ja sen edellyttämän huoltovarmuuden hyväksi. Siihen kuuluvat Huoltovarmuuskeskus (HVK) ja sen hallitus, huoltovarmuusneuvosto sekä eri toimialojen sektorit ja poolit. Lisäksi yhteistyötä tehdään alueellisten toimijoiden, kuten aluehallintovirastojen, kuntien ja kaupunkien sekä useiden alueellisten toimikuntien kanssa.
kyberresilienssi	Kyberhäiriöiden sietokyky, varautuminen ja toipumiskyky häiriön ilmetessä
pooli	Huoltovarmuusorganisaation poolit toteuttavat elinkeinoelämän ja julkishallinnon yhteistyötä. Pooleihin kuuluu tyypillisesti julkisen sektorin, yritysten, järjestöjen ja kolmannen sektorin toimijoita.

riski	Kielteisen seikan tai tapahtuman todennäköisyyden ja vaikutusten yhdistelmä.
standardi	Standardi on jonkin organisaation esittämä määritelmä siitä, miten jokin asia tulisi tehdä.
uhka	Mahdollisesti toteutuva haitallinen tapahtuma tai kehityskulku, joka uhkaa liiketoiminnan jatkuvuutta tai huoltovarmuutta laajemmin.
VAP-varaus	Henkilövaraus tai Vapaaehtoinen asepalvelusvaraus
yritysturvallisuuden osa-alueet	Tässä työssä yritysturvallisuuteen viitattaessa tarkoitetaan EK:n yritysturvallisuusmallia ja sen eri osa-alueita, jotka ovat eritelty alaluvussa 2.3.1.

2 Tausta ja viitekehys

2.1 Huoltovarmuuskeskus ja kytkös yritysturvallisuuteen

Huoltovarmuuskeskuksen mission[2] (”Huoltovarmuuskeskus huolehtii yhdessä yrityselämän, kolmannen sektorin ja viranomaistahojen kanssa siitä, että myös kriisitilanteissa yhteiskunta toimii ja elämä jatkuu mahdollisimman häiriöttä.”) mukaisesti toiminnan ytimessä on yhteistyö yritysten kanssa. Usein yhteiskunnan huoltovarmuus on myös kiinni yritysten kyvystä tuottaa palveluitaan erilaisissa häiriötilanteissa ja erityisesti tällöin on yritysten liiketoiminnan suojaaminen keskeisessä roolissa. Suomalaisen huoltovarmuusmallin mukaan yritykset ovat itse vastuussa turvallisuutensa järjestämisessä, mutta em. yhteistyön myötä kehitetään yritystenkin turvallisuutta huoltovarmuus ja yhteiskunnan tarpeet huomioiden.

Huoltovarmuuskeskuksesta ja sen roolista elinkeinoelämän toimintaedellytysten turvaajana puhutaan turhan harvoin ja merkittävää on myös se, että keskus on valtion budjetista riippumaton toimija. Riippumattomuus tulee Huoltovarmuuskeskuksen hallinnoimasta huoltovarmuusrahastosta. Rahaston olemassaolo ja huoltovarmuuskeskuksen hallintomallin kyky käyttää rahoitusta mahdollistaa toiminnan häiriötilanteissa, kun valtion budjetissa ei ole rahaa aiheeseen varattuna. Tätä kirjoitettaessa on 2023 aloittaneen Suomen hallituksen hallitusohjelmaan kirjattu tehtäväksi määritellä uusi kestävä pohja huoltovarmuusrahaston toiminnalle.

2.1.1 Huoltovarmuuskeskuksen strategia

Tätä kirjoitettaessa on viimeisin huoltovarmuuskeskuksen strategiakausi päättymässä ja uutta strategiaa luodaan tuleville vuosille. Voimassa oleva strategia[3] on vuosille 2021-2023 ja se määrittelee

[2] Lähde [9] Huoltovarmuuskeskuksen strategia yhteenveto, s. 4
[3] Lähde [8] Huoltovarmuuskeskuksen strategia

mm. johdannossa mainitun mission toiminnalle. Mission lisäksi strategia kertoo kehittämiskokonaisuuksista ja hahmottelee tiekarttaa kehitykselle, erittelee kriittisiä kyvykkyyksiä sekä asettaa tavoitteita toiminnalle.

Strategia määrittelee huoltovarmuuskeskukselle monia tehtäviä, jotka jollain tapaa vaikuttavat elinkeinoelämän toimintaan. Sellaisia ovat mm. tehtävät, joita toteutetaan suoraan Huoltovarmuuskeskuksen toimin tai yhteistyöverkoston (Huoltovarmuusorganisaatio) avulla:

- Sopimuksellisten varautumisjärjestelyjen tekeminen yritysten kanssa
- Kriittisten teknisten järjestelmien toimivuuden varmistaminen
- Huoltovarmuustoiminnan yhteistyöverkostojen ylläpitäminen ja koordinointi
- Julkishallinnon ja elinkeinoelämän varautumistoiminnan yhteensovittaminen
- Elinkeinoelämän varautumisen ohjaus
- Elinkeinoelämän jatkuvuudenhallinnan ja varautumisen tukeminen
- Laaja-alaisen elinkeinoelämää ja kansainvälisiä arvoketjuja kattavan tilannekuvan muodostaminen ja jakaminen yhteistyössä pooliorganisaation ja muiden yhteistyötahojen kanssa

Tavoitteikseen Huoltovarmuuskeskus on nostanut mm. sen, että toiminnan on määrä tuottaa selkeää lisäarvoa yritysten jatkuvuudenhallinnalle ja tekee sitä mm. tuottamalla huoltovarmuuden jatkuvaa tilannetietoisuuden ja häiriötilanteiden tilannekuvaa sidosryhmilleen.

Strategian esittelemien kehitysohjelmien aiheissa nousevat esiin edellisiin tavoitteisiin liittyen riskienhallinnan kehittäminen, havainnoinnin ja tilannekuvatoiminnan kehitys sekä poolitoiminnan ja sidosryhmäyhteistyön kehitys.

2.1.2 Huoltovarmuusorganisaation tehtävä

Huoltovarmuusorganisaatio toteuttaa toiminnassaan monia Huoltovarmuuskeskuksen strategiassa esittelemiä tehtäviä[4] ja samalla sille varataan mahdollisuus nostaa esiin elinkeinoelämän tarpeista nousevia toimenpide-ehdotuksia, joilla varmistetaan toimintaa tai muuten parannetaan huoltovarmuutta.

Huoltovarmuusorganisaatioon luetaan kuuluvaksi huoltovarmuusneuvosto, Huoltovarmuuskeskus ja sen hallitus sekä eri toimialojen sektorit ja poolit. Lisäksi yhteistyötä tehdään alueellisten toimijoiden, kuten aluehallintovirastojen, kuntien ja kaupunkien sekä useiden alueellisten toimikuntien kanssa. Valtaosassa näitä rakenteita kohtaavat julkishallinto ja elinkeinoelämän edustus sekä järjestöt ja kolmas sektori.

[4] Lähde [8] Huoltovarmuuskeskuksen strategia 2021, s. 13

Huoltovarmuusorganisaation toiminnan tavoitteena on turvata huoltovarmuuden kannalta kriittisten organisaatioiden ja sitä kautta koko yhteiskunnan toimintaedellytykset kaikissa olosuhteissa.

2.1.3 Digipooli ja Digipoolin tehtävä

Digipooli on yritysten ja viranomaisten yhteistyöhön perustuva luottamusverkosto, joka edistää yhteiskunnan digitaalista varautumista. Toiminnan kautta vahvistetaan yritysten kykyä ennakoida häiriötilanteita ja toipua niistä. Pooli on olemassa auttaakseen yrityksiä menestymään vastuullisesti ja turvallisesti.

Digipoolin kuten muidenkin poolien tehtävänä on tukea yrityksiä niiden kehityspyrkimyksissä kokonaisturvallisuuden aiheissa, koska logiikkana on se, että mitä paremmin elinkeinoelämä on liiketoimintansa jatkuvuuden varmistanut sitä paremmin toimivat häiriötilanteissa niiden tuottamat kriittiset palvelut. Monipuolisella yritysten kanssa tehtävällä yhteistyöllä voidaan tunnistaa niitä aiheita, joissa voidaan tehdä huoltovarmuutta tukevia toimenpiteitä.

Huoltovarmuuskeskuksen strategisen ohjauksen mukaan huoltovarmuusorganisaation sektoreilla ja pooleilla on toisiaan tukevia tehtäviä, ja Digipooli toteuttaa toiminnassaan niin sektorien kuin poolienkin tehtäviä[5]. Digipoolin toiminnalla vaikutetaan horisontaalisesti koko Huoltovarmuusorganisaation toimintaan.

Digipoolin omassa strategiassa korostuu neljä kokonaisuutta, joiden kautta toteutetaan em. tehtäviä.

- Strateginen halu
- Tilannekuva ja tietoisuus
- Verkostot ja keskinäisriippuvuudet
- Työkalut ja osaaminen

Digipooli pyrkii herättelemään yritysjohtoa toimenpiteisiin varautumisen aiheissa ja erityisesti kyberturvallisuuteen liittyen, mutta kokonaisturvallisuutta unohtamatta. Ja kun toimintaa yrityksissä saadaan aikaan, pyrkii vaikuttamaan resurssien käytön tehokkuuteen ohjaamalla niitä aiheisiin, joista yrityksille on lisäarvoa. Digipooli kannustaa yrityksiään verkostoitumaan, muodostamaan tilannekuvaa sekä hyödyntämään työkaluja ja osaamista.

2.2 Riskejä ja uhkia huomioitavaksi

Tässä alaluvussa tarkastellaan keskeisiä ICT-yritysten huomioitavaksi nousevia toimintoja ja niihin liittyviä uhkia. Seuraavissa kappaleissa esitellään niistä kansallisesti tunnetuimmat ja tunnistetaan

[5] https://www.huoltovarmuuskeskus.fi/huoltovarmuusorganisaatio/sektorit-ja-poolit

niistä sellaiset, jotka tulisivat ensisijaisesti huomioida ICT-yritysten turvallisuudenhallinnassa. Kappaleessa esitellään myös kansainvälisiä verrokkeja yrityksiin kohdistuvista uhista. Kappaleen viimeinen luku vetää yhteen uhka- ja riskiaiheet. Jäljempänä työssä esitellään yritysten turvallisuudenhallinnan tilanne ja peilataan sitä näihin uhkiin.

2.2.1 Yhteiskunnan turvallisuusstrategia

Yhteiskunnan turvallisuusstrategia vuodelta 2017[6] on valtioneuvoston periaatepäätös, joka yhtenäistää varautumisen kansallisia periaatteita ja ohjaa hallinnonalojen varautumista. Strategia on ensimmäisen kerran laadittu 2010 ja päivitetty epäsäännöllisesti turvallisuusympäristön muutoskohdissa kuten 2013 ja viimeisimmän kerranvuonna 2017. Strategiassa esitetään kokonaisturvallisuuden yhteistoimintamalli, jota sovelletaan laajasti julkishallinnossa, kun varaudutaan erilaisiin häiriötilanteisiin. Yhteiskunnan turvallisuusstrategia (YTS) on tehty laajassa yhteistyössä viranomaisten, elinkeinoelämän, järjestöjen ja kansalaisten kesken.

Strategia kuvaa ne toiminnot, joiden tulee toimia niin normaaliolojen häiriötilanteissa kuin poikkeusoloissa. Ja monien toimintojen osalta ICT-alan yritykset tuottavat palveluita näihin liittyen – tällöin myös yrityksen tulee varautua varmistamaan toimintansa erilaisissa häiriötilanteissa. Turvallisuusstrategia lähtee siitä, että sen erittelemien toimintojen kanssa tekemisissä olevien toimijoiden tulee huomioida vähintään kolmen vuoden välein päivitettävää kansallista riskiarviota. YTS ei tarkemmin erittele uhkia ja riskejä näihin toimintoihin ja tehtäviin liittyen, vaan viittaa kansalliseen riskiarvioon, joka tarkemmin erittelee ne uhat. (kts. alaluku 2.2.3).

Strategiassa määritellään yhteiskunnan elintärkeät toiminnot, joiden jatkuminen on pystyttävä takaamaan kaikissa olosuhteissa, kaikilla toimintatasoilla. Seuraavaan taulukkoon on koottu ne kriittiset toiminnot ja niihin liittyvät tehtävät.

Taulukko 2 YTS kansalliset toiminnot ja strategiset tehtävät

Aihe	Kriittiset tehtävät
Johtaminen	• Valtion ylimmän johdon toimintaedellytysten turvaaminen • Valtion ylimmän johdon tilannekuvan ylläpitäminen • Viestinnän toimivuus
Kansainvälinen ja EU toiminta	• Suomen toiminta Euroopan unionissa; EU-asioiden kansallisen valmistelun ja käsittelyn, yhteisvastuun sekä keski-näisen avunannon turvaaminen • Yhteyksien ja yhteistyön kehittäminen ulkovaltojen ja keskeisten kansainvälisten toimijoiden kanssa • Kansainvälinen kriisinhallinta, humanitaarinen apu sekä kansainvälinen pelastustoiminta • Suomen kansalaisten ja Suomessa pysyvästi asuvien ulkomaalaisten suojelu ja avustaminen ulkomailla • Suomen ulkomaankaupan sujuvuuden ja häiriöttömyyden varmistaminen
Puolustuskyky	• Suomen sotilaallinen puolustaminen

[6] Lähde [1] Yhteiskunnan turvallisuusstrategia, 2017

Sisäinen turvallisuus	• Oikeusturvajärjestelmän toimintakyvyn turvaaminen • Vaalien toimeenpano ja demokratian edellytysten turvaaminen • Yleisen järjestyksen ja turvallisuuden ylläpitäminen • Rajaturvallisuuden varmistaminen • Toimitusketjujen turvallisuuden ja tavaraturvallisuuden varmistaminen • Väestön suojaaminen • Meripelastustoimen suorituskyvyn varmistaminen • Hätäkeskustoiminta • Pelastustoimen ylläpito • Laajamittaisen maahanmuuton hallinta • Ympäristövahinkojen torjunta ja ennaltaehkäisy • Biologisiin uhkiin varautuminen • Säteilyvaaratilanteiden estäminen ja niihin varautuminen • Kemikaaliuhkiin varautuminen
Talous, infrastruktuuri ja huoltovarmuus	• Taloudellisten voimavarojen hankkiminen ja kohdentaminen sekä henkilövoimavarojen varmistaminen • Rahoitusjärjestelmän toiminnan turvaaminen • Julkisen hallinnon ICT-infrastruktuurin ja digitaalisten palvelujen turvaaminen • Sähköisten viestintäpalvelujen käytettävyyden ja saatavuuden varmistaminen • Vakuutustoiminnan turvaaminen • Polttoainehuollon turvaaminen • Voimahuollon turvaaminen • Sää-, meri- ja olosuhdepalvelujen saatavuuden varmistaminen • Liikennepalvelujen käytettävyyden ja saatavuuden varmistaminen • Liikenne- ja viestintäverkkojen turvallisuuden ja toimintavarmuuden varmistaminen • Suomen huoltovarmuuteen ja ulkomaankauppaan liittyvien kuljetusten jatkuvuuden varmistaminen • Sosiaali- ja terveydenhuollon tietojärjestelmien toimivuuden sekä keskeisten tarvikkeiden saatavuuden turvaaminen • Ympäristön muutosten havainnointi ja seuranta sekä muutoksiin sopeutuminen ja niistä aiheutuvien uhkien torjunta • Jätehuollon turvaaminen • Rakentamisen turvaaminen • Asumisen turvaaminen • Vesihuollon turvaaminen • Tulvariskien hallinta ja patoturvallisuuden valvonta • Työvoiman saannin turvaaminen • Koulutus- ja tutkimusjärjestelmän ylläpitäminen • Elintärkeän teollisuus- ja palvelutuotannon turvaaminen • Elintarvikehuollon turvaaminen • Päivittäistavarahuollon turvaaminen
Väestön toimintakyky ja palvelut	• Väestön viimesijaisen toimeentulon turvaaminen • Sosiaali- ja terveydenhuollon palvelujen turvaaminen • Osaamisen ylläpitäminen
Henkinen kriisinkestävyys	• Kulttuuripalvelujen ylläpitäminen ja kulttuuriomaisuuden suojelu • Hengellisen toiminnan edellytysten turvaaminen • Nuorisotyön ja -toiminnan sekä liikunnan kansalaistoiminnan ylläpitäminen • Viestintä • Syrjäytymisen ja eriarvoisuuden ehkäiseminen • Vapaaehtoistoiminnan edistäminen • Väestön toipuminen

2.2.2 Kyberturvallisuusstrategia

Suomen kyberturvallisuusstrategia vuodelta 2019[7] on valtioneuvoston periaatepäätös, jolla linjataan niistä periaatteista, joiden mukaan kyberturvallisuuden tulee toteutua yhteiskunnassa. Ensimmäisen kerran kyberstrategia laadittiin vuonna 2013 ja sitä on päivitetty epäsäännöllisesti turvallisuusympäristön muuttuessa. Kyberturvallisuusstrategia ei erittele yhteiskunnalle kriittisiä kyberturvallisuudesta riippuvaisia toimintoja tai niihin liittyviä uhkia. Mutta se nostaa esiin kyberresilienssin kannalta merkittäviä, yritysten varautumisessa huomioitavia aiheita:

- Kansainvälinen yhteistyö ja tiedonvaihto
  - Tiedonvaihto häiriötilanteissa selviytymiseksi ja suojautumiseksi
- Johtamisen koordinaatio
  - Kriittisten tietovarantojen, digitaalisten palveluiden ja infrastruktuurin määrittely
  - Viranomaisten palveluiden käyttö ja viranomaisyhteistyö
  - Yritysten palvelutuotannon ja jatkuvuudenhallinnan tukeminen
- Osaamisen kehittäminen
  - Pätevän työvoiman varmistaminen

2.2.3 Kansallinen riskiarvio

Kansallinen riskiarvio laaditaan kolmen vuoden välein ja sen tavoitteena on ennakoida Suomeen kohdistuvia äkillisiä tapahtumia, jotka vaativat viranomaisilta normaalista poikkeavia toimia tai jopa avun pyytämistä. Kansallisessa riskiarviossa tunnistetaan riskejä, jotka voivat vaikuttaa yhteiskunnan kriittisiin toimintoihin (kts. Taulukko 2).

Jos tarkastellaan viimeisimmässä kansallisessa riskiarviossa[8] vuodelta 2023 esiteltyjä uhkia niin, että jäsennetään ne ”Talous, infrastruktuuri ja huoltovarmuus” vaikutusten mukaan järjestykseen suurimmasta pienimpään sekä jätetään sieltä huomioimatta sellaiset uhat, joihin ei ole suoria keinoja lähteä yrityksissä varautumaan, saadaan seuraava erittely ICT yrityksille relevanteista huomioitavista uhista:

Taulukko 1 Kansallisen riskiarvion perusteella yrityksien huomioitavat uhat

Uhkamalli	Vaikutukset
Rahoitusjärjestelmän häiriö	3
Sähkön saannin suurhäiriö	3
Tieto- ja viestintäverkkojen ja palveluiden häiriöt	3
Kuljetusten jatkuvuuden häiriöt	3
Pandemia tai muu vastaava laajalle levinnyt epidemia	3
Vakava ydinvoimalaitosonnettomuus Suomessa tai Suomen lähialueilla	3
Informaatiovaikuttaminen	2

[7] Lähde [2] Suomen kyberturvallisuusstrategia, 2019
[8] Lähde [3] Kansallinen riskiarvio 2023, Sisäministeriö, 2023

Polttoaineiden saannin vakavat häiriöt	2
Mikrobilääkeresistenssi	2
Äärimmäisen voimakas avaruusmyrsky	2

Kansallisen riskiarvion aiheet ovat korkealla tasolla, mutta jokaisesta uhasta on johdettavissa jatkuvuutta uhkaavia riskejä.

2.2.4 Kansallisen turvallisuuden katsaus

Suojelupoliisin kansallisen turvallisuuden katsaus vuodelta 2023[9] nostaa esiin seuraavia uhkia:

- Tiedustelun ja vaikuttamisen uhka
  - Tiedonhankinta (esim. tuotekehityksestä)
  - Informaatiovaikuttaminen, jolla halutaan luoda epävakautta
- Terrorismi uhka
  - Digitaalisen rahansiirron käytön ja virtuaalivaluuttojen yleistymisen myötä epävirallisen pankki- ja rahansiirtopalvelusektorin vahvistuminen
- Uhkien jatkuva muutos
  - Verkkolaitteiden suojaamattomuus
  - Kriittisen infrastruktuurin riippuvuus avaruudesta (esim. satelliittiaika- ja paikkatieto, sekä varayhteydet)
  - Kauppapakotteiden kiertäminen (esim. häivyttämällä hankintaketjuista tieto todellisesta ostajasta sekä hankkimalla tuotteita kolmansien maiden kautta)
  - Nousevien teknologioiden kaksikäyttösovellutusten ja vientivalvonnan aukkojen hyödyntäminen
  - Kotimaisen tutkimuksen ja kehityksen suojaaminen

2.2.5 Valtioneuvoston päätös huoltovarmuuden tavoitteista

Valtioneuvoston päätös huoltovarmuuden tavoitteista vuodelta 2018[10] erittelee huoltovarmuuskriittisiä toimintoja sekä niihin liittyviä uhkia. Päätöksen teksteistä voi tunnistaa seuraavia varautumista vaativia aiheita:

- Kyberhyökkäykset
- Sähköverkon häiriöt
- Hybridivaikuttaminen
- Luonnonilmiöt
- Tartuntataudit
- Sota
- Terrori-iskut
- Taloudelliset kriisit
- Poliittiset kriisit
- Ympäristökriisit

2.2.6 Valtioneuvoston huoltovarmuusselonteko

Valtioneuvoston huoltovarmuusselonteko vuodelta 2022[11] käsittelee pitkälti samoja uhkia tai varautumista vaativia aiheita kuin vuoden 2018 päätös huoltovarmuuden tavoitteista. Huoltovarmuusselonteko korostaa verkostoituneen toiminnan kehittymistä ja toimitusketjujen toiminnan näkökulmia.

[9] Lähde [4] Kansallisen turvallisuuden katsaus 2023, Suojelupoliisi, 2023
[10] Lähde [6] Valtioneuvoston päätös huoltovarmuuden tavoitteista, Valtioneuvosto, 2018
[11] Lähde [7] Huoltovarmuusselonteko 2022, Valtioneuvosto, 2022

2.2.7 Kansainvälisesti tunnistettuja uhkia

Työtä varten etsittiin koosteita yritysten liiketoiminnan jatkuvuuden kohtaamista uhista ja kenties vakuuttavimman summauksen aiheesta tarjosi vuonna 2023 ensimmäisen kerran toteutettu, Allied Universal yrityksen toteuttama, selvitys nimeltä World Security Report. Selvitys kattoi 1775 alan asiantuntijaa yrityksistä 30 eri maassa ympäri maailman.

World Security Report 202312 tarjoaa kattavan listauksen yrityksien kohtaamista sisäisistä ja ulkoisista uhista. Kaikki sen esittämät uhat eivät kuitenkaan ole suoraan tunnistettava sellaisiksi, joita suomessa toimivat ICT yritykset toiminnassaan kohtaisivat, mutta se tarjoaa mahdollisuuden peilata tässä työssä esitettyä uhkalistaa kansainväliseen ja ajankohtaiseen koosteeseen uhista. Seuraava taulukko esittelee raportin erittelemät, yrityksiin kohdistuvat, uhat todennäköisyysjärjestyksessä.

Taulukko 3 World Security Report 2023 erittelemät yrityksiin kohdistuvat uhat

Sisäiset uhat:	Ulkoiset uhat:
Yrityksen resurssien tai tiedon väärinkäyttö	Petos
Luottamuksellisen tiedon vuoto	Kalastelu tai sosiaalinen manipulointi
Petos	Yrityksen kiinteän omaisuuden varkaus
Yrityksen kiinteän omaisuuden varkaus	Tahallinen yrityksen omaisuuden vahingoittaminen
Luvaton pääsy yrityksen tietoihin tai verkkoihin	Vandalismi
Politiikkarikkomukset	Tekijänoikeusrikkomukset
Tekijänoikeusrikkomukset	Hacktivismi
Tahallinen yrityksen omaisuuden vahingoittaminen	Toimitusketjuhyökkäykset
Immateriaalioikeuden alaisen omaisuuden varkaus	Luvaton tunkeutuminen alueelle
Rikkomus muita työntekijöitä kohtaan	Kilpailijan sabotaasi
Sabotaasi	Palveluestohyökkäykset
Teollisuusvakoilu	Rikkomus henkilöstöä kohtaan
	Graffitit
	Sabotaasi
	Tunkeutuminen
	Edistyneet jatkuvat uhat
	Protestit tai mielenosoitukset
	Valtiolliset kyberhyökkäykset
	Aseistettu ryöstö
	Terrorismi
	Kidnappaukset tai sen uhka

[12] Lähde [14] World Security Report 2023, sivu 40 ja 41

2.2.8 Muita lähteitä ICT-alalle relevanttien uhkien tunnistamisessa

Huoltovarmuusorganisaation Digipooli on toteuttanut kyberkypsyyden selvityksiä[13], joissa osana selvitystä on peilattu toimintojen kypsyyttä toimialalle oleellisiin liiketoiminnan riskeihin. Liiketoiminnan riskit on tunnistettu konsulttitahon kansainvälisen asiakasverkoston toiminnasta. Seuraava lista esittelee niitä riskejä:

- Rikollisuus Sisäinen ja/tai ulkoinen petos/kyberrikollisuus.
- Asiakas Asiakkaille aiheutetut menetykset ja vahingot sekä asiakaskato.
- Palvelu Kapasiteetin, kompetenssin, prosessien ja/tai tarpeiden epäsuhdanne.
- Teknologia Vanhentunut, toimimaton ja/tai kehityskelvoton teknologia; koodin tekijänoikeudet ja li senssiehdot. Haavoittuvuudet
- Tuotanto Infran, IT & OT ympäristön, verkon, konesalien, päätelaitteiden toimimattomuus. Kyberhyökkäykset.
- Alihankinta Toimittajien virheet ja muutoshitaus. Kumppanin kyberhäiriö.
- Kehitys Vaatimuksien määrittelyn, suunnittelun ja koodamisen virheet. Ylimääräinen koodi ohjelmistossa tai aukko asetuksissa.
- Henkilöstö Henkilöstön työmotivaation, osaamisen ja toimintakyvyn puute. Henkilöstön vaihtuvuus.
- Häiriö Rauta- ja/tai softaviat. Inhimilliset erehdykset.
- Pandemia Globaalin pandemian moniulotteiset vaikutukset, jotka näkyvät kokonaisvaltaisesti esim. tuotannossa, työntekijöissä, kyberhyökkäyksissä

2.2.9 Yhteenveto uhista ja riskeistä ICT-alan varautumisen näkökulmasta

Huomioiden tässä luvussa 2 esitettyjen lähteiden erittelemiä uhkia ja riskejä voidaan muodostaa yhteenveto ICT-alan yritysten liiketoiminnalle oleellisista riskeistä. Jokainen uhka-aihe tulee yrityksen liiketoimintojen osalta käsitellä vielä tapauskohtaisesti niin, että arvioidaan kunkin osalta se, mitä kyseinen aihe voisi vaikuttaa.

Erittely palvelee tässä työssä kuitenkin peilauksen kohteena ja sen avulla voidaan arvioida, onko ICT alan yritysten kokonaisturvallisuudenhallinnan kypsyyksissä parannettavaa, kun niitä tarkastellaan näiden riskiaiheiden kautta.

Havaintona luvun 2 esittelemistä lähteistä kootuista riskeistä voitaneen todeta, että niissä kaikissa nostetaan esiin kyberturvallisuuden merkitys, mutta myös hybridivaikuttamisen aiheet informaatiovaikuttamisesta fyysiseen vaikuttamiseen – joissa molemmissa voi olla taustalla tiedustelutarve ja pyrkimys päästä käsiksi yrityksen omistaman tai hallinnoimaan tietoon.

Taulukko 4 Yhteenveto ICT-alan yritysten liiketoiminnalle oleellisista uhista

Uhka	Kuvaus
Rikollisuus	Sisäinen ja/tai ulkoinen petos/kyberrikollisuus. Terrorismi.
Tiedustelu	Tiedonhankintaa mm. tuotekehityksestä
Vaikuttaminen	Hybridi- ja Informaatiovaikuttamista, jolla halutaan luoda epävakautta tai henkilötason vaikuttaminen, maalittaminen. Yritysten mainehaitta voi vaikuttaa liiketoiminnan jatkamiseen ja kriittisten palveluiden tuotantoon.
Asiakas	Asiakkaille aiheutetut menetykset ja vahingot sekä asiakaskato.

[13] Lähde [12] Digipoolin teettämä toimialojen kyberkypsyyden selvitys 2022, sivu 26

Palvelu	Kapasiteetin, kompetenssin, prosessien ja/tai tarpeiden epäsuhdanne.
Teknologia	Vanhentunut, toimimaton ja/tai kehityskelvoton teknologia; koodin tekijänoikeudet ja lisenssiehdot. Haavoittuvuudet. Verkkolaitteiden suojaamattomuus. Riippuvuudet avaruudesta ja satelliittiratkaisuista. Nousevien teknologioiden kaksikäyttösovellutusten ja vientivalvonnan aukkojen hyödyntäminen.
Tuotanto	Tieto- ja viestintäverkkojen ja palveluiden häiriöt - Infran, IT & OT ympäristön, verkon, konesalien, päätelaitteiden toimimattomuus. Kyberhyökkäykset. Häiriöt sähkönsaannissa.
Alihankinta	Toimittajien virheet ja muutoshitaus. Kumppanin kyberhäiriö. Kuljetusten jatkuvuuden häiriöt. Polttoaineiden saannin vakavat häiriöt.
Kehitys	Vaatimuksien määrittelyn, suunnittelun ja koodamisen virheet. Ylimääräinen koodi ohjelmistossa tai aukko asetuksissa. Kotimaisen tutkimuksen ja kehityksen suojaaminen ovat nousevia teemoja
Henkilöstö	Henkilöstön (sis. yritysjohto) työmotivaation, osaamisen ja toimintakyvyn puute. Henkilöstön vaihtuvuus. Puutteet tilanneymmärryksessä johtavat liiketoiminnan ongelmiin. pelastustoiminnan ja toimitilaturvallisuuden puutteet aiheuttavat henkilöstöön kohdistuvia uhkia. Vakava ydinvoimalaitosonnettomuus Suomessa tai Suomen lähialueilla
Pandemia	Pandemian tai muun vastaavan laajalle levinneen epidemian moniulotteiset vaikutukset, jotka näkyvät kokonaisvaltaisesti esim. tuotannossa, työntekijöissä, kyberhyökkäyksissä
Talous	Talouden tai rahoitusjärjestelmän häiriöt, ulkomaankaupan häiriöt aiheuttavat uhan holtovarmuudelle ja yritysten liiketoiminalle. Esim. Kauppapakotteiden kiertäminen häivyttämällä hankintaketjuista tiedon todellisesta ostajasta sekä hankkimalla tuotteita kolmansien maiden kautta. Digitaalisen rahansiirron käyttö ja virtuaalivaluuttojen yleistyminen vaikuttavat epäviralliseen pankki- ja rahansiirtopalvelusektorin vahvistumiseen. Yrityksen oman talouden tappiot häiriötilanteista.
Häiriöt	Rauta- ja/tai softaviat. Inhimilliset erehdykset.
Luonnonilmiöt	Äärimmäisen voimakas avaruusmyrsky
Sota	Sota uhkaa monen yrityksen liiketoiminnan jatkamisen mahdollisuuksia. Toisaalta monien liiketoiminta jatkuu, mutta muuttuneissa olosuhteissa. Valmiussuunnittelua tulee tehdä liiketoiminnan jatkamiseksi ja palveluiden tuotannon turvaamiseksi.

2.3 Turvallisuusjohtamisen malleista

Tässä luvussa luodaan katsaus turvallisuusjohtamiseen liittyviin viitekehyksiin ja pohditaan niiden suhdetta huoltovarmuuteen. Kappaleessa myös pyritään pohtimaan sitä, mitkä viitekehykset voisivat olla ICT yritysten kannalta oleellisia. Myöhemmin työssä peilataan alan yritysten käytössä olevia malleja ja pohditaan, tulisiko käytössä olla muitakin malleja.

2.3.1 EK Yritysturvallisuuden malli

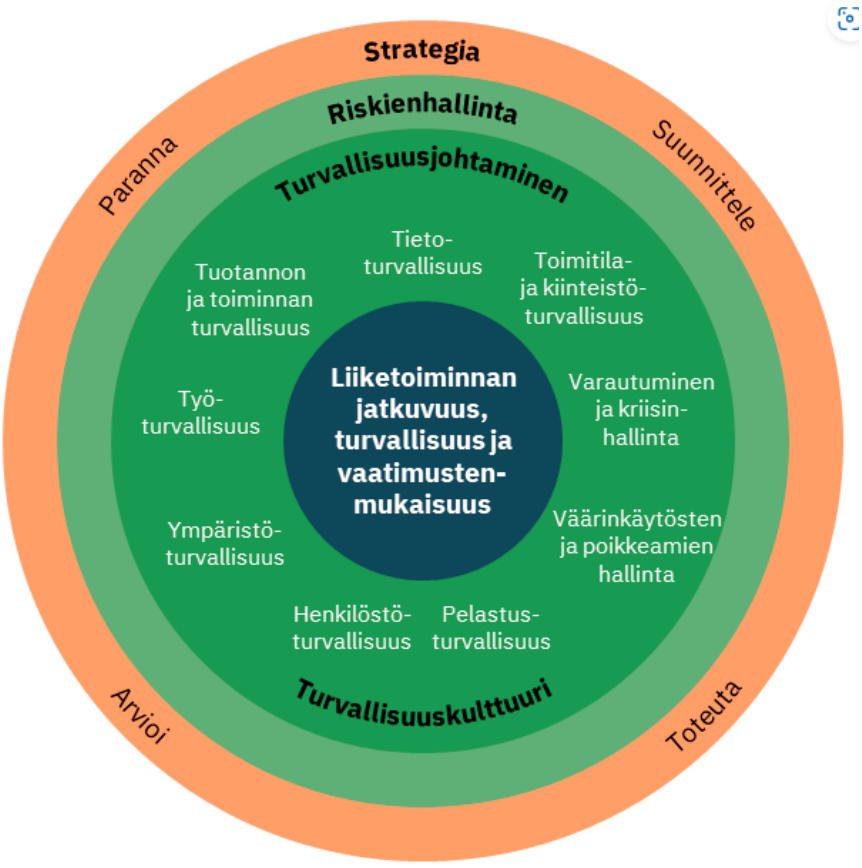
Elinkeinoelämän keskusliiton yritysturvallisuuden malli[14] on kevyt ja ilmaiseksi käytettävissä oleva malli jäsentää yrityksen kokonaisturvallisuuden toimintaa. Malli mukailee useita tunnettuja turvallisuudenhallinnan malleja ja on syntynyt tarpeesta vetää turvallisuudenhallinnan kokonaisuutta yhden nimittäjän alle. Malli on matalan kynnyksen malli lähteä jäsentämään toimintaa huomioiden oleellisimmat turvallisuudenhallinnan osa-alueet. EK:n yritysturvallisuusmallia ei varsinaisesti käytetä esim. yritysten turvallisuusjohtamisen arvioinneissa, mutta se mahdollistaa oman toiminnan vertaa-

[14] Lähde [5] Yritysturvallisuusmalli, Elinkeinoelämän keskusliitto, 1987, päivitetty 2020

misen mallin esittämiin toimintoihin ja on sikäli hyvä aloitustason viitekehys. Turvallisuusjohtamistaan kehittäville yrityksille voikin olla suositeltavaa siirtyä pian käyttämään aihealueen muita standardeja, joita löytyy useita.

EK Yritysturvallisuusmallia käytettiin tässä työssä hyödyksi sen keveyden ja kenties tiiveimmän kokonaisturvallisuudenhallinnan kuvauksen tähden. Mallin avulla voidaan peilata yrityksen toimintaa mallin aiheisiin ja samalla kuitenkin muutamilla tarkistuskysymyksillä voidaan arvioida mallin aiheiden kypsyyttä yrityksessä.

Huoltovarmuuden kannalta EK yritysturvallisuuden malli on myös hyvä viitekehys, sillä se kannustaa varautumaan ja toimimaan pitkälti samoja riskienhallintakeskeisiä toimintatapoja kuin huoltovarmuustoiminta. Malli myös huomioi Varautuminen ja kriisinhallinta osa-alueen osana valmiussuunnittelun, jota eivät kaikki alan standarditkaan huomioi – kenties koska kyseessä on kotimaisen lainsäädännön mukainen jako, jota ei kansainvälisesti tunnisteta ainakaan samanlaisena. Huoltovarmuus onkin yrityksen toimintojen turvallisuutta ja resilienssiä, kun erilaisiin häiriöihin on varauduttu.



Kuva 1 EK:n yritysturvallisuusmalli kuvana

Yritysturvallisuuden malli kuvaa kaikkien osa-alueiden osalta myös sen, mitä aiheita osa-alueeseen kuuluu tai kertoo esimerkkejä aiheista, joita siihen voi kuulua. Toisin sanoen malli tunnistaa ja tunnustaa sen, että jokaisessa yrityksessä on eroja järjestäytymisessä ja jotkin mallin aiheet voivat käytännössä olla jonkin toisen osa-alueen kyljessä. EK:n yritysturvallisuusmalli kuvaa Varautumisen ja kriisinhallinnan aiheita seuraavan tiiviin erittelyn avulla.

Taulukko 5 Varautuminen ja kriisinhallinta EK:n mallissa

Varautuminen ja kriisinhallinta	
1) Jatkuvuussuunnittelu	
• **Liiketoimintariskien arviointi ja vaihtoehtosuunnittelu** • **Tuotannon keskeytyminen tai pysähtyminen** • **Suunnittelu ja sietokyvyn kehittäminen**	• Kannattavuus • Sopimukset
2) Kriisinhallinta	
• **Ennaltaehkäisy ja arviointi** • **Toiminta kriisitilanteessa** • **Toipumissuunnitelmat** • **Oppiminen**	• Varautuminen • Akuutit kriisit • Kehittyvät kriisit • Nopea ja oikea vaste • Viestintä
3) Valmiussuunnittelu (poikkeusoloihin varautuminen)	
• **Velvoitteiden tunnistaminen** • **Tuotannon ja toiminnan suunnittelu**	• Henkilövaraukset (VAP) • Energiahuolto • Materiaalivarastointi • Raaka-aineet, koneet ja laitteet • Korjaus ja huolto, varaosat • Alihankinta ja palvelut

2.3.2 ISO Standardit

International Organization for Standardization (ISO) standardit ovat laajasti elinkeinoelämässä käytettyjä standardeja, jotka kuvaavat esim. jonkin järjestelmän toiminnan kattavasti. ISO standardien käyttö on vakiintunutta ja niiden käyttö on edelleen laajenevaa yrityskentässä. Useat yritykset kasvaessaan alkavat ensin soveltaa jotain standardia toiminnassaan ja myöhemmin päättävät sertifioitua eli osoittaa toimintansa olevan standardin mallin mukaista. Johtuen siitä, että mallia on ensin lähdetty soveltamaan toiminnassa, tehdään sertifioituminen useimmiten kaupallisen hyödyn tähden.

ISO standardien joukossa on useita malleja johtamis- tai hallintajärjestelmille, jotka ovatkin elinkeinoelämässä useimmiten sellaisia standardeja, että niiden käyttö sertifioidaan. Suosituimpien standardien joukosta ei kuitenkaan löydy EK:n yritysturvallisuusmallin kaltaista turvallisuusaiheita yhteen vetävää standardia.

Taulukko 6 Turvallisuudenhallintaan liittyvät hallintajärjestelmästandardit

Standardin nimi	**Tunnus**
Laadunhallintajärjestelmä	ISO 9001
Tietoturvallisuuden hallintajärjestelmä	ISO/IEC 27001
Riskienhallintajärjestelmä	ISO 31000
Turvallisuus ja kriisinkestävyys Liiketoiminnan jatkuvuudenhallinnan järjestelmä	ISO 22301
Työterveys ja turvallisuusjohtaminen	ISO 45001

Johtamisjärjestelmien auditointi	ISO 19011
Toimitusketjun turvallisuuden hallintajärjestelmä	ISO 28001
Yhteiskuntavastuu	ISO 26000
Ympäristöjärjestelmä	ISO 14001
Energianhallintajärjestelmä	ISO 50001
Lahjonnan ja korruption estäminen	ISO 37001
IT-palvelunhallintajärjestelmä	ISO 20000

ISO standardien kanssa yhteydessä puhutaan täydentävänä International Electrotechnical Commission (IEC) standardeista. Useat tietotekniikkaan tai tietoturvallisuuteen liittyvät standardit on tehty ISO/IEC-yhteistyössä. Standardeja löytyy moniin ICT-aiheisen toiminnan aiheisiin, kuten datakeskusten toimintaan liittyen. ISO ja erityisesti IEC on kiinnittänyt toiminnassaan huomiota myös nouseviin teknologioihin ja valikoimaan onkin tuoreeltaan tullut yhteistyön tuloksena myös tekoälyn hallintaan liittyvä standardi ISO/IEC 42001:2023.

2.3.3 ISO27001 ja EK Yritysturvallisuusmallin vertailua

Alalla yleisesti sovellettu standardi ISO27001 on erityisesti tietoturvallisuudenhallintaan liittyvä standardi ja silti sitä on sovellettu yritysten turvallisuudenhallinnan ainoana standardina. Tämän takia se ohjaa yrityksiä painottamaan turvallisuudenhallintaansa korostuneesti tietoturvallisuuden aiheisiin.

Jos verrataan EK:n yritysturvallisuusmallin sisältöä ISO27001 standardiin, huomataan, että se kattaa pelkästään aiheiltaan vain osan yritysturvallisuusmallin aiheista. Sen lisäksi, jos tarkastellaan esim. väärinkäytösten ja poikkeamien hallintaa, voidaan todeta, että EK:n mallissa sisältö on laajempi ja pitää sisällään mm. taloushallinnon poikkeamat ja väärinkäytökset, kun taas ISO27001 mallissa keskitytään tietoturvahäiriöiden hallintaan. Toisena esimerkkinä ISO27001 mallin Fyysinen turvallisuus kokonaisuus käsittelee lähinnä turva-alueita, kulunvalvontaa, tilojen ja laitteiden suojausta keskittyen laitteisiin, kaapelointeihin ja näiden huoltoon. EK:n yritysturvallisuusmallin Kiinteistö ja toimitilaturvallisuus aihe pitää esimerkiksi sisällään laajemmin aiheita ja esim. sopimusvalvonnan tilojen ja kiinteistöjen osalta.

Selvityksen toteuttajan tulkintana voinee kuitenkin todeta, että ICT yrityksissä monet EK:n mallin aiheet ovat lakisääteisinä toteutettu hyvin ja sikäli ei ole kenties nähty oleelliseksi niihin keskittyä tai niitä eivät asiakkaat ole tämän takia myöskään vaatineet. Lakisääteiset toiminnot yhdessä ISO27001 sertifikaatin velvoittavien aiheiden kanssa on kuitenkin jo lähellä EK:n yritysturvallisuuden mallia.

Yleisesti ottaen ISO27001 malli ei kata yritysten turvallisuuskokonaisuutta niin kattavasti kuin EK:n yritysturvallisuusmalli. Lakisääteisten velvollisuuksien kanssa yhdessä sillä saadaan katettua aiheita, mutta voitaneen arvioida, että riskitarkastelun kautta se jättää moniin aihealueisiin kehittämisen varaa.

Taulukko 7 Hallintakeino kategoriat ja osa-alueet rinnakkain

ISO27001 Hallintakeinojen kategoriat	EK:n yritysturvallisuusmallin osa-alueet
	Tietoturvallisuus
Tietoturvapolitiikat	
Tietoturvallisuuden organisointi	
Tietoturvahäiriöiden hallinta	Väärinkäytösten ja poikkeamien hallinta
Pääsynhallinta	
Salaus	
Järjestelmien hankkiminen, kehittäminen ja ylläpito	
Suhteet toimittajiin	
Vaatimustenmukaisuus	
Liiketoiminnan jatkuvuuden hallintaan liittyviä tietoturvanäkökohtia	Varautumisen ja kriisinhallinta
Henkilöstöturvallisuus	Henkilöstöturvallisuus
Suojattavan omaisuuden hallinta	
Fyysinen turvallisuus ja ympäristön turvallisuus	Kiinteistö- ja toimitilaturvallisuus
Käyttöturvallisuus	
Viestintäturvallisuus	
	Pelastusturvallisuus
	Tuotannon ja toiminnan turvallisuus
	Ympäristöturvallisuus
	Työturvallisuus (työterveyshuolto ja työsuojelu)

2.3.4 Muita turvallisuudenhallinnan standardeja

Yrityksen toiminnan turvallisuuden standardeja löytyy maailmalta rajallisesti ja toisaalta monet niistä ovat keskittyneet johonkin kokonaisturvallisuuden osa-alueeseen.

Esimerkkinä mainittakoon NIST Cybersecurity Framework (CSF), joka on laajalle levinnyt ja tunnettu malli. Monessa suomalaisessa, mutta kansainvälisissä, yrityksessä on käytössä niin ISO 27001 kuin Cybersecurity Framework CSF[15] yhtaikaa. Näiden lisäksi ISAE (International Standard on Assurance Engagements) standardit ovat aiheiltaan sellaisia, että ne ovat relevantteja ICT-yrityksille. ISAE-standardeja ei kuitenkaan ole laajemmin sovellettu kotimaisissa yrityksissä – vain kaksi haastatelluista yrityksistä käyttää niitä. (kts. Kuva 1).

[15] https://csrc.nist.gov/Projects/Cybersecurity-Framework/Filters#/csf/filters

Yrityksen toiminnan standardoimisen sijasta onkin tarjolla henkilötason standardeja. Sertifiointia turvallisuudenhallinnan aiheissa tarjoavatkin monet toimijat, joista hyvänä esimerkkinä on ASIS International[16]. Toinen jatkuvuudenhallintaan liittyvä, sertifiointeja henkilökohtaisella tasolla tarjoava, toimija on The Business Continuity Institute (BCI)[17].

2.4 EU direktiivit ja regulaation vaikutuksia yritysten kokonaisturvallisuuden hallintaan

Kotimainen lainsäädäntö on turvallisuudenhallinnan osalta pirstaleinen ja vaikutuksia yritysten turvallisuudenhallintaan tulee monista toimialakohtaisista lainsäädännöistä tai asetuksista. Suurin osa näistä ei siis kannusta yrityksiä kokonaisvaltaiseen turvallisuudenhallintaan, vaan nostavat esiin jonkin osa-alueen tärkeyden toimialan yrityksissä huomioitavaksi. ICT yritykset pääsevät toteuttamaan alakohtaista lainsäädäntöä asiakassopimustensa kautta. Ja tehtyjen haastatteluiden perusteella onkin todettu, että tehokkuuden kannalta ICT yritysten ei kannata pyrkiä pistemäisiin ratkaisuihin vaan nostaa tasonsa lähelle kovimpia asiakasvaatimuksia, jotta niiden avulla ollaan valmiita täyttämään useimmat asiakasvaatimukset.

Esimerkkejä toimialakohtaisesta lainsäädännöstä, jolla on vaikutuksia turvallisuudenhallintaan:

- Kemikaalilaki
- Sähköturvallisuuslaki
- Ydinenergialaki
- Ilmailulaki
- Terveydenhuoltolaki ja usea muu alan lainsäädäntö

Toimialakohtaisen lainsäädännön ja asetusten lisäksi moni yleisesti kaikkia koskeva lainsäädäntö vaikuttaa yrityksiin ja niiden turvallisuudenhallintaan. Turvallisuuden hallinnan aiheita ohjaavat mm.

- Työturvallisuuslaki
- Tietosuojalaki ja laki yksityisyyden suojasta työelämässä
- Ympäristönsuojelulaki
- Rikoslaki
- Pelastuslaki
- Valmiuslaki

[16] https://www.asisonline.org/
[17] https://www.thebci.org/

ICT-alalle relevantti lainsäädäntö on myös Laki sähköisen viestinnän palveluista[18]. Erityisesti lainsäädäntö vaikuttaa tietoverkkojen kanssa toimiviin yrityksiin. Lainsäädäntö onkin vahvimmin ohjannut ns. operaattoreita turvallisuuteen liittyvissä toimissaan.

Tätä kirjoitettaessa EU-regulaatio on lisääntynyt ja lisääntyneen regulaation myötä sitä toteuttava kotimainen lainsäädäntö on edennyt ja tulee myös vaikuttamaan yritysten turvallisuudenhallinnan toimiin. Erityisesti on mainittava EU verkko- ja tietoturvadirektiivi NIS, jonka voimaantultua nähtiin vaikutuksia laajasti em. lainsäädäntöön. Nyt valmisteilla oleva NIS2-direktiivin kansallinen toimeenpano tulee vastaavasti vaikuttamaan lainsäädäntöön laajasti, ja edellisen päivityskierroksen jälkeen päivitetäänkin taas toimialakohtaista lainsäädäntöä, sekä tehdään uutta lainsäädäntöä, joka ehdotuksen mukaisesti on nimetty Laiksi kyberturvallisuuden riskienhallinnasta. Toisin sanoen tämä lainsäädäntö velvoittaa yritykset laajasti huolehtimaan kyberturvallisuudestaan (ja joiltain riippuvin osin siihen liittyvästä fyysisestä infrastruktuurista).

NIS2-direktiiviä ja sen perusteella tehtävää kotimaista lainsäädäntöä enemmän yritysten kokonaisturvallisuudenhallintaan vaikuttaa kenties CER-direktiivi (Critical Entities Resilience) ja sitä seuraava kotimainen lainsäädäntö. Tätä kirjoitettaessa ei lainsäädännön ehdotusta ole vielä nähtävillä, mutta hyvin todennäköisesti se tulee edellyttämään yrityksiltä riskienhallintaperusteista turvallisuudenhallintaa, joka huomioi mm. hybridivaikuttamisen tai luonnon aiheuttamat riskit turvallisuudelle. Sen myötä myös kokonaisturvallisuudenhallinnan tilasta tulee raportoida viranomaisille.

NIS2-direktiivi tulee velvoittamaan jo hyvin laajaan joukkoa yrityksiä, mutta ei kuitenkaan kaikkia yrityksiä kaikilla aloilla – se tulee kuitenkin velvoittamaan kaikkia Huoltovarmuusorganisaation Digipoolin yrityksiä – eli niiltä edellytetään kyberturvallisuuden riskienhallintaa ja siitä raportointia. CER-direktiivin kohteena on alustavien arvioiden mukaan vain noin 100 kriittisintä yritystä suomesta ja on hyvin todennäköistä, että sen velvoittavuus tulee koskemaan vain muutamaa ICT-alan yritystä suomessa. Toisin sanoen yrityksen kokonaisturvallisuuden hallintaa ei lainsäädännöllä edellytetä alan yrityksiltä, mutta kyberturvallisuuden riskienhallintaa edellytetään.

Direktiivit ja niiden myötä päivitetty kotimainen lainsäädäntö (NIS2 HE ehdotus[19]) viittaavat standardeihin. NIS2-direktiivi ja sitä seuraava kansallinen lainsäädäntö erittelee ISO27001 standardin olevan suositeltava viitekehys, jota riskienhallintaperusteisesti tulee soveltaa. CER-direktiivi 16 artikla taas nostaa esiin sen, että paikallisen lainsäädännön tulee ”silloin, kun siitä on hyötyä, kannustettava käyttämään kriittisiin toimijoihin sovellettaviin toimenpiteisiin turvallisuuden ja häiriönsietokyvyn kannalta olennaisia eurooppalaisia ja kansainvälisiä standardeja ja teknisiä eritelmiä siten, että ne

[18] Laki sähköisen viestinnän palveluista 917/2014 - Ajantasainen lainsäädäntö - FINLEX ®
[19] Lähde [13] NIS2 Luonnos hallituksen esitykseksi laista kyberturvallisuuden hallinnalle

eivät kuitenkaan määrää käyttämään jotain tiettyä teknologiaa tai suosi jotain tiettyä teknologiaa muiden kustannuksella”.

Yhteen vetäen voinee todeta, että kotimaisen moninaisen lainsäädännön ja EU-direktiivien ohjaaman tavoitetilan kannalta on suositeltavaa, että yritykset jäsentävät turvallisuuttaan jonkin viitekehyksen avulla. Suositus on tehokkuusnäkökulmasta hyvä koskea koko yrityskenttää alasta ja yrityksen koosta huolimatta. Sertifiointi standardien mukaisen toiminnan osalta on yritysten oma päätös, josta voi olla hyötyä oman kehityksen kannalta tai viranomaisille turvallisuudenhallinnan tilasta raportoitaessa.

2.5 Turvallisuudenhallinnan painotuksista tehtyjä selvityksiä?

Tämän selvitystyön myötä ei tunnistettu, että ICT yritysten (tai muidenkaan alojen) turvallisuudenhallintaa olisi selvitetty kattavasti. Tyypillisempää on se, että yrityksissä keskitytään yksittäisiin kokonaisturvallisuudenhallinnan aiheisiin ja arvioidaan niiden tilaa sen kehitykseen keskittyen.

3 Tutkimuksen toteutuksesta

Tämä kappale esittelee tutkimuksen toteutukseen käytetyt välineet ja toteutustavan. Lisäksi kappale käsittelee opit, jotka selvityksen järjestämisestä saatiin. Oppeja voidaan hyödyntää vastaavia selvityksiä tehtäessä.

Työssä tehtiin kirjallisuustutkimusta avoimista lähteistä löytyviin materiaaleihin liittyen ja kerättiin havaintoja muistiinpanoina talteen, joista lopulta tiivistettiin havainnot tähän dokumenttiin. Kirjallisuustutkimuksen lisäksi toteutettiin kyselytutkimus sekä haastatteluita, joilla kerättiin tietoa Digipoolin verkostoon kuuluvista ICT – alan yrityksistä niiden turvallisuuden hallinnan tilaan liittyen. Kyselyn ja haastatteluiden merkitys työssä oli suuri.

3.1 Välineet

Kirjallisuustutkimusta tehtäessä käytettiin hakukoneita Bing ja Google sekä tekoälysovellusta Bing Chat Enterprise. Näistä käytettiin versioita, jotka olivat Teknologiateollisuus ry lisensoimia ja sikäli selvitykseen käytettävissä olevia sovelluksia. Bing chat Enterprise -sovellus ei ole avoimesti saatavilla, vaan on sidottu MS Office lisensointiin.

Kyselytutkimuksen luontiin ja kyselyn toteuttamiseen käytettiin Teknologiateollisuus ry:n lisensoimaa Webropol-kysely- ja raportointisovellusta. Webropol sovelluksen tuottamia raportteja käytettiin tulosten taltiointiin dokumenttimuotoon.

Haastattelututkimuksessa käytettiin OneNote sovellusta, joka on osa MS Office tuotepakettia. OneNote sovellukseen tehtyjen muistiinpanojen ja kyselytutkimuksen tietoja käsiteltiin niin ikään MS

Office tuoteperheen Excel-sovelluksessa. Loppuraportti kirjoitettiin MS Office -tuoteperheen Word tekstinkäsittelysovelluksella.

3.2 Kyselytutkimus

Kyselytutkimuksen sisältö rakennettiin työn suunnitteluvaiheessa. Sisällön määrittelyä ohjasi tarve ymmärtää paremmin ICT-alan yritysten tilannetta kokonaiskuvallisuuden hallinnan suhteen. Selvityksellä haluttiin kerätä tietoa siitä, mitkä standardien avulla yritykset ohjaavat toimintaansa ja kuinka ne vastaavat toimintaverkoston odotuksiin tai verkoston tunnistamiin riskeihin.

Toisaalta sisältöä ohjasi tarve selvittää yritysten kokonaisturvallisuuden hallinnan tilannetta jonkin määrämuotoisen mallin avulla. EK:n yritysturvallisuuden malli tarjosi tähän tarpeen yksinkertaisen, mutta eri turvallisuuden osa-alueet huomioivan mallin. Kyselytutkimuksen sisältö lähti siis rakentumaan standardien hyödyntämiseen liittyvien kysymysten ja EK yritysturvallisuusmallin20 aiheita tiedustelevien kysymysten ympärille. Muita sisältöä ohjaavia tarpeita olivat tarve selvittää yritysten valmiutta EU NIS2 ja CER direktiiveistä seuraavan uuden lainsäädännön tuloon, johtuen siitä, että direktiivit ja niistä seuraava kotimainen lainsäädäntö tulee edellyttämään osin niitä turvallisuudenhallinnan toimenpiteitä, joita selvityksessä arvioitiin. Jotta saatiin tietoa yritysten valmiudesta direktiivien edellytyksiin, lisättiin kyselyyn kysymyksiä.

Kyselytutkimus kohdistettiin Digipoolin verkoston ICT yrityksiin. Verkostossa on 105 yritystä ja kysely lähetettiin sähköpostitse yritysten nimeämille yhteyshenkilöille. Kyselyn lähetyksen yhteydessä yhteyshenkilöitä pyydettiin vastaamaan itse tai välittämään kysely henkilöille, ketkä osaisivat siihen parhaiten vastata.

Kyselyyn vastasi lopulta 32 eri yrityksen edustajaa. Vastaajien otosta voidaan pitää kuitenkin varsin hyvänä otoksena huolimatta siitä, että se edusti vain 30,5% Digipoolin verkoston yrityksistä. Väitettä perustelee se näkökulma, että mikäli tästä kohdejoukosta löytyy kehityskohteita selvityksen perusteella ovat ne hyvin todennäköisesti yleistettävissä kotimaisiin ICT yrityksiin laajemminkin sillä lähtökohtaisesti huoltovarmuuskriittisten yritysten osalta odotusarvot turvallisuudenhallinnalle ja varautumiselle ovat korkealla tasolla.

[20] Lähde [5] Yritysturvallisuusmalli, Elinkeinoelämän keskusliitto, 1987, päivitetty 2020

3.3 Haastattelut

Selvityksen sisältöjä päätettiin sen suunnitteluvaiheessa täydentää haastatteluilla. Haastatteluilla pyrittiin keräämään hiljaista ja tulkinnallisempaakin tietoa yritysten kokonaisturvallisuuden hallinnan painotuksista ja päätösperusteista, jotka olivat johtaneet nykyiseen tilanteeseen yrityksessä.

Haastatteluiden sisältö noudatti samaa runkoa kuin kyselytutkimus jakaen sisällön 4 aihealueeseen, joiden alla keskustelut käytiin. Haastattelija käytti kyselyn kysymyksiä keskustelun tarkistuslistana ja kysyi tarkentavia kysymyksiä, mikäli keskustelu ei olisi aiheesta muuten edennyt. Samalla haastattelijan oli mahdollista esittää tarkistuskysymyksinä sellaisia turvallisuudenhallinnan toimenpiteitä, joita oli tunnistettu edistyneiden organisaatioiden käsitelleen toiminnassaan.

Keskusteluita käytiin seuraavien aiheiden alla:

- Kokonaisturvallisuuden standardit ja mallit
- Turvallisuudenhallinnan kypsyys yrityksessä EK:n yritysturvallisuusmallin aiheissa
- Turvallisuudenhallinnan organisoituminen
- Direktiivien vaikutukset

Haastatteluihin valittiin kutsuttavaksi Digipoolin aktiivisten yritysedustajien muodostamien ryhmien jäseniä. Valinta tehtiin siksi, että Digipoolin ryhmissä on mukana suomen suurimmat ICT-alan toimijat ja näiden tuottamat palvelut edustavat merkittävää osaa suomessa muun yhteiskunnan hyödyntämiä ICT-palveluita ja siten niitä tuottavien yritysten turvallisuudenhallinnan tilalla on merkitystä laajemminkin. On myös hyvin mahdollista, että mikäli CER-direktiiviä seuraavan kotimaisen lainsäädännön myötä lainsäädännön kohteeksi tulee ICT-alan yrityksiä, löytyvät ne tästä joukosta.

Haastatteluiden tavoite otokseksi määritettiin kymmenen yritystä. Haastatteluihin osallistui lopulta kaikki tavoitellut kymmenen yritystä, joiden tuottamat palvelut siis kattavat suurimman osan kotimaisen ICT-alan markkinoista. Haastattelut toteutettiin kyselyn tavoin anonyyminä ja tulokset pseudonymisoitiin, jottei vastaajaa tai hänen edustamaansa yritystä voida niistä tunnistaa kohteen suojelemiseksi ja luottamuksellisuuden takaamiseksi.

3.4 Tulokset ja tuotokset

Siinä missä tämä dokumentti esittelee tuloksista tehtyjä tulkintoja aihealueittain, on taustalla luonnollisesti tulokset, jotka saatiin kyselystä vastauksina sekä haastatteluista muistiinpanoina.

4 Selvitystyön havaintoja

Tässä luvussa tarkastellaan Digipoolin yritysten kokonaisturvallisuuden hallinnan nykytilaa. Tarkastelu perustuu kyselyn ja haastatteluiden myötä saatuun tietoon yritysten tilanteesta. Tulokset on

esitelty kyselyiden ja haastatteluiden aiheissa ja muodostettu niiden mukaan käsitys yritysten tilanteesta. Kappale nostaa esiin niin positiivisia kuin negatiivisiakin havaintoja tilanteesta.

Selvityksen tulosten perusteella on yleistilanteesta todettava, että selvityksen kohteena olevat yritykset ovat kaikki jollain tavalla huomioineet turvallisuutta ja hallitsivat sitä jokainen jollain olemassa olevalla tavalla. Lakisääteiset yritysturvallisuuteen kuuluvat tehtävät ovat tuttuja ja jollakin tavalla dokumentoituna olemassa yritysten toiminnassa.

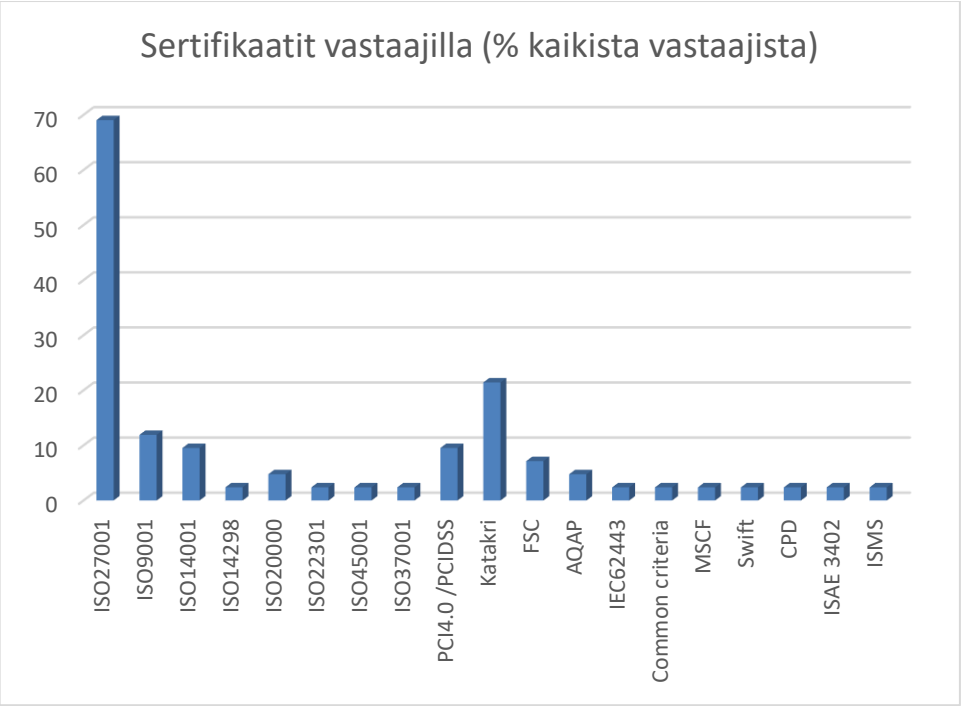
Geopoliittinen tilanne tätä kirjoitettaessa on haastava Venäjän hyökkäyssodan ollessa käynnissä Ukrainassa ja se näkyy myös vastanneiden yritysten vastauksissa. Kohonnut uhkataso on saanut yritykset kiinnittämään turvallisuuteen huomiota ja käsittelemään uhkia tai riskejä, joita ei ole aiemmin käsitelty. Silti haastatteluita tehtäessä oli helppo esittää potentiaalisia uhkia, joita yrityksessä ei ollut käsitelty. Käsittelemättömät uhat alleviivaavat tarvetta riskien käsittelylle varautumista ohjaavana toimintana. Toisaalta pandemian uhka on löytänyt kaikkien yritysten riskikartoille ja on aiheuttanut toimenpiteitä, jotka tuoreena ovat muistissa ja dokumentoitu toimintatapoihin.

Vähemmän positiivisena havaintona voidaan todeta, että yritysten välillä käsitykset riittävästä tai hyvästä turvallisuuden hallinnan tasosta eri aiheissa vaihtelevat valtavasti ja sikäli vertailukelpoisten tulosten saaminen on lähes mahdoton tehtävä. Haastattelut alleviivasivat kypsyyden tulkinnan haastetta ja antoivat aihetta kyseenalaistaa kyselyyn annettuja numeerisia arvioita. Ne kertovat kuitenkin siitä kuinka hyväksi vastaaja kokee tilanteen. Numeeristen arvioiden sijaan pyritäänkin tässä siis tekemään aiheittain tulkintaa yritysten kypsyydestä ja tekemään päätelmiä alan yritysten tilanteesta ja havaintoja mahdollisista kehittävistä kohteista näiden tulkintojen perusteella.

4.1 ICT-yrityksissä sovelletut standardit

Tämän selvitystyön kyselyyn ja haastatteluun osallistui yhteensä 42 yritystä. Neljä yritystä ei tunnistanut soveltavansa varsinaisesti mitään standardia toiminnassaan. Loput, eli 38 yritystä (90%) toisin sanoen soveltavat jotain mallia toiminnassaan. 32 yritystä (76%) ilmoittaa hallussaan olevan sertifikaatti yhden tai useamman standardin osalta.

Ehdottomasti laajimmin sovellettu standardi ICT alan yrityksissä on ISO27001 – sen soveltamisesta on myös eniten todistuksia eli sertifikaatteja alalla. Vastanneista 32 ilmoitti soveltavansa sitä ja 29/42 (69%) yritystä ilmoitti sertifioituneensa kokonaan tai osittain sen mukaisesti.



Kuva 1 Kyselyn ja haastatteluiden perusteella ICT yritysten sertifikaatit

Kaikkein isoimmilla yrityksillä on oma mallinsa, joka on tyypillisesti laajempikuin vain ISO27001, koska huomioi laajasti asiakasvaatimuksia. Tyypillisesti mallin ilmoitettiin olevan ISO27001 yhteensopiva. Se, että isoilla yrityksillä on oma mallinsa, alleviivaa sitä, että ICT-yrityksen on tehokkaampaa ja kannattavampaa toimia laajasti tiukimpien asiakasvaatimusten mukaisesti vastaten näin suoraan asiakkaiden vaatimuksiin.

Sovellettavien standardien tai mallien lista on luonnollisesti laajempi kuin sertifioitujen. Sovellettavissa malleissa, joihin ei ole sertifioiduttu, erottuu mm. ISO9001 laadunhallinnan standardi. Yhteensä 7 yritystä kertoo soveltavansa sitä toiminnassaan, mutta vain 4/42 yrityksestä on hankkinut sertifikaatin laadunhallinnan standardin soveltamisesta. Tässä on eroa myös kyselyyn vastanneiden ja haastateltujen välillä – useimmilla haastatelluilla yrityksillä on sertifikaatti ISO9001 laadunhallinnan standardin soveltamisesta.

Samoin ympäristöjärjestelmään liittyen soveltavat useat ISO14001 standardia ja vain osa 7/42 on hankkinut sertifikaatin sen soveltamisesta. Haastatelluista suurin osa on sertifioitunut ympäristöjärjestelmän osalta, kun kyselyyn vastanneista vain yksittäiset ovat näin tehneet.

PCIDSS tai muut finanssisektorin standardit näkyvät sovellettujen standardien listoilla ja monet alan yritykset ovat myös hankkineet sertifikaatin asiakasvaatimusten täyttämiseksi – se ei kuitenkaan ole läpileikkaavasti kaikilla alan toimijoilla.

Vastaavasti julkishallinnon asiakkuuksissa toimivien yritysten standardeissa ja malleissa näkyvät katakri[21] ja julkri[22] ja muutamat ilmoittavat niiden myötä heidän toimintaansa myös auditoidun. Puolustusvoimien kanssa työtä tekevillä toimijoilla nousee esiin FSC (Fasility Security Certificate) sekä AQAP (Allied Quality Assurance Publications). Vain 2 toimijaa vastanneista ilmoittaa AQAP sertifioituneensa, vaikka suomen liittyminen puolustusliitto NATOon on nähty olevan liiketoimintamahdollisuuksia tuova. AQAP on NATO:n luoma malli laadunvarmistustoimille ja se on monien yhteistyösopimusten edellytys.

Muita useampien soveltamia malleja ovat liiketoiminnan jatkuvuudenhallinnan järjestelmä ISO22301 ”Turvallisuus ja kriisinkestävyys” ja ISO45001”Työterveys ja turvallisuusjohtaminen” tai IT-palvelunhallintajärjestelmä ISO20000. Nämä mallit keräsivät kahdesta kolmeen mainintaa koko vastaajajoukosta.

Erityismaininnan ansaitsee yksi yritys, joka vastaajajoukosta on hankkinut sertifikaatin ISO37001 Lahjonnan ja korruption vastaisen hallinnon mallin soveltamisesta. Malli on kansainvälisesti yleinen, mutta suomessa hyvin harvinainen yritysten käytössä.

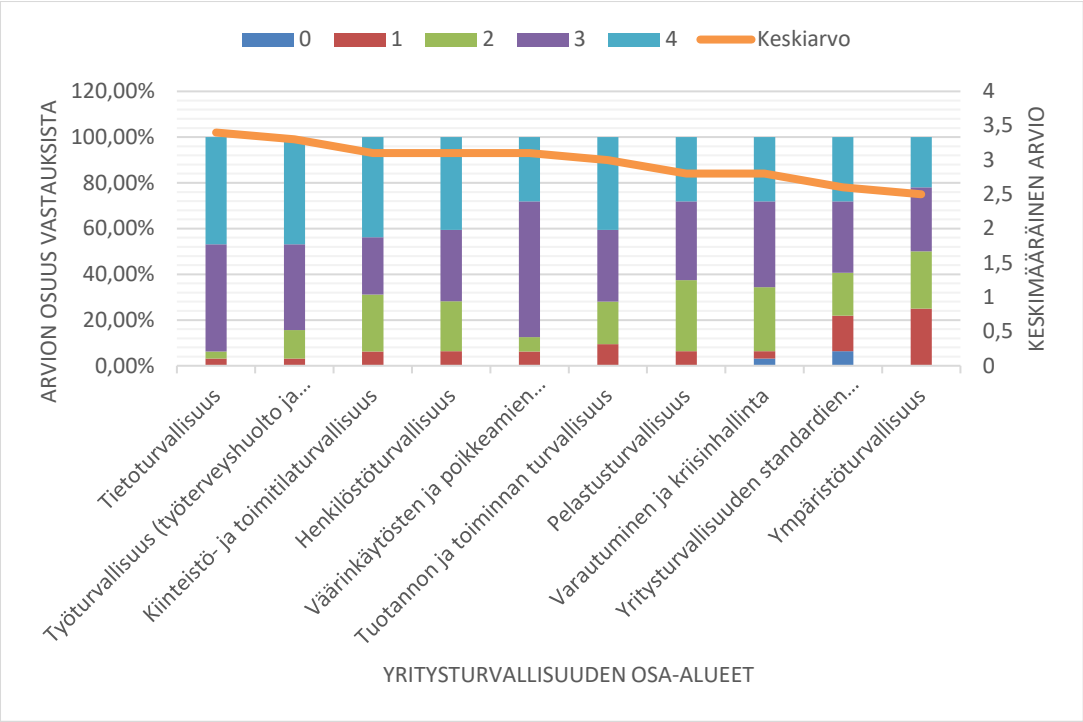
Monet kohdan 3.3.2 standardeista eivät saaneet vastaajajoukossa mainintoja niiden soveltamisesta tai että niiden soveltamisesta olisi sertifikaatti. Sellaisia malleja ovat esim. Riskienhallintajärjestelmä ISO31000, Johtamisjärjestelmien auditointi ISO19011, Toimitusketjun turvallisuuden hallintajärjestelmä ISO28001, Yhteiskuntavastuu ISO26000, Energianhallintajärjestelmä ISO50001.

Kun kysyttiin motivaatiota sertifikaatin hankkimiselle, oli ehdottomasti suosituin peruste kaupallinen etu ja selvästi toisena oli asiakasvaatimukset – vasta kolmantena mainittiin oman kehityksen tukeminen. Vaatimuksiin vastaaminen eli ”compliance” nousi esiin kommenteissa.

4.2 Yritysturvallisuusmallin osa-alueiden kypsyys yrityksissä

Luku käsittelee yritysturvallisuusmallin osa-alueiden kypsyyttä, kuten sitä on arvioitu selvitykseen osallistuneiden yritysedustajien toimesta. Osallistujat arvioivat yrityksensä kypsyyttä kussakin aiheessa kyselyyn vastaamalla tai osallistumalla haastatteluun.

[21] Lähde [11] Katakri-tietoturvallisuuden-auditointityokalu-viranomaisille
[22] Lähde [10] Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri)



Kuva 2 Kyselyn kypsyys arvioiden hajonta ja arvioiden keskiarvo

4.2.1 Henkilöturvallisuus

Henkilöturvallisuuden kypsyyttä kyselyllä kysyttäessä asteikolla 0-4, saa aihe keskiarvoisesti arvioksi 3,1. 41% yrityksistä arvioi sen korkeimmalle kypsyystasolle 4 (Prosesseja optimoidaan ja tapahtuu jatkuvaa parantamista), 31% tasolle 3 (Prosesseja myös mitataan ja hallitaan), 22% tasolle 2 (Prosessit on laadittu sekä käytössä koko organisaation tasolla) ja 6% tasolle 1 (Prosesseja ja perusohjausta on osassa organisaatiota).

Toisin sanoen hajontaa yritysten välillä on painottuen kypsempiin asteikon pykäliin ja samalla se on sijoitettu aiheita priorisoitaessa pääasiassa sijoille 5-8, eli ei aivan päällimmäisenä kun turvallisuusaiheita tarkastellaan. Aihetta ei ole myöskään nostettu esiin, kun on kysytty kehitystä kaipaavaa aihetta. Yli puolet (51%) vastaajista kuitenkin kertoo aiheen olevan yrityksen voimassa olevan strategian aiheena.

Haastatelluista yrityksistä lähes kaikki arvioivat henkilöturvallisuuden olevan hyvällä tasolla 4, samalla kuitenkin useimmat olivat tunnistaneet kehitystä vaativia asioita henkilöturvallisuuden aiheissa, ja toimenpiteitä on käynnissä turvallisuuden kehittämiseksi. Edistyneiden suurten yritysten kehitystoimenpiteissä näkyy mm. henkilöturvallisuuden mittaamisen kehittämistarve.

Eroja henkilöturvallisuudenhallinnassa näkyy kansainvälisissä organisaatioissa ja mm. matkustuksen turvallisuuteen on kiinnitetty eri tavoin huomiota riippuen yrityksen kansainvälisyydestä ja toisaalta paljon matkustavissa yrityksissä vaikuttaa olevan hyvin eri tavoin kiinnitetyn huomiota matkustamisen turvallisuuteen.

Henkilöstölle psykologista tukea turvallisuustapahtumiin liittyen tarjoavia yrityksiäkin on joukossa mukana, mutta palveluiden tarjoaminen tehdään tyypillisimmin kumppanin tuella tai sitä mietitään kehityskohteena.

Etätyön turvallisuus todettiin useammankin vastaajan toimesta kypsymättömäksi aiheeksi, jossa on vielä kehitettävää ja mm. etätyönteon työnantajan vastuut, velvollisuudet tai valtuudet ovat monilla määrittelemättömät.

Ylipäänsä henkilöturvallisuuden aiheena koettiin olevan hyvällä ja kypsällä tasolla yrityksissä. Aiheeseen on lähtökohtaisesti kiinnitetty huomiota yritysten toiminnassa, ja kehitystarpeet ovat varsin kehittyneitä ja vaativia, joka kertoo aiheen suhteellisesta kypsyydestä. Hajonnan tähden yritykset hyötyisivät yhteisten toimintatapojen ja käytäntöjen jakamisesta aiheessa.

4.2.2 Kiinteistö- ja toimitilaturvallisuus

Kiinteistö- ja toimitilaturvallisuus sai kyselyssä kypsyysarvioita, joiden keskiarvo on 3,1. Aiheen on arvioinut korkeimmalle kypsyystasolle 43,80 % vastaajista ja samalla kypsyystasot 3 ja 2 ovat saaneet 25% arvioista ja 6% antaa arvion 1. Aiheen on arvioinut kypsimmäksi kyselyn suurin joukko vastaajista.

Kun kysyttiin mitkä kokonaisturvallisuuden aiheet kaipaavat kehitystä, nosti 3 vastaajaa aiheen esiin ja alleviivasi sen merkitystä etätyönteon aikana toimitilojen ollessa tyhjänä tai koska aiheessa oli tunnistettu kehitettävää.

Tarpeen todettiin ohjaavan tässäkin aiheessa ja toimitiloissa on eri tasoisia turvallisuusratkaisuita käyttötarpeen mukaan. On mm. todettu, että toimistotilojen turvallisuus ja esim. konesalien turvallisuus on useimmiten hyvin erilaisella kypsyystasolla. Toisaalta toimistotilojen turvallisuuteen on kiinnitetty enemmän huomiota, kun työtä on tarve tehdä ns. turvatiloista. Tarpeen määrittää useimmiten siis liiketoiminta ja asiakasvaatimukset – ja asiakkuustiimillä onkin merkitystä tilaturvallisuusratkaisuissa. Kyselyn ja haastatteluiden perusteella erityyppisten tilojen turvallisuus on myös hallittu erikseen – erityisesti suuremmissa yrityksissä. Toimitilojen turvallisuutta on todettu myös tarkastettavan - erityisesti asiakkaiden asettamien vaatimusten täyttämisen toteamiseksi.

Hyvin yleisesti alan yritykset toimivat vuokratiloissa ja useimmat aihealueen turvallisuuden vastuut koetaan olevan vuokranantajalla, vaikkei niistä ole erityisesti sovittu – näin on erityisesti toimistotilojen osalta. Kypsimmät yritykset huolehtivat turvallisuudestaan mahdollisuuksien mukaan itse ja yhteistyössä vuokranantajan tai kiinteistön kanssa. Vuokratiloissa toimivat tilaturvallisuudestaan huolehtivat toimijat tuottavat vaatimuksia vuokranantajalle turvallisuuden kovennusten suhteen.

Yksityisen turvallisuusalan palveluiden ja vartioinnin osalta käytännöt vaihtelevat ja osalla toimijoista on suoria sopimuksia vartiointiyritysten kanssa ja osalla taas nojataan täysin vuokranantajan kautta järjestettyihin palveluihin.

Kiinteistö- ja toimitilojen sopimushallinnalle ei vastaajajoukossa ole mitään yhtä mallia. Vastuu sopimuksista on usein talousjohtajalla tai sellaisella roolilla, kenelle vastuu on keskitetty. Suuremmilla yrityksillä vaikuttaa olevan tiimi, jonka vastuulla toimitilojen sopimukset ovat.

Ylipäänsä kiinteistö- ja toimitilaturvallisuuden aiheen koettiin olevan hyvällä ja kypsällä tasolla yrityksissä. Aiheeseen on kiinnitetty paljon huomiota yritysten toiminnassa, ja kehitystarpeet ovat kehittyneitä ja asiakkaiden ohjaava vaikutus on ilmeinen. Hajonta kertoo, että vähemmän kypsät yritykset hyötyisivät kypsempien yritysten kokemusten jakamisesta.

4.2.3 Pelastusturvallisuus

Pelastusturvallisuuden kypsyysarvioiden keskiarvo kyselyssä oli 2,8. Parhaan arvosanan 4 antoi 28,1% vastaajista ja tason arvioi olevan 3 34,4% vastaajista, tason 2 31,2% vastaajista ja tason 1 6,3%. Vastausten painottuessa arvioon 3 vaikuttaisi aiheen olevan kypsynyt, mutta siinä arvellaan olevan kehitettävää.

Aiheiden prioriteettia toiminnassa kysyttäessä hajaantuu vastaukset laajasti ja moni vastaaja jättää aiheen häntäpäähän sijoille 3-4 ja samalla monet vastaajista nostaa sen sijalle 8. Aihetta ei ole nostettu esiin kun kysyttiin aihetta, joka toiminnassa vaatisi kehitystä.

Aihe on hyvin pitkälti sidoksissa toimitilaturvallisuuteen ja vastauksissa näkyy aiheen olevan niiden vastuulla, ketkä vastaavat toimitiloista. ICT yritysten ollessa usein vuokralla jää pelastusturvallisuuden aiheet usein vuokranantajan vastuulle.

Henkilöstön koulutuksia järjestetään kaikissa haastatelluissa yrityksissä ja ylipäänsä lakisääteiset vastuut huolehditaan yrityksissä hyvin. Pelastusturvallisuus vaikuttaisi kuuluvan henkilöstön koulutuksiin alan yrityksissä.

Lakisääteisiä pelastussuunnitelmia vaikuttaa löytyvän yrityksiltä. Toisaalta niitä on ainakin osa vastaajista vaatinut vuokranantajalta ja osa on huolehtinut itse.

Palo- tai muiden harjoitusten järjestämisen käytännöt vaihtelevat laajasti yrityksissä. Toisaalta vaikuttaa siltä, että poistuminen ja kokoontuminen on ohjeistettu hyvin, mutta harjoittelu on harvaa ja satunnaista ja vaihtelee kohteittain. Kohteissa, missä tehdään tuotantotyötä tai on esim. konesaleja on pelastussuunnitelmiin luonnollisesti kiinnitetty toimistokohteita enemmän huomiota.

Palovakuutukset ja muut pelastusturvallisuuteen liittyvät vakuutukset eivät olleet vastaajajoukossa tuttuja, vastaajat epäilivät niiden olevan kunnossa ja huolehdittuna kiinteistön puolesta.

Yleisesti pelastusturvallisuuden koettiin olevan lakisääteisenä aiheena hyvässä kypsyyden tasossa yrityksissä. Aihe ei kuitenkaan ollut kovin keskeinen haastatteluiden tai kyselyn kohteille ja siitä kenties johtui hieman ristiriitainen arvio – aiheessa arvioitiin olevan kehitettävää, mutta se mitä tulisi kehittää ei tullut vastaajien osalta eritellyksi. Pelastusturvallisuuden kytkös kiinteistöihin ja vuokrasopimuksiin on keskeistä alan yritysten kannalta ja näihin sopimuksiin voisi olla hyödyllistä kiinnittää huomiota.

4.2.4 Tuotannon ja toiminnan turvallisuus

Tuotannon ja toiminnan turvallisuus aiheena sai kyselyssä keskiarvoksi 3,0. Arviot jakaantuivat korkeimmalle tasolla 4 40,6%, tasolle 3 31.3%, tasolle 2 18,7% ja tasolle 1 9,4%. Arviot painottuivat selvästi asteikon parempaan päähän ja yritykset kokivatkin aiheen olevan tarpeen hyvässä hallinnassa.

Kun kysyttiin toimintojen prioriteettia yrityksessä, oli jopa 25% vastaajista arvioinut aiheen viimeiseksi ja 15,6% toiseksi viimeiseksi. Samaan aikaan näkyi yrityksissä nostetun aihe jopa sijalle 8 (12,5%). Eron voi tulkita johtuvan yritysten välisistä liiketoiminnan eroista – kaikki ICT yritykset eivät koe tekevänsä tuotantoa, jonka turvallisuuteen tulisi kiinnittää huomiota. Tähän vaikuttaisi vaikuttaneen myös se, että tuotanto ja toiminta koettiin vahvasti olevan riippuvainen aiheista, joihin omat vaikutusmahdollisuudet olivat pienet, kuten valmisohjelmistojen toimitukset tai tuotannon riippuvuudet tietoliikenneyhteyksistä.

Ohjelmistokehityksen turvallisuus liittyy vahvasti tuotannon ja toiminnan turvallisuuteen ja se vaikutti olevan useimmille haastatelluille tuttu aihe, mutta ei ollut päällimmäisenä kehitettävien aiheiden listalla. Ohjelmistokehitys on kuitenkin vain osa vastaajien liiketoiminnasta. Aihe oli ennemminkin riippuvainen asiakkaiden vaatimuksista kuin omasta proaktiivisuudesta.

Tuotannon ja toiminnan turvallisuus oli nostettu kehitettävien aiheiden listalle useammankin vastaajan toimesta. Kehitettäväksi se oli nostettu mm. koska epäiltiin direktiivien niin tekevän ja toisaalta tunnistettiin, että nopea teknologinen kehitys kannustaa kiinnittämään asiaan huomiota – erityisesti yrityksissä, missä oltiin tekemisissä sulautettujen järjestelmien tai automaation kanssa.

Toimitusketjujen turvallisuus ja sopimussuhteinen varautuminen nousi myös esiin ja siihen todettiin kiinnitetyn huomiota ollen keskeinen osa tuotannon ja toiminnan turvallisuutta. Sopimushallinta vaikutti olevan yrityksissä kuitenkin aihe, mikä oli ratkottu eri yrityksissä eri tavoin. Toimitusketjun sopimus vastuut vaihtelivat liiketoiminnoista keskitettyyn lakitoiminnon huolehtimaan malliin ja malleihin, jotka olivat jotain tältä väliltä.

Tuotannon ja toiminnan vakuuttaminen näyttäytyi kyselyn ja haastatteluiden perusteella myös vähemmän tutulta turvallisuudenhallinnan osalta. Vakuuttamista tunnistettiin tehtävän, mutta se ei vaikuttanut olevan säännönmukainen osa riskiperusteista turvallisuuskokonaisuutta. Vakuuttamisen todettiin usein olevan akselilla HR, Legal tai talous. Tyypillisimmin liiketoiminnan johdon vastuuvakuutuksia, muita vastuuvakuutuksia tai liiketoiminnan keskeytysvakuutuksia on käytössä alalla, mutta esim. projektivakuutukset eivät ole vakiintunut toimintatapa - joskin niitä on joissain tapauksissa olemassa. Logistiikkaan liittyviä vakuutuksia epäiltiin olevan olemassa.

Yleisesti Tuotannon ja toiminnan turvallisuus on yritysten oman arvion mukaan hyvässä tilanteessa, mutta selvityksen toteuttajalle jää kokonaisuudesta mielikuva, ettei aihe ole tuttu. Vaikuttaa siltä, että se mitä kaikkea kuuluu tuotannon ja toiminnan turvallisuuteen vaihtelee yrityksittäin eikä siihen ole erityisesti keskitytty kuin suurimmissa yrityksissä.

4.2.5 Ympäristöturvallisuus

Ympäristöturvallisuuden kypsyys sai kyselyssä keskiarvon 2,5 ja arviot jakaantuivat tasaisesti kaikille asteikon arvioille (Korkeimman arvosanan 4 antoi 21,90%, arvosanan 3 28,10%, arvion 2 25,00% ja Arvion 1 25% vastaajista). ICT-alan yrityksissä ympäristöturvallisuuden kypsyys vaihtelee laajasti.

Kun kysyttiin aiheen prioriteettia yrityksen toiminnassa, nosti sen samalla 18,8% tärkeimmäksi aiheeksi ja 21,9% vähiten tärkeäksi aiheeksi. Joka myös alleviivaa yritysten hajanaisuutta aiheen hallinnassa.

Kysyttäessä kehitystä vaativia aiheita, nosti vain yksi vastaaja aiheen esiin korostaen energiatehokkuuteen liittyviä näkökohtia.

Haastatelluissa 10 alan suurimmassa yrityksessä on näkymä ympäristöturvallisuuteen taas hyvin kehittynyt. Lähes kaikki kokivat aiheen olevan kypsimmällä tasolla 4. Kaikki yhdistivät aiheen vastuullisuuteen, joka myös on hyvin korkealla prioriteetilla näissä yrityksissä. Kaikki haastatellut yritykset eivät kuitenkaan ole sertifioituneet aiheessa – viisi kymmenestä ilmoitti sertifioituneensa ISO14001 osalta.

Haastatteluissa korostuvat asiat ja aiheet, jotka ajavat ympäristöturvallisuutta eteenpäin. Vaikuttimiksi mainitaan vastuullisuus, asiakaspaine, maine, kilpailuetu ja monet muut aiheet, jotka koetaan tuottavan henkisen paineen – ”Ei koeta olevan vaihtoehtoa olevan tarjoamatta tähän liittyvää tietoa”. Edistävänä aiheena mainitaan myös ympäristöturvallisuustoimenpiteistä saatavat säästöt ja tehokkuus. Lisäksi aihe mainitaan hyvänä henkilöstöä rekrytoitaessa, koska valistuneet työnhakijat odottavat työnantajaltaan vastuullista toimintaa.

Ympäristöturvallisuuden toimenpiteissä on yrityksissä siis kirjoa kautta linjan – ja pelkästään haastatelluissa yrityksissä on tehty hyvin erilaisia toimenpiteitä sen nimissä. Aktiivisimmat seuraavat laitteiden kierrätystä, konesalien hiilidioksidipäästöjä tai jopa ohjelmistokehityksen hiilijalanjälkeä (Kuinka tehokasta tuotettu koodi on, jotta päästöt jäävät vähäisiksi). Sähkönkulutusta optimoidaan ja toisaalta kompensoidaan mm. istuttamalla puita.

Yritykset vaikuttavat omalla toiminnallaan myös toimitusketjun ympäristöaiheisiin ja pyrkivät vaikuttamaan teknologiajättien, kuten Microsoft, Amazon ja Google toimintaan ympäristöturvallisuuden puolesta. Aktiivisissa yrityksissä ympäristöturvallisuutta tuetaan mm. sillä, että on mahdollistettu henkilöstölle käyttää säännöllisesti työpäivä vastuullisuusaiheen edistämiseen.

Vastuullisuusraportointi ja siten ympäristöturvallisuus on myös usein seurattu erillisillä järjestelmillä ja erilaisia aihealueen mittareita voidaan seurata näistä järjestelmistä. Samoin myös johto usein seuraa näitä mittareita. N. 30% vastaajista kertoi ympäristöturvallisuuden tai vastuullisuuden olevan voimassaolevan strategian ohjaama aihe.

Ympäristöturvallisuuden ohjaus myös vaihtelee yrityksissä – vaikuttaisi siltä, että ne ketkä aiheeseen ovat erityisesti panostaneet ovat sen myös erikseen resursoineet ja johtoryhmästä löytyy vastuullisuusjohtaja tai päällikkö ja/tai sitä seurataan erillisessä työryhmässä. Toisaalta vaikuttaa siltä, että monissa yrityksissä tämäkin aihe on yksittäisen henkilön, kuten talousjohtajan, vastuulla - kuten niin moni muukin turvallisuusaihe.

Yleisesti voidaan todeta ympäristöturvallisuuden olevan alan yritysten agendalla. Yritysten välillä on tässä kuitenkin eroja ja kärjistäen voidaan väittää, että suurimmat yritykset ovat tässäkin aiheessa pisimmällä. Yritysten välisiä eroja selittää myös liiketoiminnan erot, ja mitä vähemmän fyysisen maailman resursseja yrityksellä on käytössään, sitä vähemmän aihe näkyy agendalla. Oman toiminnan tuottamia haittoja nähtiin alalla vähemmän muissa kuin energian kulutuksen aiheissa, vaikka muitakin ympäristölle haitallisia vaikutuksia on yrityksissä riippuen fyysisistä riippuvuuksista.

4.2.6 Tietoturvallisuus

Kuten ICT yrityksissä käytettyjä standardeja tarkasteltaessa (Kappale 4.1) käy ilmi, on tietoturvallisuus luonnollisesti ICT alan yritysten osalta aihe, johon eniten kiinnitetään huomiota. Aihe sai kyselyssä korkeimman maturiteetin keskiarvon 3,4. Jopa 46,9% vastaajista arvioi sen korkeimmalle kypsyyden tasolle 4. Vastaavasti 46,9% arvioi sen myös tasolle 3. Loput arvioivat sen alemmille tasoille, mutta pääasiassa aihe koettiin olevan hyvin kypsällä tasolla yrityksissä.

Toimintojen prioriteettia kysyttäessä nostettiin tietoturvallisuus tärkeimmäksi tai toiseksi tärkeimmäksi aiheeksi 43,7% vastaajista. Ja vaikka aihe koettiin varsin kypsäksi yrityksissä, koki moni sen

olevan myös tärkein kehitystä vaativa aihe. Tämä on toisaalta hyvin looginen lopputulos, koska aiheeseen on kiinnitetty eniten huomiota, on siihen liittyen tunnistettu myös eniten kehitystarpeita.

Kehitystä tuntuu tarvitsevan ohjelmistokehityksen turvalliset tavat, tietoturvallisuus hankinnoissa ja sopimussuhteissa sekä nopeasti kehittyvä teknologia. Haastatteluissa nousee esiin se haaste, että vaikka aiheessa tehdään paljon kehitystä, on se suurissa ICT yrityksissäkin haastavaa saada henkilöstön tietoisuus ja osaaminen tarvittavalle tasolle. Toinen esiin nouseva haaste on asiakkaiden kypsyyden ja sitä myötä asiakasvaatimusten vaihtelu, joka haastaa tietoturvan tehokasta toteutusta ja toisaalta toteutuskustannusten viemistä asiakashintoihin.

Tietoturvallisuuden organisoituminen yrityksissä ohjaa vahvasti sitä, kuinka turvallisuutta ylipäänsä hallitaan ICT alan yrityksissä. Tavat organisoitua vaihtelevat, mutta niistä on löydettävissä yhteisiä piirteitä. Alaluku 4.3 kuvaa laajemmin turvallisuudenhallinnan organisoitumista yrityksissä.

Tietoturvallisuus on myös aihe, jota johto yrityksissä seuraa – 90,6% kyselyn vastaajista kertoi sen olevan jollain tavalla mukana myös voimassaolevassa strategiassa. Strategiassa aihe on käsitelty hyvin eri tasoisesti – ylätason maininnoista erityiseen strategian painopisteeseen ja yrityksen arvoihin. 48,1% vastaajista myös kertoo, että aihetta käsitellään vastuullisuusotsikon alla, vaikka vastuullisuusstandardit eivät näin tee.

Yleisesti voitaneen todeta, että tietoturvallisuus on (vähemmän yllättävästi) parhaiten hallittu kokonaisturvallisuuden osa-alue ICT yrityksissä. Aihetta pidetään yrityksissä ennen kaikkea mainekysymyksenä ja siitä on liiketoiminnan edellytyksenä pidettävä hyvää huolta. Aiheen kehitystarpeet ovat alalla hyvin kehittyneitä tai vaativia ja sikäli niihin myös kiinnitetään erikseen huomiota.

4.2.7 Väärinkäytösten ja poikkeamien hallinta

Aihe sai kyselyssä vastausten keskiarvoksi 3,1 ollen aiheiden keskikastia. Suurin osa vastaajista (59,4%) oli arvioinut aiheen kypsyyden tasolle 3 ja 28,1% tasolle 4. Jakauma kuvastaa aiheeseen liittyvää pientä epävarmuutta – pitkälti lakisääteinen aihe on yrityksissä hyvinkin käsitelty, mutta ei välttämättä samojen toimintojen tai henkilöiden toimesta kuin muut turvallisuudenhallinnan aiheet.

Haastatteluissa korostui useiden vastaajien osalta tuntuma siitä, että aihe ei ollut täysin tuttu ja siihen kuuluvia asioita ei suoraan tunnistettu. EK:n mallin mukaan aiheen ensimmäinen osa oli selvästi tutumpi, eli toimintaan, henkilöstöön ja omaisuuteen kohdistuvien haitallisten tapahtumien kanssa toimiminen on tuttua – erityisesti ICT järjestelmiin liittyen. Mallin toisen osan eli varsinaisten hallintakeinojen (ennaltaehkäisyn toimet, paljastaminen, Sisäinen tarkastus, viranomaisyhteistyö ja toiminta rikostapauksissa) koettiin liittyvän ennen kaikkea finanssitoimintoihin, jotka ovat yleisimmin yritysten taloushallinnon ja juristien toimintakenttää turvallisuusihmisten keskittyessä ensimmäiseen.

Haastatelluissa yrityksissä aihe oli hyvinkin tuttu ja siihen vaikutti olevan panostettu muita enemmän. Aiheeseen tunnistettiin kuuluvaksi Ilmoituskanavat ja sisäinen tarkastus (taloudenhallintaan liittyen), joita molempia tunnistettiin olevan käytössä haastatelluissa yrityksissä hallinnan keinona.

Korostuneesti finanssitoimintojen väärinkäytökset ja poikkeamat on erillään muusta turvallisuudenhallinnasta. Poikkeamia hallitaan erityisesti tietoturvallisuuteen liittyen ja joissain yrityksissä samalla myös muihin turvallisuusaiheisiin, kuten fyysiseen turvallisuuteen liittyen, mutta erillään taloushallinnon poikkeamista. Vaikuttaisi siltä, että yritysten liiketoiminnan riskienhallinnassa ja esim. kriisinhallinnassa näkyy talousaiheet ja mm. väärinkäytöksiin varautuminen jopa paremmin kuin muut turvallisuusaiheet. Tämä johtunee mm. pörssilainsäädännöstä ja sen toteutuksesta (hallinnan vastuut organisaatiossa) yrityksissä.

Toimintojen prioriteettia kysyttäessä ei väärinkäytösten ja poikkeamien hallintaa nostettu tärkeimmäksi tai jätetty viimeiseksi. Enemmistö arvioi sen neljänneksi (34,4% vastaajista). Aihetta ei myöskään mainittu kehitystä vaativaa aihetta kysyttäessä.

Aiheeseen liittyvä vakuuttaminen oli myös vastaajajoukossa vieras aihe, jonka kuitenkin arveltiin olevan kunnossa. Yleisesti ottaen vakuuttaminen osana kokonaisturvallisuudenhallintaa ei vaikuttaisi olevan saumattomasti integroituna turvallisuudenhallinnan kokonaisuuteen.

Yleisesti väärinkäytösten ja poikkeamienhallinta ICT yrityksissä vaikuttaisi olevan varsin kypsä ja hallittu aihe. Siihen on erikseen kiinnitetty huomiota ja sen hallinta on vastuutettu organisaatioissa. Taloudenpitoon liittyvät väärinkäytökset ja poikkeamat on hallittu sekä samoin muut väärinkäytökset ja poikkeamat (esim. ICT järjestelmien osalta) on hallittu, mutta eri prosesseissa talouden kanssa.

4.2.8 Varautuminen ja kriisinhallinta

Varautuminen ja kriisinhallinta sai kyselyssä keskiarvon 2,8 ollen alempaa keskikastia. Arviot aihealueen kypsyydestä jakaantuivat arvosanoille 2, 3 ja 4 niin, että suurin osa arvioi kypsyydeksi 3 (37,5%).

Aiheen prioriteettiä kysyttäessä toiminnassa hajosi vastaukset laajasti, mutta suurin osa vastaajista oli sijoittanut toiminnon prioriteetissä kuudenneksi (21.9%). Yksikään vastaaja ei ollut sijoittanut tehtävää tärkeimmäksi. Vastauksista voidaan päätellä se, että pääpiirteissään varautumiseen ja kriisinhallintaan käytetään suhteessa vähemmän resursseja kuin moniin muihin aiheisiin.

Kun kysyttiin aiheita, joita tulisi kehittää, nimesi neljä vastaajaa aiheen vaativan kehitystä. Yhdistettynä tietoon siitä, että aihe ei ole yrityksissä prioriteettilistoilla voidaan melko varmasti todeta, että aihe on kypsymätön koska se ei ole ollut yritysten turvallisuustoimenpiteissä mukana.

Haastatelluista yrityksistä useimmat arvioivat aiheen myös tasolle kolme, joka kertoo myös siitä, että kehitettävää arvion mukaan on. Vaikka arviot haastatelluissa yrityksissä olivat samankaltaisia kuin kyselyssä vaikuttaisi haastateltujen yritysten olevan kypsempiä tässäkin toiminnassa. Useimmat mm. kuvaavat kriisinhallintatiimien ja kriisinhallintamallien ja suunnitelmien olevan olemassa ja koulutetun henkilöstölle. Useilla on kriisinhallintaan sovittu omat organisaationsa ja määritelty vastuut häiriötilanteiden varalle.

Tässäkin aiheessa vaikuttaisi olevan suuria asiakkuuskohtaisia eroja – eli mitä valistuneempi asiakas, sen pidemmälle on suunnittelu viety. Yrityksen oman toiminnan ja asiakaskohtaisten suunnitelmien välillä ei välttämättä ole siis yhteyttä.

Haastatteluista kehitystarpeena nousee suunnitelmallisuuden lisääminen ja harjoittelun kautta mallien kehittäminen. Asiakassopimussuhteissa tehtävän kriisinhallinnan suunnittelun epäiltiin vaativan toimenpiteitä. Haastatteluista löytyy myös havaintoja siitä, että kriisimallit ovat eri tavalla hallittuna perinteisemmän turvallisuuden puolella ja ICT aiheisten kriisien osalta tulee malleja yhdenmukaistaa ja toisaalta havaintoja on myös siitä, että ICT aiheinen varautuminen on pitkälle viety mutta muuten ei – eli yhteenvetona voinee todeta, että myös varautumisessa ja kriisienhallinnassa (kuten riskienhallinnassa) tulee harkita prosessien yhdenmukaistamista ja samoihin prosesseihin viemistä. Yhtenä havaintona nostettiin myös esiin se, että varautumista ei ole mietittynä poikkeusoloihin asti – muuten kuin henkilöstön VAP-varausten osalta. Vaikuttaisi siis siltä, että valmiussuunnittelua tulee miettiä osana jatkuvuudenhallintaa – jotta liiketoiminnalla on edellytyksiä jatkua myös poikkeusoloissa.

Varautuminen ja kriisinhallinta on ylipäänsä yritysten agendalla kehitystä vaativa aihe. Asiakaskohtaisista ratkaisuista tulisi päästä yritysten tason nostoon niin, että se kattaa asiakasvaatimukset. Muutakin kehitettävää on, kuten asiakassopimussuhteissa yhdessä tehtävä suunnittelu ja harjoittelun kautta toiminnan kehittäminen. Valmiussuunnittelun tekeminen poikkeusolojen varalle on myös selvityksen perusteella selvä kehitysaihe.

4.2.9 Työturvallisuus (työterveyshuolto ja työsuojelu)

Kyselyn perusteella Työturvallisuuden aihe on arvioitu olevan yksi kypsimmistä turvallisuusaiheista yrityksissä, jopa 46,9% arvioi sen kypsimmälle tasolle 4. Kyselyssä aihe sai kypsyydelle keskiarvon 3,3, joka on tietoturvallisuuden jälkeen kehittynein arvio. Toimintojen priorisoinnissa taas vastaukset hajosivat kaikille sijoille ja useimmat vastaajat olivat arvioineet sen olevan prioriteettisijalla 5 (18,7%).

Kehitystä vaativissa aiheissa Työturvallisuutta ei ole nostettu esiin. Aiheen koetaan lakisääteisenä olevan hyvin hallinnassa eikä sen koeta olevan ICT alan yrityksissä samalla tavalla tärkeää kuin

esim. teollisuudessa. Tässä ICT yritykset vaihtelevat sikäli, että toisilla on enemmän fyysisiä riippuvuuksia kuin toisilla ja tällöin aihe on tärkeämpi kuin jos toimitaan täysin virtuaalisesti.

Haastatelluissa yrityksissä on kaikissa lakisääteisenä työsuojeluun liittyvä organisaatio olemassa ja se tekee aktiivisesti työtään. Aiheita myös seurataan ja mitataan kyselyin ja HR-järjestelmän mittauksin, ja tulosten perusteella tehdään toimenpiteitä.

Haastatteluiden mukaan aihealueen vastuutuksessa tai organisoitumisessa on eroja – osassa yrityksiä on hankittu työsuojelu palveluna ja osassa järjestetty itse esim. henkilöstöhallinnon tai taloushallinnon ollessa vastuussa.

Kehitettävää aiheeseen liittyen vaikuttaisi olevan esimiestyössä – useampikin vastaaja nostaa esiin, että sitä on tuoreeltaan kehitetty tai siinä on tunnistettu olevan kehitettävää. ICT yrityksissä työturvallisuuden aiheissa korostuvat etätyöolosuhteet, ergonomia, työhyvinvointi sen erinäisine toimenpiteineen ja mm. kuntoilun tukeminen.

Yleisesti ottaen työturvallisuus on siis vahvasti ICT yritystenkin agendalla, vaikkei ole yhtä tärkeä aihe kuin muilla toimialoilla. Aiheessa on tunnistettu hyvin vähän kehitettävää, mutta esimiestyössä sitä tuntuisi olevan.

4.3 Turvallisuudenhallinnan organisoituminen

Kyselyllä ja haastattelulla selvitettiin myös yritysten turvallisuudenhallinnan organisoitumista. Saatujen vastausten perusteella malleja organisoitua turvallisuusaiheissa on yhtä monta kuin yrityksiäkin, mutta vastauksista on tunnistettavissa piirteitä keskitetystä, hajautetusta tai hybridimallista. Hybridimallisella organisoitumisella tarkoitettiin tässä mallia, missä yrityksellä on tiivis konsernitason yksikkö ja käytännön vastuuhenkilöitä liiketoiminnoissa ja tukifunktioissa.

42 vastaajan kuvauksesta organisoitumisesta 23 oli lähinnä keskitettyä mallia kuvaavia, 9 hajautettua ja 9 selvästi hybridimallisia. Kommenttien perusteella keskitetyn mallin toimijoillakin oli käytännön toteuttajia liiketoiminnoissa tai asiakaskohtaisissa kokonaisuuksissa. Korostuneesti isoimmat kansainväliset yritykset lähinnä kuvailivat organisoitumistaan hybridimallisiksi. Lisäksi selvityksen aikana havaittiin 2 suuren yrityksen purkaneen konsernitason turvallisuusfunktionsa ja päätyivät liiketoimintoihin hajautettuun turvallisuudenhallintaan. Haastatteluiden perusteella suurissa yrityksissä organisoituminen on tehnyt historiassa aaltoliikettä vuoroin hajautettuun ja vuoroin keskitettyyn suuntaan.

Useissa yrityksissä on päädytty korostamaan CISO (Chief Information Security Officer) roolia. Rooli on nähty useammankin yrityksen johtoryhmässä. Joka osaltaan korostaa tietoturvallisuuden merki-

tystä ICT alan yrityksissä. Samalla muiden turvallisuusaiheiden ollen vastuutettu esim. henkilöstöhallinnon tai taloushallinnon vastuualueelle. Korostuneesti alan yritykset siis panostavat tietoturvallisuuden hallintaan siihen varatuin resurssein ja muut yritysturvallisuuden osa-alueet ovat tyypillisesti hallittu muun tehtävän tai toiminnon osana sivutuotteena.

Kyselyyn saatujen kommenttien sekä haastatteluiden perusteella organisoitumisessa on kehitettävää monien vastaajien mielestä. Kehitystä kaipaaviksi aiheiksi on esitetty seuraavia aiheita:

- hallituksen ja johtoryhmän roolien ja vastuiden selkeyttämisen tarve
- operatiivisen toiminnan ja johdon kommunikaatio turvallisuusaiheista
- kokonaisturvallisuuden tilannetietoisuus
- aihe omistajien (ja vastuun) nimeämisen tarve
- lisäresursoinnin tarve

Yleisenä havaintona organisoitumisesta voinee todeta, että organisoituminen ja turvallisuusaiheiden vastuutus yrityksessä vaikuttaa siihen, kuinka hyvin kokonaisturvallisuuden tilannetta ymmärretään organisaatiossa ja kuinka turvallisuustieto välittyy johtoryhmänkin käsiteltäväksi. Vaikuttaisi siltä, että tilannetta ymmärretään paremmin kokonaisuutena organisaatioissa, missä myös lakisääteisiä turvallisuudenhallinnan osa-alueita (kuten väärinkäytökset, vakuuttaminen, paloturvallisuus) johdetaan yhdessä tietoturvallisuuden kanssa.

Johdon raportoinnista ja tilannekuvan muodostamisesta kysyttäessä ei kyselyn ja haastatteluiden mukaan vaikuta siltä, että yrityksissä olisi mitään vakiintunutta yhdenmukaista toimintatapaa. Raportointisyklit ja tavat kerätä turvallisuuteen liittyvää informaatiota vaihtelevat suuresti. Myös se, käsitteleekö johtoryhmä turvallisuutta kokonaisuutena, vaihtelee ja vaikuttaisi mm. siltä, että monissa yrityksissä on turvallisuushavaintoja käsittelevä ryhmä erikseen ja johtoryhmä käsittelee lähinnä sinne eskaloituja havaintoja. Yrityksen koko vaikuttaa myös tässä, eli mitä pienempi yritys on, sitä todennäköisempää on, että johtoryhmä käsittelee tietoa kootusti. Tietoteknisten järjestelmien käyttö turvallisuuteen liittyvien havaintojen käsittelyssä on arkipäivää ja näkymiä tietoon on saatavilla – samalla kuitenkin osa vastaajista kertoo, ettei tietoa koosteta.

78,1% vastaajista kertoo, että turvallisuudelle on asetettu mittareita ja niitä mitataan. Erityisesti seurataan tietoturvallisuuden toteutumista laajasti. Muita turvallisuudenhallinnan osa-alueiden tavoitteita on asetettu hyvin vaihtelevasti. Mitattavat suureet myös vaikuttavat vaihtelevan jopa yrityksittäin.

Johtoryhmien ja hallitusten välineenä useat vastaajat ovat nostaneet esiin sisäiset ja ulkoiset auditoinnit, joiden tuloksia tarkastellaan ja joiden pohjalta päätetään toimenpiteistä. Voisikin olla hyödyllistä miettiä suositus sisäisille ja ulkoisille arvioinneille ja niiden taajuudelle.

ICT-alan yrityksissä on siis yleisesti hajontaa ja osa toimijoista on tässäkin hyvin kehittyneitä ja suurella osalla on taas valtavasti kehitettävää. Keskimäärin vaikuttaa siltä, että alan yritysten kannattaa kiinnittää huomiota organisoitumiseen ja suunnitella turvallisuuden johtaminen kokonaisuutena ja samalla suunnitella se, kuinka siihen liittyvää tietoa hallitaan johtamisen tukena.

Digipoolin toimialojen kyberkypsyysselvityksen perusteella monilla toimialoilla oli haastavaa saada operatiivisen tason kyberriskejä tai poikkeamia nostettua johdon agendalle ja tällöin toimivaksi oli todettu se, että riskejä ja poikkeamia tai yleisesti turvallisuus tietoa kommunikoitaessa olisi suotavaa kommunikoida jalostettua tietoa niin, että on arvioitu liiketoimintavaikutuksia. Tässä kyselyssä johdon raporttien sisältöä kysyttäessä on 3 vastaajaa nostanut tämän esiin johdon raportoinnin sisällössä. Tällä perusteella voisi olla hyödyllistä laajemminkin miettiä johdon raportoinnin kehitystä liiketoimintavaikutuksia arvioivaan suuntaan.

4.4 Strategia

Kun kysyttiin mitä kokonaisturvallisuuden aiheita näkyy yrityksen strategiassa vastasi jopa 90,6% vastaajista tietoturvallisuuden olevan strategiassa tavalla tai toisella. Henkilöstö ja työturvallisuus seurasivat aiheina tietoturvallisuutta, mutta selvästi harvemmissa strategioissa.

Kuva 2 Kokonaisturvallisuuden aiheet strategioissa

Strategiateksteistä puhuttaessa on yksittäistä kokonaisturvallisuuden aiheen sijaan turvallisuus yleisesti huomioituna. Turvallisuudesta puhutaan niin yritysten tuotteiden, palveluiden tai muun tekemisen yhteydessä sekä omassa toiminnassa. Aiheet, kuten ympäristöturvallisuus ja henkilöstöturvallisuus, näkyvätkin usein yritysten arvoissa, jotka ohjaavat toimintaa sisäisesti ja ulkoisesti.

Strategiassa mainittujen kokonaisturvallisuusaiheiden aiheiden ilmenemismäärä vastaa pitkälti selvityksen muita havaintoja aiheiden kypsyydestä yrityksissä. Kaikkia aiheita on jollain tasolla käsitelty, mutta monissa on kehittämisen varaa. Poikkeuksiakin toki löytyy, kuten kiinteistö ja toimitilaturvallisuus, joka oli arvioitu olevan korkealla tasolla, vaikkei ole aiheena useinkaan strategiassa. Vastuullisuus ja ympäristöaiheet taas korostuvat ja nousevat esiin kaikissa yrityksissä, mutta sen taso vaihtelee suuresti ja on vähän yllättäen harvemmassa yrityksessä strategia aiheena.

Turvallisuudesta ja strategioista puhuttaessa vaikuttaisi monessa strategiassa turvallisuus aiheiden kuuluvan vastuullisuus teemaan. Vastuullisuus kattaa mallien mukaan ympäristöturvallisuuden, sosiaalisen vastuun ja hyvän hallinnon tai taloudellisen oikein toimimisen, joka taas kuuluu kokonaisturvallisuudessa väärinkäytösten aiheeseen. Kyselyn vastausten perusteella vastuullisuusteemaan miellettiin kuuluvan ennen kaikkea ympäristö- ja työ- sekä henkilöstöturvallisuus ja näiden perässä tietoturvallisuus. Mutta esim. väärinkäytösten ehkäisyn koki harvempi kuuluvan aiheeseen yrityksessään.

Tietoturvallisuutta käsitellään ja siitä raportoidaan useimmiten vastuullisuusteemasta erillään, vaikkakin joissain tapauksissa sen voi lukea olevan osa vastuullista toimintatapaa – tässä vastuullisuusstandardit ohjaavat eikä tietoturvallisuuden tilaa siten raportoida useinkaan sen osana. Vastuullisuudesta raportoidaan usein taloushallinnon toimesta käyttäen ESG (Environmental, Societal, Governance) mallia tai CSRD (Corporate Sustainability Reporting Directive, 2022) direktiivin myötä muodostetuilla ESRS (European Sustainability Reporting Standards) raportointimalleja, jotka eivät suoraan edellytä tietoturvallisuuden raportointia. Vastuullisuuteen tai ehkäpä tarkemmin kestävään kehitykseen (esim. YK:n malli) liittyen vastauksissa näkyy esimerkkejä siitä, kuinka tietoturvallisuuttakin on käsitelty teeman sisällä – erityisesti aiheena on tällöin ollut vastuu henkilöön liitettävästä tiedosta ja vastuu asiakkaiden luottamuksellisesta tiedosta laajemmin.

Pääpiirteissään strategian ohjaus näyttäisi vaikuttavan turvallisuusaiheiden kypsyyteen yrityksessä tai ainakin niin, että aiheen ollessa strategiassa on todennäköisempää, että siihen on panostettu ja kypsyys arvioitu näin suuremmaksi.

4.5 NIS2- ja CER-direktiiveistä

Critical Entities Resilience (CER) ja Network and Information Security, 2023 (NIS2) -direktiivit ohjaavat EU jäsenvaltioita päivittämään lainsäädäntöään. Jäsenvaltioiden lainsäädännössä tulee eritellä kriittisen infrastruktuurin toimijoita sekä kriittisiä ict palveluita tuottavia toimijoita ja asettaa näille velvoitteita turvallisuuden toteutuksen suhteen. Sen lisäksi että se velvoittaa kehittämään turvallisuutta velvoittaa se turvallisuuden tilasta raportointia viranomaisille. Direktiivien jäsenvaltioille osoittama siirtymäaika lainsäädännön voimaansaattamiseksi etenee jotakuinkin rinnakkain, ja niiden tulee olla voimassa 2024 vuoden viimeisestä neljänneksestä alkaen. Kun kysely ja haastattelut tehtiin

tätä selvitystä varten, ei ollut vielä julkistettu kotimaisen lainsäädännön ehdotuksia, ja vastauksia tuotettiin direktiivitekstien viitoittaman tiedon perusteella.

Direktiivien myötä tehtävän kotimaisen lainsäädännön vaatimusten kohteena olemisesta kysyttäessä vastasivat kaikki haastatellut ja 72% kyselyyn vastanneista olevansa NIS2 direktiivin kohteena. CER direktiivi ei ollut vastaavasti tuttu ja sen kohteena arvioi olevansa 31% vastaajista – samalla haastatteluissa pohdittiin sitä tulevatko ICT yritykset olemaan kohteena ja jos, niin ehkäpä juuri alan suurimmat toimijat. 31% Kyselyn vastaajista vastasi rehellisesti, ettei tiedä tuleeko se koskemaan heitä.

Kun kysyttiin direktiivien myötä yrityksille tulevia vaikutuksia, arvioivat monet kyselyyn vastanneista ja haastatelluista, että täyttävät jo nykyisellään tiukkoja vaatimuksia ja siten direktiivien vaatimukset eivät tulisi vaikuttamaan. Samalla osa vastaajista kuitenkin koki, että heihin kohdistuu uusia vaatimuksia – joka vastaa aiempien kohtien havaintoja yritysten välisen kypsyyden hajonnasta. Useat vastaajat arvioivat direktiivien tuottavan uusia asiakasvaatimuksia olivatpa he itse kohteena tai eivät.

Ilmeisin, kaikkien tunnistama, vaikutus on raportointivelvollisuudet, jotka tulee yrityksessä vastuuttaa, toteuttaa ja kirjata suunnitelmiin.

Merkittävä osa vastaajista nosti esiin sen, että yrityksen tulee pystyä esittämään (kyber)turvallisuudenhallintansa kypsyystaso niin viranomaisille kuin asiakkaillekin ja se tultaneen tekemään erilaisin sertifioinnein tai todistuksin. 53% kyselyyn vastanneista koki, että direktiivit ovat saaneet yrityksen pohtimaan lisäsertifiointien tarvetta, jotta vaatimustenmukaisuus voidaan osoittaa.

Yleisesti voinee todeta, että direktiivit tulevat vaikuttamaan ICT alan yrityksiin suoraan ja välillisesti asiakkaiden kautta. Yritysten kypsyys direktiivien aiheissa vaihtelee ja sen myötä turvallisuuden toteutuksen tarvittavan työn määrä myös vaihtelee yrityksittäin. Vaikutuksina on lisäksi lisääntyvä raportointivelvollisuus sekä tarve osoittaa niin kyber- kuin muun turvallisuudenhallinnan kypsyyden tila.

4.6 Riskipeilaus

Jos tarkastellaan kohdassa 2.2.9 esiteltyjä alan liiketoimintaa uhkaavia riskiaiheita ja peilataan niitä EK:n yritysturvallisuusmallin osa-alueiden selvityksen osoittamaan kypsyyteen, voidaan arvioida sitä, missä prioriteettijärjestyksessä turvallisuusaiheita tulisi lähteä kehittämään alalla.

Seuraavassa taulukossa on esitetty arvio siitä, mitkä riskiaiheet ovat kullekin turvallisuuden osa-alueelle oleellisia. Arvio on annettu perustuen osa-alueen kuvaukseen ja selvitystyöstä saatuun tietoon yrityksen tilanteesta vastaamalla riskiaiheittain seuraaviin kysymyksiin.:

- Tuottaako uhka ilmeisiä riskejä turvallisuuden osa-alueessa ja siihen kuuluvissa aiheissa?

- Onko turvallisuuden osa-alueella ja riskiaiheella jokin kytkös?

Taulukko 8 Turvallisuuden osa-alueiden suhde riskiaiheisiin

KA		Rikollisuus	Tiedustelu	Vaikuttaminen	Asiakas	Palvelu	Teknologia	Tuotanto	Alihankinta	Kehitys	Henkilöstö	Pandemia	Talous	Häiriöt	Luonnonilmiöt	Sota	Yht.	Käänteinen suhdeluku KA/Yht.
2,5	Ympäristöturvallisuus	Kyllä	Ei	Ei	Kyllä	Ei	Kyllä	Kyllä	Kyllä,	Kyllä	Kyllä	Ei	Ei	Kyllä	Ei	Ei	8	3,20
2,8	Varautuminen ja kriisinhallinta	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	15	5,36
2,8	Pelastusturvallisuus	Ei	Ei	Ei	Kyllä	Kyllä	Kyllä	Kyllä	Ei	Ei	Kyllä	Ei	Ei	Kyllä	Kyllä	Kyllä	8	2,86
3	Tuotannon ja toiminnan turvallisuus	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	15	5,00
3,1	Henkilöturvallisuus	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Ei	Ei	Ei	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	12	3,87
3,1	Kiinteistö- ja toimitilaturvallisuus	Kyllä	Kyllä	Ei	Ei	Ei	Kyllä	Kyllä	Kyllä	Ei	Kyllä	Ei	Ei	Kyllä	Kyllä	Kyllä	9	2,90
3,1	Väärinkäytösten ja poikkeamien hallinta	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Ei	Kyllä	Kyllä	Ei	Ei	12	3,87
3,3	Työturvallisuus (työterveysshuolto ja työsuc	Kyllä	Kyllä	Kyllä	Ei	Ei	Ei	Ei	Kyllä	Ei	Kyllä	Kyllä	Kyllä	Kyllä	Ei	Kyllä	9	2,73
3,4	Tietoturvallisuus	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Ei	Kyllä	Kyllä	Ei	Kyllä	13	3,82

Vastausten perusteella on laskettu numero riskien vaikutuksesta turvallisuuden osa-alueeseen niin että mitä useampi riskiaihe on sille relevantti, sitä suurempi numero on. Numeron avulla on laskettu käänteisesti suhdeluku. Suhdeluku on jaettu turvallisuuden osa-alueen kyselyssä saamalla keskimääräisellä kypsyysarviolla ja näin on muodostettu riskipainotettu prioriteettijärjestys turvallisuuden osa-alueille ICT-alalla huomioitavaksi.

Taulukko 9 Riskipainotettu prioriteettijärjestys turvallisuuden osa-alueille ICT-alan yrityksissä

Prio.	Suhde-luku	Turvallisuuden osa-alue
1.	5,36	Varautuminen ja kriisinhallinta
2.	5,00	Tuotannon ja toiminnan turvallisuus
3.	3,87	Henkilöturvallisuus
4.	3,87	Väärinkäytösten ja poikkeamien hallinta
5.	3,82	Tietoturvallisuus
6.	3,20	Ympäristöturvallisuus
7.	2,90	Kiinteistö- ja toimitilaturvallisuus
8.	2,86	Pelastusturvallisuus
9.	2,73	Työturvallisuus (työterveyshuolto ja työsuojelu)

Havaintona todettakoon, että näin priorisoituna jäivät lakisääteiset työturvallisuus ja pelastusturvallisuus aiheet järjestyksessä viimeiseksi. Tämä korreloi myös selvitystyön havaintoon aiheiden käsittelystä alalla. Johtopäätöksenä voidaan väittää, että riskipeilauksen myötä näiden aiheiden prioriteetti alalla ei muuttunut ja siten kypsyyden voi tulkita olevan alalle riittävä.

4.7 Selvityksen havaintoja osa-alueittain

Kappale esittelee yritysturvallisuuden osa-alueet prioriteettijärjestyksessä, joka on saatu aikaan painottamalla osa-alueen suhteellista kypsyyttä toimialan tyypillisimmillä riskeillä. Samalla esitellään

siihen liittyvät havainnot selvityksestä. Havaintoja esitetään siten että niitä voidaan käsitellä suosituksina alan yrityksille – asioita, joihin on hyvä kiinnittää huomiota.

Taulukko 10 Turvallisuuden osa-alueet ja suositukset prioriteettijärjestyksessä

Prio.	Turvallisuuden osa-alue	
1.	Varautuminen ja kriisinhallinta	• Aiheen prioriteettia turvallisuustoimenpiteissä tulee nostaa. • Varmista kriisinhallintamallien ja -suunnitelmien olemassaolo ja kouluta ne henkilöstölle. Määrittele organisaatio, roolit ja niiden vastuut ja valtuudet. • Pyri asiakaskohtaisista suunnitelmista siihen, että yrityksen oman toiminnan mallit käyvät useimmille asiakkaille. • Lisää suunnitelmallisuutta ja harjoittele suunniteltua ja edelleen kehitä toimintatapoja. • Kiinnitä huomiota asiakassopimussuhteissa tehtävään kriisinhallintaan ja pyri sopimaan sen periaatteista. • Suositellaan perinteisen turvallisuuden ja ICT turvallisuuden aiheiden prosessien yhdenmukaistamista tai samoihin prosesseihin viemistä. • Laajenna varautumissuunnitelmia paremmin kattamaan myös poikkeusolot, jotta liiketoiminnalla on edellytyksiä jatkua myös poikkeusoloissa.
2.	Tuotannon ja toiminnan turvallisuus	• Määrittele tuotannon ja toiminnan turvallisuuden kokonaisuus yrityksessäsi • Arvioi ohjelmistokehityksen turvallisuuden vaikutukset omalle yritykselle ja asiakkaille – vaikka yritys ei itse ohjelmistokehitystä tekisikään. Valmisohjelmistoissakin olevat puutteet voivat aiheuttaa harmia asiakkaille. • Arvioi direktiivien vaikutukset tuotannon toimintaan • Määrittele tavat toimia, jolla varmistat teknologian nopean kehityksen myötä nousevien riskien tunnistamisen. • Kiinnitä huomiota toimitusketjujen turvallisuuteen ja sopimussuhteissa varautumisaiheisiin. • Tarkastele kriittisesti tapaa, jolla olette organisoituneet sopimushallinnassa, jotta se ottaa tuotannon turvallisuusaiheet paremmin huomioon. • Varmista, että vakuuttaminen kuuluu myös erottamattomana osana Tuotannon ja toiminnan turvallisuudenhallinnan välineistöä eikä jää erilliseksi liiketoiminnan kapean tarkastelun osaksi.
3.	Henkilöturvallisuus	• Aseta tavoitteet ja kehitä henkilöturvallisuuden mittaustapoja • Kehitä matkustusturvallisuutta siihen paljon huomiota kiinnittäneiden organisaatioiden tuella. • Tarkastele myös tarvetta henkisen tuen palveluille henkilöstölle turvallisuustapahtumissa ja ulota palvelut perhepiiriin ja vaikka ulkoistat palvelun kanna itse vastuu. • Keskity etätyön turvallisuuden haltuunottoon ja tarjoa henkilöstölle ratkaisuita siihen. Määrittele etätyönteon työnantajan vastuut, velvollisuudet ja valtuudet.
4.	Väärinkäytösten ja poikkeamien hallinta	• Kehitä väärinkäytösten ja poikkeamienhallinnan kokonaisuutta yrityksessä laajantamalla sen vaikutuspiiriä • Kiinnitä huomiota siihen, ovatko finanssitoimintojen väärinkäytökset ja poikkeamat erillään muusta turvallisuudenhallinnasta ja esim. ICT poikkeamista. • Varmista, että vakuuttaminen kuuluu myös erottamattomana osana väärinkäytösten ja poikkeamien hallinnan välineistöä muutenkin kuin finanssitoimintojen osana.
5.	Tietoturvallisuus	• Nosta tietoturvallisuus osaksi vastuullista toimintatapaa, varmista sen paikka yhtenä yrityksen arvona. • Panosta kulttuuriin ja tee toimenpiteitä henkilöstön tietoisuuden ja osaamisen varmistamiseksi. • Kiinnitä huomiota ohjelmistoturvallisuuteen niin valmisohjelmistoissa kuin osana ohjelmistokehityksen turvallisia tapoja.

		• Kehitä tapoja varmistaa tietoturvallisuus hankinnoissa ja toimitussopimussuhteissa • Määrittele tavat toimia, jolla varmistat teknologian nopean kehityksen myötä nousevien riskien tunnistamisen. • Pyri nostamaan yrityksen oman toiminnan maturiteetti yli korkeimpien direktiivi tai asiakasvaatimusten, jotta se palvelee tehokkaasti asiakastoimituksissa ja täyttää ilman eri ponnistuksia lainsäädännön vaatimukset ja mahdollistaa ennakoitavan hinnoittelun.
6.	Ympäristöturvallisuus	• Toimi vastuullisesti ja huomioi ympäristöturvallisuus • Käännä vaikea aihe hyödyksi ja nosta se yrityksen arvoihin – nosta esiin ympäristöturvallisuustoimista saatavat hyödyt – tehokkuus, säästöt ja maine. • Seuraa erityisesti energiatehokkuutta, mutta myös muita yrityksen vaikutuksia ympäristöön. • Seuraa laitteiden kierrätystä, toimistojen ja konesalien hiilidioksidipäästöjä • Harkitse seurattavan ohjelmistokehityksen hiilijalanjälkeä ja tuotetun koodin energiatehokkuutta tai vaadi valmisohjelmistoja siitä kertomaan. • Kompensoi yrityksen hiilijalanjälkeä. • Pyri vaikuttamaan myös toimitusketjun ympäristöaiheisiin ja pyri vaikuttamaan teknologiajättien, kuten Microsoft, Amazon ja Google toimintaan ympäristöturvallisuuden puolesta. • Anna henkilöstölle mahdollisuuksia vaikuttaa.
7.	Kiinteistö- ja toimitilaturvallisuus	• Suunnittele turvallisuusratkaisut kiinteistön käyttötarpeen mukaan. • Nosta tilaturvallisuuden taso kattamaan useimmat asiakasvaatimukset sekä lainsäädännön vaatimukset ja toisaalta henkilöstön suojauksen tarpeet. • Harkitse tilaturvallisuuden havaintojen hallintaa samoissa prosesseissa kuin muitakin turvallisuushavaintoja (esim. ict) tilannekuvan muodostamiseksi. • Vuokralla oltaessa varmista, että vuokranantajan vastuut ovat selvät. • Varmista oma ohjauskyvykkyys myös yksityisen turvallisuusalan palvelutuottajaan – suorassa sopimussuhteessa tai vuokranantajan kautta. • Vastuuta kiinteistöturvallisuus omalle vastuuhenkilöstölle, vaikka ette toimisi omassa kiinteistössä. • Tee yhteistyötä vuokranantajan tai kiinteistön edustajien kanssa. • Kiinnitä huomiota siihen, miten kiinteistöjen ja niihin liittyvien palveluiden sopimushallinta on järjestetty. Onko sopimushallintaan resursseja ja onko turvallisuusaiheet mukana sopimuksissa em. vaatimustasolla.
8.	Pelastusturvallisuus	• Kiinnitä huomiota vuokrasopimuksiin pelastusturvallisuuden osalta. • Älä jätä pelastusturvallisuuden aiheita vuokranantajan vastuulle, vaan pidä niistä huoli kuin omassa kiinteistössäkin. • Huolehdi henkilöstön koulutuksista ja varmista säännöllinen harjoittelu. • Varmista pelastussuunnitelmien olemassaolo myös vuokrasuhteissa ja varmista suunnitelmien riittävä laatutaso. • Varmista vakuutusten olevan huolehdittuna.
9.	Työturvallisuus (työterveyshuolto ja työsuojelu)	• Tarkastele ja kehitä työterveyshuollon palveluita jatkuvasti • Tarkastele työterveyshuollon ja työsuojelun sopimusten kattavuutta (kun ulkoistettu) • Kouluta henkilöstöä ja kehitä esimiestyötä työsuojelun kannalta • Kehitä työsuojelun konseptia kattamaan etätyöolosuhteet, ergonomia, työhyvinvointi ja tue kuntoilua

Tässä kuvatut suositukset on myös muutettu tavoitetilaksi. Dokumentin liite 6 kuvaa sanallisesti tavoitetilan digipoolin verkoston yritysten toiminnalle yritysturvallisuuden osa-alueittain.

5 Digipoolin toiminnan kehitys

Digipooliin kuuluvat huoltovarmuuskriittiset ICT alan yritykset ovat hallinneet ja teknisesti toteuttaneet kyberturvallisuuden osa alueen keskimäärin hyvin kypsällä tasolla, ja tästä huolimatta on Digipoolin toimintaa sen johtoryhmän ohjaamana ohjattu keskittymään toiminnassaan Kyberturvallisuuden kypsyyden kasvattamiseen. Tämä on ollut tietoinen valinta ja on vaikuttanut mm. siihen, että iso-osa toiminnasta on ohjattu tukemaan muiden toimialojen yrityksiä niiden jatkuvuudenhallinnan ICT riippuvuuksissa.

Tarjoamaa oman alan yritysten kokonaisturvallisuudenhallinnan tukemiseksi on kehitetty selvästi toissijaisesti ja tähän on määrä tehdä muutos. Muutoksen tueksi tarvitaan tietoa nykytilasta, jota tämäkin selvitys edustaa. Tämä kappale kuvaa tutkimuksen myötä heränneitä kehitysajatuksia Digipoolin toiminnan kehittämisestä niin, että se paremmin tukee yritysten kokonaisturvallisuudenhallinnan kehitystä. Kappale nostaa esiin mahdollisia toiminnassa huomioitavia aiheita, joiden edistämisestä päätetään Poolin toimikunnissa yhdessä elinkeinoelämän edustajien kanssa.

5.1 Digipoolin toiminta ja sisältöaiheet

Digipoolin toiminta perustuu dialogiin, jota käydään yritysten kanssa niiden edustajien välityksellä erilaisilla tavoilla. Yritysedustajia tavataan kahdenvälisesti ja tutustutaan yrityksiin ja tarjotaan niille palveluita varautumisen (jatkuvuudenhallinta ja valmiussuunnittelu) tukemiseksi. Dialogia käydään myös Digipoolin vakiintuneissa toimintaryhmissä, joita ovat Johtoryhmä, Kyberryhmä ja ICT-ryhmä.

Johtoryhmän roolina on asettaa strategia ja tavoitteet toiminnalle, päättää rahankäytöstä ja linjata toimintaa strategian ohjaamana. Kyberryhmä edustaa eri toimialoilla kulloinkin ajankohtaisia toiminnan kehitysaiheita ja tarpeita. Kun taas ICT ryhmä edustaa pooliin kuuluvia yrityksiä, ja käsittelee muulle huoltovarmuusorganisaatiolle kriittisiä tarjoama-aiheita sekä oman alan yritysten varautumisen kehitystä.

Lisäksi dialogia tehdään jaoksissa, jotka pyrkivät pureutumaan Huoltovarmuusorganisaation yritysten tarvitsemiin palveluihin – tarjoama-aiheisiin ja niiden tuotantoedellytyksiin, eli samoin edistävät myös oman alan varautumista näissä aiheissa. Kaikki ryhmät ovat suoraan tai epäsuorasti neuvonantajina Huoltovarmuuskeskuksen Digitaalinen turvallisuus 2030 -kehitysohjelmassa (DT2030) ja voivat toisin sanoen nostaa kehitysehdotuksia ohjelmaan toteutettavaksi kehitysprojektiksi.

Digipooli myös toteuttaa itse projekteja kehitysohjelmaan kuuluvien projektien lisäksi – kaikissa projekteissa on määrä tarjota verkoston yrityksille osallistumisen mahdollisuuksia em. dialogin mahdollistamiseksi. Projektien lisäksi dialogia yritysten kanssa käydään poolin järjestämissä harjoituksissa (kuten TIETO-harjoitukset), järjestämällä koulutuksia (kuten valmius/varautumiskoulutukset, digi-

taalinen turvallisuus huoltovarmuusorganisaatiossa) sekä seminaarit (kuten vuosiseminaarit #Digi-Signaali). Muita tapoja käsitellä eri aiheita ovat mm. Työpajapäivät, missä voidaan keskittyä käsittelemään tiettyjä aiheita ja tuottaa toimenpide-ehdotuksia tai saada sinällään jo muutosta aikaiseksi.

Näin kuvattuna ei selvityksen perusteella tule suoraan vaikutuksia Digipoolin ryhmärakenteeseen tai dialogin muihin välineisiin. Ennemminkin voi nähdä asian niin, että olemassa olevissa elementeissä tulee sisältönä käsitellä tässä selvityksessä esiin nostettuja aiheita ja pyrkiä nostamaan yhteistyöllä esiin toimenpiteitä, joilla kypsyyden näissä aiheissa saisi nousemaan yrityksissä.

Digipoolin toiminnan sisältöaiheissa korostuu kyberturvallisuus nykyisen ohjauksen perusteella, mutta kuten todettua on alan yritysten omassa toiminnassa aiheen kypsyys jo korkeaa tasoa ja siten sen kehittäminen vaatii erityisiä ponnisteluita. Kyber- tai tietoturvallisuuden tukemista tulee siis edelleen jatkaa alan yritystenkin osalta, mutta sen rinnalle on hyvä ottaa muita yritysturvallisuuden osa-alueita, jotka ovat selvästi jääneet yrityksissä vähemmälle huomiolle.

Varautumisen ja kriisinhallinnan teema, joka selvityksessä tehdyn riskipeilauksen ja alan yritysten suhteellisen kypsyyden mukaan on tärkein kehityskohde, on syytä olla toiminnan ytimessä. Tämä huoltovarmuusorganisaation pooleille kenties ilmeinen havainto onkin kyberturvallisuusaiheiden rinnalla kantava teema, jota Digipooli toteuttaa mm. TIETO-harjoituksissa ja valmius/varautumiskoulutuksissa. Selvityksestä saatiin kuitenkin selviä kehitysehdotuksia sille, mitä aiheita näissä tulisi painottaa. Esim. varautumiskoulutuksissa on hyvä korostaa yrityksille sopimussuhteiden sopimussisällön merkitystä ja toisaalta yrityksen oman toiminnan tasosta suhteessa asiakassopimuksiin.

Samoin monet muut selvityksen aiheet on syytä olla osana varautumiskoulutuksia esim. asioita henkilöstöturvallisuudesta ja kiinteistö- ja toimitilaturvallisuudesta. Aiheita ja asiaa on kuitenkin jopa pieneen koulutusohjelmaan, joten selvityksen perusteella on hyvä nostaa keskusteltavaksi Digipoolin ryhmissä koulutusohjelman synnyttäminen. Huoltovarmuusorganisaation yritykset voivat lähettää henkilöstönsä jo nyt koulutettavaksi varautumiskoulutuksiin ja jatkossa olisi siis tarjolla koulutusohjelma, mihin henkilöstön eri rooleissa toimivia henkilöitä voisi lähettää koulutettavaksi. Katso myös kohta 5.2. – ehdotuksia huoltovarmuuskeskukselle poolien ohjaukseen.

Toiseksi tärkeimmäksi teemaksi noussut ’Tuotannon ja toiminnan turvallisuus’ on myös ollut digipoolin käsittelemissä sisällöissä mukana ja esim. ohjelmistokehityksen turvallisuus on ollut käsittelyssä mukana ja sitä tullaan varmasti edelleen käsittelemään, koska vaikuttaa siltä, ettei elinkeinoelämän kypsyys aiheessa ole omalla painollaan kehittymässä tarpeen nopeasti verrattuna uhkiin. Samalla aihe ei määritelmänsä mukaan ollut vastaajille tuttu kuten ei myöskään ’väärinkäytösten ja poikkeamien hallinta’ ja tietoisuutta näistä voisi olla hyvä viedä eteenpäin niihin erikseen keskittyen. Tämä voisi tarkoittaa niihin keskittyviä työpajoja yritysten kanssa tai mahdollisia seminaareja ja koulutuksia aihealueisiin liittyen.

Digipooli pyrkii myös herättelemään yritysten hallituksia ja johtoryhmiä huomioimaan digitaalisen turvallisuuden aiheita paremmin esim. strategioita ja tavoitteita asetettaessa. Selvityksen perusteella tähän kokonaisuuteen voi nähdä liittyvän yritysten organisoitumisesta ja sen merkityksestä suositusten tekemisen. Asia lienee hyvä tarjota käsiteltäväksi niissä yhteistyöryhmissä, missä strategisen halun herättelyn teemaa kulloinkin käsitellään.

Toimenpide-ehdotuksena voi kuitenkin olla myös olla uusien – johonkin tiettyyn turvallisuusaiheeseen keskittyvien - jaosten perustaminen. Sillä jaosten toiminta-ajatuksena on kerätä yhteen elinkeinoelämän edustajia, jotka roolinsa puolesta edistävät tiettyä aihetta ja sikäli alan toimijoiden itse ideoimat kehitystoimet saa heidät myös samalla sitoutumaan niiden toteutukseen omassa yrityksessä.

Kuitenkin ennen kuin toimenpiteenä lähdetään uusia jaoksia perustamaan, tulee tulokset käsitellä olemassa olevissa ryhmissä. Katso kohta 5.3.

5.2 Toimenpide-ehdotuksia Huoltovarmuuskeskukselle poolien ohjaukseen

Huoltovarmuusorganisaation poolien toimistot, eli henkilöstö, joka on käytettävissä toimenpiteiden toteutukseen, on hyvin rajallinen suhteessa kunnianhimoisiin tavoitteisiin elinkeinoelämän resilienssin kasvatuksesta verkoston toimenpitein. Tämän takia on hyvä kiinnittää huomiota tehokkuuteen ja välttää päällekkäisyyksiä.

Sen sijaan, että yksittäiset huoltovarmuusorganisaation poolit toteuttavat omia koulutuksiaan olisi tehokasta toteuttaa koulutusohjelma, joka tukee kaikkia pooleja yritysturvallisuuden eri aiheissa. Ja tätä kirjoitettaessa onkin Huoltovarmuuskeskus lähtenyt ottamaan yhteyttä pooleihin niiden toteuttamiin koulutuksiin liittyen pyrkimyksenään ensin tuottaa yhdessä kaikkia palvelevaa koulutussisältöä. Tällöin Digipooli voi keskittyä suunnittelemaan esim. digitaalisen turvallisuuden koulutuksia, jotka huoltovarmuusorganisaatiossa on kaikkien ulottuvilla.

Toisin sanoen selvityksen perusteella on tilausta koulutusohjelmalle, joka tukee myös ICT alan yritysten kokonaisturvallisuudenhallinnan kehitystä. Ja joitain aiheeseen liittyviä koulutuksia kannattaa tehdä poolin toimesta, mutta monissa aiheissa on syytä lähteä toteuttamaan yhteistä koulutusta ja hakea sitä tekemään aiheen parhaat asiantuntijat. Tässä voisikin selvityksen perusteella nähdä erikoistumisen paikan – eli kuten Digipooli digitaalisessa turvallisuudessa voisi esim. yksityisen turva-alan pooli vastata koulutussisällöistä, jotka liittyvät alan toimijoiden liiketoiminnan ytimeen – esim. Kiinteistö- ja toimitilaturvallisuus, Henkilöturvallisuus jne.

5.3 Jatkotoimet - (sis. Tulosten esittely ja hyödyntäminen)

Tämä raportti julkaistaan kokonaan tai osittain Huoltovarmuusorganisaation Extranetissä ja sen sisällöstä tehtyjä aihenostoja julkaistaan Digipolin viestinnässä - verkkosivuilla sekä sosiaalisen median kanavissa. Sisältöä tarjotaan myös Teknologiateollisuus ry:n viestintään ja tapahtumiin sekä huoltovarmuuskeskuksen viestintäkanaviin. Näillä toimenpiteillä saavutetaan laaja elinkeinoelämä.

Raportin nostamia aiheita käsitellään Digipoolin toiminnassa eli raportti tullaan käsittelemään ryhmissä ja jaoksissa. Erityisesti Johtoryhmässä ja ICT ryhmässä. Jälkimmäisen ollessa alan yritysten edustaja ja sikäli paras ryhmä ideoimaan havaintojen perusteella kehitystoimia alan yritysten kypsyyden kohottamiseksi. Johtoryhmän on syytä huomioida raportin sisältö, kun Digipoolin tavoitteita ja strategiaa uudistetaan vuoden 2024 aikana.

Käsittelyn tavoitteena on johtaa havaintoihin liittyviä toimenpide-ehdotuksia, joiden avulla alan yritysten kypsyys saadaan nousuun. Pyrkimyksenä on toistaa vastaava kysely ja haastattelut esim. kahden vuoden välein, jolloin saadaan myös tietoa kypsyyden kehityksestä yrityksissä.

Tuloksia käsitellään myös Digipoolin työvaliokunnassa ja työvaliokunta voi suoraan ottaa myös kantaa muihin kohdan 5.1 ehdotuksiin. Esimerkiksi työvaliokunta voi päättää vuoden 2024 Työpajapäivien teemoista ja selvityksen prioriteettilistan kärkipäässä olevat teemat ovat hyvin potentiaalisia aiheita niissä käsiteltäväksi ja toimenpiteitä tehtäväksi. Tämän lisäksi työvaliokunta voi määrittää vuoden 2024 vuosiseminaarin aiheet, jotka samoin voivat olla selvityksen esiin nostamia. Raportin alleviivaamat aiheet ovat potentiaalisia aiheita Digipoolin seminaareissa ja tapahtumissa käsiteltäväksi.

Digipoolin toimisto osallistuu Huoltovarmuuskeskuksen johdolla koulutuskokonaisuuden uudistuksiin ja edustaa työssä selvityksen esiin nostamia tarpeita, jotta niitä voidaan koulutusohjelmissa lähteä toteuttamaan. Digipooli myös keskittyy kehittämään digitaalisen turvallisuuden koulutuskokonaisuutta tähän visioon nojaten.

6 Yhteenveto

Tutkimus Huoltovarmuusorganisaation Digipoolin yritysten kokonaisturvallisuudenhallinnan tilasta onnistui varsin hyvin tuottaen tietoa yritysten tilaan liittyen. Tutkimus koosti perusteita kokonaisturvallisuudenhallinnan tilan kehittämiselle, se koosti alan yrityksille relevantin riskiluettelon toiminnassa huomioitavaksi sekä se tuotti tietoa niistä aiheista, joihin alan yrityksissä tulisi kiinnittää huomiota kypsyysarvion ja riskipeilauksen myötä.

Tutkimus luo hyvän pohjan ohjata huoltovarmuusorganisaation Digipoolin toimintaa tukemaan yrityksiä varautumisen kehityksessä erityisesti tutkimuksen korostamissa turvallisuuden osa-alueissa. Lisäksi tutkimus tarjoaa osa-alueisiin liittyen tarkempaa tietoa aiheista, jotka kaipaavat kehitystä.

Tutkimukseen eivät osallistuneet kaikki Digipooliin kuuluvat yritykset (yli 110 yritystä), mutta siihen osallistui kymmeniä yrityksiä muodostaen merkittävän otoksen poolin yrityksistä. Haastatteluilla varmistettiin, että otoksessa oli mukana keskimääräisten digipoolin yritysten lisäksi myös suurimmat ja laajimmin huoltovarmuusorganisaatiossa vaikuttavat yritykset ja siten tulosten voi väittää olevan alan yritysten tilaa edustavia havaintoja.

Turvallisuudenhallinnan tila Huoltovarmuusorganisaation Digipoolin yrityksissä eli ICT alan yrityksissä vaikuttaisi olevan hyvällä tasolla. Kaikki turvallisuudenhallinnan osa-alueet on huomioitu yritysten toiminnassa, mutta hyvin erilaisin painotuksin yritysten liiketoiminnan erojen takia. Kysely ja haastattelut paljastivat eroja käsityksessä hyvästä ja riittävästä turvallisuuden tasosta. Ja vaikka yritysten itsensä tekemät kypsyysarviot olivat asteikon kypsemmässä päässä, on useissa osa-alueissa kuitenkin kehitettävää.

Tutkimus koosti perusteita kokonaisturvallisuudenhallinnan tilan kehittämiselle useista lähteistä. Perusteita koostettiin Huoltovarmuuskeskuksen ohjauksesta, joka perustuu laajaan analyysityöhön, jota keskus tekee elinkeinoelämän toimintojen varmistamisen tueksi sekä EU:n lisääntyvä regulaatio (erityisesti NIS2 ja CER direktiivit) ja niistä poikiva kotimainen lainsäädäntö.

Työ koosti uhka- ja riskiluettelon, joka useammankin lähteen mukaan on alan yrityksille huomioitavaa sisältöä varautumista kehitettäessä. Koosteen perusteella ICT alalle oleellisia - toiminnassa huomioitavia - uhkia ja riskejä ovat:

- Rikollisuus, Tiedustelu, Vaikuttaminen, Pandemia, Talous, Häiriöt, Luonnonilmiöt, Sota, Asiakas, Palvelu, Teknologia, Tuotanto, Alihankinta, Kehitys, Henkilöstö

Ennen kaikkea työ tuotti tietoa tutkimuskysymyksensä aiheesta eli ICT alan kokonaisturvallisuudenhallinnan osa-alueiden kypsyydestä ja asetti osa-alueet riskipeilauksen kautta tärkeysjärjestykseen. Riskipeilauksen myötä ICT alan yrityksille suositeltu prioriteettijärjestys turvallisuudenhallinnan osa-alueiden kehitystoimenpiteille on:

1. Varautuminen ja kriisinhallinta
2. Tuotannon ja toiminnan turvallisuus
3. Henkilöturvallisuus
4. Väärinkäytösten ja poikkeamien hallinta
5. Tietoturvallisuus
6. Ympäristöturvallisuus

7. Kiinteistö- ja toimitilaturvallisuus
8. Pelastusturvallisuus
9. Työturvallisuus (työterveyshuolto ja työsuojelu)

Lisäksi työ tarjosi kaikkiin osa-alueisiin liittyen tietoa aiheista, joissa tehtävillä toimenpiteillä todennäköisesti voitaisiin osa-alueen kypsyyttä kehittää. Esimerkiksi tärkeimmäksi kehitettäväksi osa-alueeksi tunnistetun Varautuminen ja kriisinhallinta osa-alueen suosituksena kehotetaan pyrkimyksiin nostaa aiheen prioriteettia yrityksen agendalla ja tutkimaan mahdollisuutta yhdistää perinteisen turvallisuudenhallinnan ja ict turvallisuuden aiheiden hallinta samoihin prosesseihin organisaatiossa varautumisen ja tilannetietoisuuden tehostamiseksi.

Työn myötä saatiin muitakin havaintoja alan turvallisuudenhallintaan liittyen ja niiden osalta tulee käydä keskustelua ja arvioida havainnon merkitystä ja sitä tuleeko asiaa pyrkiä jotenkin muuttamaan. Sellaisia havaintoja ovat:

- Turvallisuudenhallinnan organisoitumisen merkitys kokonaisturvallisuuden hallinnalle, kun vaikuttaa siltä, että tilannetta ymmärretään paremmin kokonaisuutena organisaatioissa, missä myös lakisääteisiä turvallisuudenhallinnan osa-alueita (kuten väärinkäytökset, vakuuttaminen, paloturvallisuus) johdetaan yhdessä tietoturvallisuuden kanssa.
- Regulaation ja kotimaisen lainsäädännön vaikutus yrityksissä on kiistaton, mutta vaikuttaa johtavan siihen, ettei aiheita nosteta strategisiksi tavoitteiksi ja siten niitä toteutetaan lainsäädännön minimitasolla. Jotta aihetta erityisesti kehitetään, tulisi se nostaa strategian aiheeksi, asettaa yrityksen arvoksi tai laajentaa käsitystä vastuullisuudesta (, joka myös vaikuttaa vaihtelevan laajasti).
- Turvallisuudenhallinnan malleista alalla korostui ylivoimaisesti ISO27001, joka oli sertifioitu 69% osallistuneista yrityksistä. Monet muilla aloilla tyypilliset mallit, kuten Riskienhallintajärjestelmä ISO31000, eivät olleet yritysten ohjelmassa. Riskienhallintajärjestelmän kehittämistä alan yrityksissä voidaankin pitää huoltovarmuuden kannalta arvokkaana tavoitteena.
- NIS2- ja CER-direktiivit ja niiden myötä luotava kotimainen lainsäädäntö tunnistetaan edellyttävän aktiivista riskienhallintaa ja vaativan erillistä resursointia, jota ei vielä ole yrityksissä tehty velvoitteiden ollessa toistaiseksi epäselviä. Riskienhallinnan merkitys alan yrityksissä on kenties tunnistettu, mutta sitä ei osoiteta sertifioinnein ja tämä voi nousta tärkeydessä ja vaatia tukea toteutuakseen alan yrityksissä. Ylipäänsä vaikuttaa olevan todennäköistä, että sertifikaattien merkitys korostuu jatkossa.

Digipoolin toiminnassa tulee huomioida selvityksen priorisoimat aiheet, kuten varautumisen ja kriisinhallinta sekä tuotannon turvallisuus. Priorisoitujen aiheiden käsittely toiminnassa on oleellista tuettaessa yrityksiä kiinnittämään huomiota oleellisimpiin turvallisuudenhallinnan osa-alueisiin. Näihin liittyvät sisällöt tulee näkyä toiminnassa, tuotetuissa materiaaleissa, seminaareissa ja koulutuksissa.

Koulutuksia tulee tuottaa yhdessä huoltovarmuuskeskuksen ja muun huoltovarmuusorganisaation kanssa. Digipoolin yrityksille oleellinen koulutussisältö muodostuu huoltovarmuuskeskuksen tuottamista kaikille yhteisistä koulutuksista, mutta myös huoltovarmuusorganisaatiossa osa-alueisiin keskittyviin asiantuntevimpien toimijoiden tuottamiin koulutuksiin. Digipoolille looginen osa-alue on tietoturvallisuus ja siinä koulutuksen tuottaminen huoltovarmuusorganisaatiolle.

Tämän työn tulokset julkaistaan Huoltovarmuusorganisaatiolle ja erityisesti Digipooli yrityksille. Raportti ja niissä esitetyt havainnot käsitellään Digipoolin työryhmissä ja pyritään yritysten kanssa suunnittelemaan toimenpiteitä, joilla tuetaan yritysten pyrkimyksiä kehittää osa-alueita edelleen.

Lähdeviitteet ja kirjallisuusluettelo

[1] Yhteiskunnan turvallisuusstrategia, Turvallisuuskomitea, 2017

[2] Suomen kyberturvallisuusstrategia 2019, Turvallisuuskomitea, 2019

[3] Kansallinen riskiarvio 2023, Sisäministeriö, 2023

[4] Kansallisen turvallisuuden katsaus 2023, Suojelupoliisi, 2023

[5] Yritysturvallisuusmalli, Elinkeinoelämän keskusliitto, 1987, päivitetty 2020

[6] Valtioneuvoston päätös huoltovarmuuden tavoitteista, Valtioneuvosto, 2018

[7] Huoltovarmuusselonteko 2022, Valtioneuvosto, 2022

[8] Huoltovarmuuskeskuksen strategia 2021

[9] Huoltovarmuuskeskuksen strategia yhteenveto

[10] Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri)

[11] Katakri-tietoturvallisuuden-auditointityokalu-viranomaisille

[12] Digipoolin toimialojen kyberkypsyyden selvitys 2022 – Kansallinen koosteraportti

[13] NIS2 Luonnos hallituksen esitykseksi laista kyberturvallisuuden hallinnalle

[14] World Security Report 2023, Allied Universal, 2023

7 Liitteet

Verkkoversiossa ei ole liitteitä mukana – ne ovat saatavilla pyydettäessä.

[1] Liite 1 Digipoolin kokonaisturvallisuuden hallinnan selvitys - kyselyn kysymykset webropo-lista.pdf

[2] Liite 2 Kyselyn saate sähköposti.pdf

[3] Liite 3 Digipoolin kokonaisturvallisuudenhallinnan selvitys 2023 – Webropol vastaukset raaka.pdf

[4] Liite 4 HaastatteluidenTuloksetPseudo.xlsx

[5] Liite 5 Digipoolin kokonaisturvallisuuden hallinnan selvitys_haastattelupohja.pdf

[6] Liite 6 Digipoolin yritysten yritysturvallisuuden osa-alueiden tavoitetila.docx