

Turvallisuudenhallinnan painopisteet

Huoltovarmuusorganisaation Digipoolin yrityksissä

Turvallisuusjohdon koulutusohjelma

Lopputyöraportti

Antti Nyqvist

Huoltovarmuusorganisaation Digipooli, Teknologiateollisuus ry

Espoo 3.12.2023

Aalto University Executive Education and Professional Development

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 Supply 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
1.1	Työn tausta.....	1
1.2	Työn tavoitteet eli tutkimusongelma	2
1.3	Tutkimusmenetelmä.....	2
1.4	Tavoitteiden painotus.....	3
1.5	Tutkimuksen rajaukset	3
1.6	Tutkimuksen aineisto	4
1.7	Terminologia.....	4
2	Tausta ja viitekehys.....	6
2.1	Huoltovarmuuskeskus ja kytkös yritysturvallisuuteen	6
2.1.1	Huoltovarmuuskeskuksen strategia	6
2.1.2	Huoltovarmuusorganisaation tehtävä.....	7
2.1.3	Digipooli ja Digipoolin tehtävä	8
2.2	Riskejä ja uhkia huomioitavaksi	9
2.2.1	Yhteiskunnan turvallisuusstrategia	9
2.2.2	Kyberturvallisuusstrategia	11
2.2.3	Kansallinen riskiarvio	12
2.2.4	Kansallisen turvallisuuden katsaus	13
2.2.5	Valtioneuvoston päätös huoltovarmuuden tavoitteista	13
2.2.6	Valtioneuvoston huoltovarmuusselonteko.....	14
2.2.7	Kansainvälisesti tunnistettuja uhkia.....	14
2.2.8	Muita lähteitä ICT-alalle relevanttien uhkien tunnistamisessa 15	
2.2.9	Yhteenveto uhista ja riskeistä ICT-alan varautumisen näkökulmasta	16
2.3	Turvallisuusjohtamisen malleista.....	17
2.3.1	EK Yritysturvallisuuden malli	17
2.3.2	ISO Standardit.....	19
2.3.3	ISO27001 ja EK Yritysturvallisuusmallin vertailua	20
2.3.4	Muita turvallisuudenhallinnan standardeja	22
2.4	EU direktiivit ja regulaation vaikutuksia yritysten kokonaisturvallisuuden hallintaan	22
2.5	Turvallisuudenhallinnan painotuksista tehtyjä selvityksiä?.....	25
3	Tutkimuksen toteutuksesta.....	26
3.1	Välineet	26
3.2	Kyselytutkimus	27
3.3	Haastattelut	28

3.4	Tulokset ja tuotokset	29
4	Selvitystyön havainnot	30
4.1	ICT-yrityksissä sovelletut standardit.....	31
4.2	Yritysturvallisuusmallin osa-alueiden kypsyys yrityksissä.....	33
4.2.1	Henkilöturvallisuus	34
4.2.2	Kiinteistö- ja toimitilaturvallisuus.....	35
4.2.3	Pelastusturvallisuus	36
4.2.4	Tuotannon ja toiminnan turvallisuus.....	37
4.2.5	Ympäristöturvallisuus	38
4.2.6	Tietoturvallisuus.....	40
4.2.7	Väärinkäytösten ja poikkeamien hallinta	41
4.2.8	Varautuminen ja kriisinhallinta.....	43
4.2.9	Työturvallisuus (työterveyshuolto ja työsuojelu).....	44
4.3	Turvallisuudenhallinnan organisoituminen.....	45
4.4	Strategia.....	47
4.5	NIS2- ja CER-direktiiveistä	49
4.6	Riskipeilaus	50
4.7	Selvityksen havainnot osa-alueittain	52
5	Digipoolin toiminnan kehitys.....	56
5.1	Digipoolin toiminta ja sisältöaiheet.....	56
5.2	Toimenpide-ehdotuksia Huoltovarmuuskeskukselle poolien ohjaukseen.....	59
5.3	Jatkotoimet - (sis. Tulosten esittely ja hyödyntäminen).....	60
6	Yhteenveto	61
7	Lähdeviitteet ja kirjallisuusluettelo	65
8	Liitteet	66

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 eli tutkimusongelma

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 kehitysaideiden suosittelu ja tulosten käsittely Digipoolin työryhmissä. Käsittelyn avulla pyritään (tähän työhön kuulumattomasti) löytämään toimenpiteitä, joiden avulla yritykset lähtisivät kehittämään toimintaansa työn esittämässä 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 haastattelulla. Kysely toimi EK yritysturvallisuusmallin¹ 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 tavoitteista 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

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

voitiin painottaa kokonaisturvallisuuden aiheita yhdessä kypsyystiedon kanssa.

Lopulta turvallisuuden osa-alueiden kypsyys suhteutettiin tunnettuihin riski-aiheisiin. Riskien oleellisuus alan yrityksille arvioitiin ja annettiin sille suhdeluku, jolla painotettiin osa-alueiden suhteellista kysyyttä. Näin saatiin riskien ja kypsyiden 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 selvittävä 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?
- Mitä aiheita käsitellään vastuullisuus otsikon alla?
- Yritysten valmius NIS2 ja CER direktiiveistä poikiviin vaatimuksiin?

1.5 Tutkimuksen rajaukset

Kysely ja haastattelut rajataan 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 rajataan 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	Ohjalleivassa tehtävässä käytetty lausuma. Direktiivisellä lausumalla puhuja käsklee, 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 materiaalistien 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 mission² (”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 strategia³ on vuosille 2021-2023 ja se määrittelee mm. johdannossa mainitun

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

³ Lähde [8] Huoltovarmuuskeskuksen strategia

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 tehtäviä⁴ ja samalla sille varataan mahdollisuus nostaa esiin elinkeinoelämän tarpeista nousevia toimenpide-ehdotuksia, joilla varmistetaan toimintaa tai muuten parannetaan huoltovarmuutta.

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

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.

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 tehtäviä⁵. 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

⁵ <https://www.huoltovarmuuskeskus.fi/huoltovarmuusorganisaatio/sektorit-ja-poolit>

- 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 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 2017⁶ 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 kerran vuonna 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

⁶ Lähde [1] Yhteiskunnan turvallisuusstrategia, 2017

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	<ul style="list-style-type: none"> • Valtion ylimmän johdon toimintaedellytysten turvaaminen • Valtion ylimmän johdon tilannekuvan ylläpitäminen • Viestinnän toimivuus
Kansainvälinen ja EU-toiminta	<ul style="list-style-type: none"> • Suomen toiminta Euroopan unionissa; EU-asioiden kansallisen valmistelun ja käsittelyn, yhteisvastuun sekä keskinäisen 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 suojeleminen ja avustaminen ulkomailla • Suomen ulkomaankaupan sujuvuuden ja häiriöttömyyden varmistaminen
Puolustuskyky	<ul style="list-style-type: none"> • Suomen sotilaallinen puolustaminen
Sisäinen turvallisuus	<ul style="list-style-type: none"> • Oikeusturvajärjestelmän toimintakyvyn turvaaminen • Vaalien toimeenpano ja demokratian edellytysten turvaaminen • Yleisen järjestyksen ja turvallisuuden ylläpitäminen • Rajaturvallisuuden varmistaminen • Toimitusketjujen turvallisuuden ja tavaturvallisuuden varmistaminen • Väestön suojaaminen • Meripelastustoimen suorituskyvyn varmistaminen • Hätäkeskustoiminta • Pelastustoimen ylläpito • Laajamittaisen maahanmuuton hallinta • Ympäristövahinkojen torjunta ja ennaltaehkäisy • Biologisiin uhkiin varautuminen • Säteiluvaaratilanteiden estäminen ja niihin varautuminen • Kemikaaliuhkiin varautuminen
Talous, infrastruktuuri ja huoltovarmuus	<ul style="list-style-type: none"> • 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

	<ul style="list-style-type: none"> • 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 • Päivittäistavara- ja huollon turvaaminen
Väestön toimintakyky ja palvelut	<ul style="list-style-type: none"> • Väestön viimesijaisen toimeentulon turvaaminen • Sosiaali- ja terveydenhuollon palvelujen turvaaminen • Osaamisen ylläpitäminen
Henkinen kriisinkestävyys	<ul style="list-style-type: none"> • Kulttuuripalvelujen ylläpitäminen ja kulttuuriomaisuuden suojeleminen • 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 2019⁷ 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:

⁷ Lähde [2] Suomen kyberturvallisuusstrategia, 2019

- 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 ennakoita 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 1).

Jos tarkastellaan viimeisimmässä kansallisessa riskiarviossa⁸ 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 3 Kansallisen riskiarvion perusteella yrityksiä 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
Polttoaineiden saannin vakavat häiriöt	2
Mikrobilääkeresistenssi	2
Äärimmäisen voimakas avaruusmyrsky	2

⁸ Lähde [3] Kansallinen riskiarvio 2023, Sisäministeriö, 2023

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 2023⁹ 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 2018¹⁰ 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

⁹ Lähde [4] Kansallisen turvallisuuden katsaus 2023, Suojelupoliisi, 2023

¹⁰ Lähde [6] Valtioneuvoston päätös huoltovarmuuden tavoitteista, Valtioneuvosto, 2018

2.2.6 Valtioneuvoston huoltovarmuusselonteko

Valtioneuvoston huoltovarmuusselonteko vuodelta 2022¹¹ käsittelee pitkälti samoja uhkia tai varautumista vaativia aiheita kuin vuoden 2018 päätös huoltovarmuuden tavoitteista. Huoltovarmuusselonteko korostaa verkostoituneen toiminnan kehittymistä ja toimitusketjujen toiminnan näkökulmia.

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 yrityksiä kohtaa- mista 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 4 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

¹¹ Lähde [7] Huoltovarmuusselonteko 2022, Valtioneuvosto, 2022

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

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

2.2.8 Muita lähteitä ICT-alalle relevanttien uhkien tunnistamisessa

Huoltovarmuusorganisaation Digipooli on toteuttanut kyberkypsyyden selvityksiä¹³, 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 epäsuhtaanne.
- Teknologia Vanhentunut, toimimaton ja/tai kehityskelvoton teknologia; koodin tekijänoikeudet ja lisenssiehdot. Haavoittuvuudet
- Tuotanto Infran, IT & OT ympäristön, verkon, konesalien, päätelaitteiden toimimattomuus. Kyberhyökkäykset.
- Alihankinta Toimittajien virheet ja muutoshäiriö. Kumppanin kyberhäiriö.
- Kehitys Vaatimuksien määrittelyn, suunnittelun ja koodaamisen 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

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

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 kypsyysissä 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 5 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	Asiakkailla aiheutetut menetykset ja vahingot sekä asiakaskato.
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 sähkösaannissa.
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 toimintaturvallisuuden 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 liiketoiminnalle. Esim. Kauppapakotteiden kiertäminen häivyttämällä hankintaketjuista tiedon todellisesta ostajasta sekä hankkimalla tuotteita kolmansien maiden kautta. Digitaalisen rahansiirron käyttö ja virtuaalivaluuttojen yleistyminen vaikuttavat epävirallisen pankki- ja rahan siirtopalvelusektorin 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 viitekehyyksiin ja pohditaan niiden suhdetta huoltovarmuuteen. Kappaleessa myös pyritään pohtimaan sitä, mitkä viitekehyykset 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 malli¹⁴ 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 oleellimmat turvallisuudenhallinnan osa-alueet. EK:n yritysturvallisuusmallia ei varsinaisesti käytetä esim. yritysten turvallisuusjohtamisen arvioinneissa, mutta se mahdollistaa oman toiminnan vertaamisen mallin esittämiin toimintoihin ja on sikäli hyvä aloitustason viitekehys. Turvallisuusjohtamistaan kehittäville yrityksille voikin olla suositeltavaa siirtyä pian käyttämään aihealueen muita standardeja, joita löytyy useita.

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

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 6 Varautuminen ja kriisinhallinta EK:n mallissa

Varautuminen ja kriisinhallinta	
1) Jatkuvuussuunnittelu	
<ul style="list-style-type: none"> • Liiketoimintariskien arviointi ja vaihtoehtosuunnittelu • Tuotannon keskeytyminen tai pysähtyminen • Suunnittelu ja sietokyvyn kehittäminen 	<ul style="list-style-type: none"> • Kannattavuus • Sopimukset
2) Kriisinhallinta	
<ul style="list-style-type: none"> • Ennaltaehkäisy ja arviointi • Toiminta kriisitilanteessa • Toipumissuunnitelmat • Oppiminen 	<ul style="list-style-type: none"> • Varautuminen • Akuutit kriisit • Kehittyvät kriisit • Nopea ja oikea vaste • Viestintä
3) Valmiussuunnittelu (poikkeusoloihin varautuminen)	
<ul style="list-style-type: none"> • Velvoitteiden tunnistaminen • Tuotannon ja toiminnan suunnittelu 	<ul style="list-style-type: none"> • 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 7 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 voidaan kuitenkin todeta, että ICT yrityksissä monet EK:n mallin aiheet ovat lakisäätteisinä toteutettu hyvin ja sikäli ei ole kenties nähty oleelliseksi niihin keskittyä tai niitä eivät asiakkaat ole tämän takia myöskään vaatineet. Lakisäätteiset toiminnot yhdessä ISO27001 sertifiointin 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. Lakisäätteisten velvollisuuksien kanssa yhdessä sillä saadaan katettua aiheita, mutta voitaneen arvioida, että riskitarkastelun kautta se jättää moniin aihealueisiin kehittämisen varaa.

Taulukko 8 Hallintakeino kategoriat ja osa-alueet rinnakkain

ISO27001 Hallintakeinojen kategoriat	EK:n yritysturvallisuusmallin osa-alueet
	Tietoturvallisuus
Tietoturvapoliitikat	
Tietoturvallisuuden organisointi	
Tietoturvahäiriöiden hallinta	Väärinkäytösten ja poikkeamien hallinta
Pääsynhallinta	
Salaus	
Järjestelmien hankkiminen, kehittäminen ja ylläpito	
Suhteet toimittajiin	
Vaativuuden mukaisuus	
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 CSF¹⁵ yhtäaikaan. 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).

Yrityksen toiminnan standardoimisen sijasta onkin tarjolla henkilötason standardeja. Sertifiointia turvallisuudenhallinnan aiheissa tarjoavatkin monet toimijat, joista hyvänä esimerkkinä on ASIS International¹⁶. 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 yri-

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

¹⁶ <https://www.asisonline.org/>

¹⁷ <https://www.thebci.org/>

tyksiä 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
- Ydinenergi laki
- Ilmailulaki
- Terveysturvallisuuslaki 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

ICT-alalle relevantti lainsäädäntö on myös Laki sähköisen viestinnän palveluista¹⁸. 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

¹⁸ [Laki sähköisen viestinnän palveluista 917/2014 - Ajantasainen lainsäädäntö - FINLEX®](#)

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 kyberturvallisuudesta (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. hybridi-vaikuttamisen 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 ehdotus¹⁹) 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 eivät

¹⁹ [Lähde \[13\] NIS2 Luonnos hallituksen esitykseksi laista kyberturvallisuuden hallinnalle](#)

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 viitekehysten avulla. Suositus on tehokkuusnäkökulmasta hyvä koskea koko yrityskehitystä 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 raportoidessa.

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 henkilölle, jotka osaisivat siihen parhaiten vastata. Kyselyn saatteena lähetetty sähköposti on tämän dokumentin liitteenä 2.

Kyselyyn vastasi lopulta 32 eri yrityksen edustajaa. Vastajien 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

Kyselytutkimuksen sisältöön, eli kysytyihin kysymyksiin voi tutustua kokonaisuudessaan tämän dokumentin liitteistä. Kyselytutkimuksen kysymykset löytyvät dokumentin liitteenä 1.

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 tarkistuskysymyksiä 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.

Haastatteluiden tuottama materiaali löytyy tämän dokumentin liitteestä 4.

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. Nämä tulokset löytyvät dokumentin liitteistä 3 ja 4.

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 turvallisuuden 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.

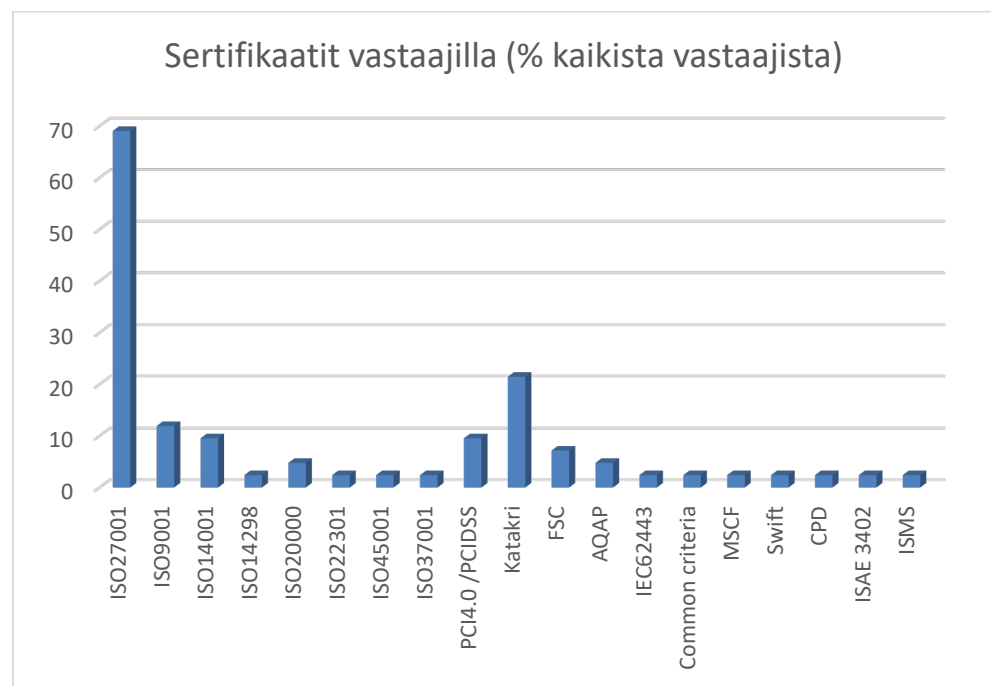
Vähemmän positiivisena havaintona voidaan todeta, että yritysten välillä käsitykset riittävästä tai hyvästä turvallisuuden hallinnan tasosta eri aiheissa vaihtelevat valtavasti ja sikäli vertailukelpoisten tulosten saaminen on lähes mahdoton tehtävä. Haastattelut alleviivasivat kypsyyden tulkinnan haastetta 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

kypsyystä ja tekemään päätelmiä alan yritysten tilanteesta ja havaintoja mahdollisista kehittävästä 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 2 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 sertifioitu, 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 katakri²¹ ja julkri²² ja muutamat ilmoittavat niiden myötä heidän toimintaansa myös auditoidun. Puolustusvoimien kanssa työtä tekevillä toimijoilla nousee esiin FSC (Facility 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

²¹ Lähde [11] Katakri-tietoturvallisuuden-auditointityökalu-viranomaisille

²² Lähde [10] Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri)

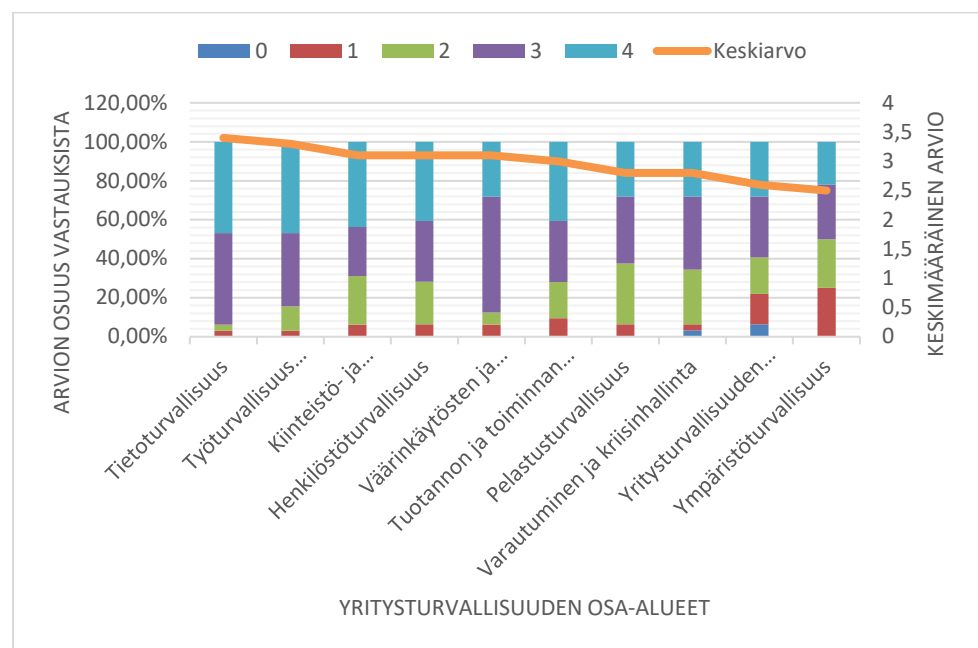
soveltamisesta. Malli on kansainvälisesti yleinen, mutta Suomessa hyvin harvinainen yritysten käytössä.

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. Vaatimukseen vastaaminen eli ”compliance” nousi esiin kommentteissa.

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.



Kuva 3 Kyselyn kypsyys arvioiden hajonta ja arvioiden keskiarvo

4.2.1 Henkilöturvallisuus

Henkilöturvallisuuden kypsyttä kyselyllä kysyttäessä asteikolla 0-4, saa aihe keskiarvoisesti arvioksi 3,1. 41% yrityksistä arvioi sen korkeimmalle kypseytasolle 4 (Prosesseja optimoidaan ja tapahtuu jatkuvaa parantamista), 31% tasolle 3 (Prosesseja myös mitataan ja hallitaan), 22% tasolle 2 (Prosesseja 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 aiheetta. 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 tunnistaneeet 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 hyötyivät yhteisten toimintatapojen ja käytäntöjen jakamisesta aiheesta.

4.2.2 Kiinteistö- ja toimitilaturvallisuus

Kiinteistö- ja toimitilaturvallisuus sai kyselyssä kypsyyсарvioita, joiden keskiarvo on 3,1. Aiheen on arvioinut korkeimmalle kypsyytasolle 43,80 % vastaajista ja samalla kypsyytasot 3 ja 2 ovat saaneet 25% arvioista ja 6% antaa arvon 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 aiheesta oli tunnistettu kehitettävää.

Tarpeen todettiin ohjaavan tässäkin aiheesta ja toimitiloissa on eri tasoisia turvallisuusratkaisuita käyttötarpeen mukaan. On mm. todettu, että toimistotilojen turvallisuus ja esim. konesalien turvallisuus on useimmiten hyvin erillaisella kypsyytasolla. Toisaalta toimistotilojen turvallisuuteen on kiinnitetty enemmän huomiota, kun työtä on tarve tehdä ns. turvataloista. Tarpeen määrittää useimmiten siis liiketoiminta ja asiakasvaatimukset – ja asiakkuustilillä 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 toteutukseksi.

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 vartiointin osalta käytännöt vaihtelevat ja osalla toimijoista on suoria sopimuksia vartiointiyriytysten 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 arviointiin 3 vaikuttaisi aiheen olevan kypsä, 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, jotka 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 oh-

jeistettu 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 kypsytyden tasossa yrityksissä. Aihe ei kuitenkaan ollut kovin keskeinen haastatteluiden tai kyselyn kohteille ja siitä kenties johtui hieman ristiriitainen arvio – aiheesta 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 painoutuivat 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 4.2) 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 kypsyiden 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. Tavot organisoitua vaihtelevat, mutta niistä on löydettävissä yhteisiä piirteitä. Alaluku 4.12 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 – ylätasoinen mainnosta 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 kypsyiden tasolle 3 ja 28,1% tasolle 4. Jakauma kuvastaa aiheeseen liittyvää pientä epävarmuutta – pitkälti lakisäätöinen 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 (ennaltaehkäisyyn 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 tietoturvalisuuteen 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 johtuu mm. pörssilainsäädännöstä ja sen toteutuksesta (hallinnan vastuut organisaatioissa) 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 kypsytön 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 kriisinhallinnassa (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 ratkaisuksista 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 merkitystä 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 voidaan todeta, että organisoituminen ja turvallisuusaiheiden vastuutus yrityksessä vaikuttaa siihen, kuinka hyvin kokonaisturvallisuuden tilannetta ymmärretään organisaatioissa ja kuinka turvallisuustieto välittyy johtoryhmänkin käsiteltäväksi. Vaikuttaisi siltä, että tilannetta ymmärretään paremmin kokonaisuutena organisaatioissa, missä myös lakisäätteisiä 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, käsittelee johtoryhmä turvallisuutta kokonaisuutena, vaihtelee ja vaikuttaisi mm. siltä, että monissa yrityksissä on turvallisuushavainvoja käsittelevä ryhmä erikseen ja johtoryhmä käsittelee lähinnä sinne eskaloituja havainvoja. 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 mieltä 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 kyberkypsyys selvityksen 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 kommunikoidessa 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 mieltä 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 4 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, Social, 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 kypsytyteen 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 tiukoja 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 kypsyytensä 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 kypsyyden 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 3.2.8 esiteltyjä alan liiketoimintaa uhkaavia riskiaihteita ja peilataan niitä EK:n yritysturvallisuusmallin osa-alueiden selvityksen osoittamaan kypsyyteen, voidaan arvioida sitä, missä prioriteettijärjestyksessä turvallisuusaihteita 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 9 Turvallisuuden osa-alueiden suhde riskiaiheisiin

KA		Rikollisuus	Tiedustelu	Vaikututtaminen	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	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	Kyllä	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	Ei	Ei	Ei	Kyllä	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 (työterveyshuolto ja työsuojelu)	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 kypsyyssarviolla ja näin on muodostettu riskipainotettu prioriteettijärjestys turvallisuuden osa-alueille ICT-alalla huomioitavaksi.

Taulukko 10 Riskipainotettu prioriteettijärjestys turvallisuuden osa-alueille ICT-alan yrittäjissä

Prio.	Suhdeluku	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 11 Turvallisuuden osa-alueet ja suositukset prioriteettijärjestyksessä

Prio.	Turvallisuuden osa-alue	
1.	Varautuminen ja kriisinhallinta	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Määrittele tuotannon ja toiminnan turvallisuuden kokonaisuus yrityksessäsi • Arvioi ohjelmistokehityksen turvallisuuden vaikutukset omalle yritykselle ja asiakkaille – vaikka yritys ei itse ohjelmistokehitystä tekiskään. 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 turvallisuuden 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	<ul style="list-style-type: none"> • 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 kannalta itse vastuu. • Keskity etätyön turvallisuuden haltuunottoon ja tarjoa henkilöstölle ratkaisuita siihen. Määrittele etätyönteon työnantajan vastuut, velvollisuudet ja valtuudet.
4.	Väärinkäytösten ja poikkeamien hallinta	<ul style="list-style-type: none"> • Kehitä väärinkäytösten ja poikkeamienhallinnan kokonaisuutta yrityksessä laajentamalla 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	<ul style="list-style-type: none"> • 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 maturiteettiä yli korkeimpien direktiivi tai asiakasvaatimusten, jotta se palvelee tehokkaasti asiakastoimituksissa ja täyttää ilman eri ponnistuksia lainsäädännön vaatimukset ja mahdollistaa ennakoitavan hinnoittelun.
6.	Ympäristöturvallisuus	<ul style="list-style-type: none"> • Toimi vastuullisesti ja huomioi ympäristöturvallisuus • Käänä 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 konealusten hiilidioksidipäästöjä

		<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Suunnittele turvallisuusratkaisut kiinteistön käyttötarpeen mukaan. • Nosta tilaturvallisuuden taso kattamaan useimmat asiakasvaatimukset sekä lainsäädännön vaatimukset ja toisaalta henkilöstön suojausten tarpeet. • Harkitse tilaturvallisuuden havaintojen hallintaa samoissa prosesseissa kuin muitakin turvallisuushavaintoja (esim. ict) tilannekuvan muodostamiseksi. • Vuokralla oltaessa varmista, että vuokranantajan vastuut ovat selvät. • Varmista oma ohjauskyvykyys 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	<ul style="list-style-type: none"> • Kiinnitä huomiota vuokrasopimukseen 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)	<ul style="list-style-type: none"> • 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 huoltovarmuskriittiset 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 kypsytyksen 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 kehittämistä niin, että se paremmin tukee yritysten kokonaisturvallisuudenhallinnan kehitystä. Kappale nostaa esiin mahdollisia toiminnassa huomioitavia aiheita, joiden edistämistä 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 rahan käytöstä 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, digitaalinen turvallisuus huoltovarmuusorganisaatiossa) sekä seminaarit (kuten vuosiseminaarit #DigiSignaali). Muita tapoja käsitellä eri aiheita ovat mm. Työpajapäivät, missä voidaan keskittyä käsittelemään tiettyjä aiheita ja tuottaa toimenpide-ehdotuksia tai saada sinällään jo muu-
tosta aikaiseksi.

Näin kuvattuna ei selvityksen perusteella tule suoraan vaikutuksia Digipoolin ryhmärakenteeseen tai dialogin muihin välineisiin. Enemminkin 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 ponnisteluja. 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 käsittelemässä 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 Digipoolin 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 kypsyiden 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 kypsyiden 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 kehittämiseksi, 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 kypsemässä päässä, on useissa osa-alueissa kuitenkin kehitettävää.

Tutkimus koosti perusteita kokonaisturvallisuudenhallinnan tilan kehittämiseksi useista lähteistä. Perusteita koostettiin Huoltovarmuuskeskuksen oh-

jauksesta, 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 kypsyystä 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 kehoitetaan pyrkimykseen 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 strategiseksi 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.

7 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

8 Liitteet

Liite 1 Digipoolin kokonaisturvallisuuden hallinnan selvitys - kyselyn kysymykset webropolista.pdf

Liite 2 Kyselyn saate sähköposti.pdf

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

Liite 4 HaastatteluidenTuloksetPseudo.pdf


Liite 5 Digipoolin kokonaisturvallisuuden hallinnan selvitys_haastattelu-pohja.pdf

Liite 6 Digipoolin yritysten yritysturvallisuuden osa-alueiden tavoite-tila.docx



Huoltovarmuusorganisaatio
Digipooli

Selvitys Digipoolin yritysten kokonaisturvallisuuden hallinnan tilasta

 Pakolliset kysymykset merkitty tähdellä (*)

Saate:

Arvon verkostomme yrityksen edustaja - olet vastaamassa kyselyyn, jonka avulla arvioidaan verkostomme yritysten kokonaisturvallisuudenhallinnan tilaa (kokonaisturvallisuuden ohjauksen ja hallinnan nykytila ja kehitystarpeet). Kysely tehdään EK:n yritysturvallisuusmallia* mukaillen.

Kyselyssä on 23 kysymystä ja siihen vastaamiseen on hyvä varata n.30 minuuttia. Kysely ei kysy vastaajan henkilöön tai yritykseen liittyviä tunnistetietoja. Vaikka yritykset ovat usein kansainvälisiä on tähän kyselyyn hyvä vastata lähinnä yrityksen Suomen toimintojen näkökulmasta. Rajaamalla kyselyn kohdetta helpotetaan siihen vastaamista ja tuotetaan kuitenkin huoltovarmuustoiminnalle relevanttia tietoa.

Toivomme kyselyyn vastauksia henkilöiltä, jotka vastaavat yrityksessänne kokonaisturvallisuudenhallinnasta tai osaavat muuten arvioida sen tilaa. Välitäthän kyselyn siis sellaiselle henkilölle, jos et itse koe sellainen olevasi.

Kyselyyn kannattaa osallistua, sillä pyrimme tuottamaan yrityksille tietoa kehitysaieista sekä löytämään aiheita, joissa kehitysponnisteluita voitaisiin tukea huoltovarmuusorganisaation toimesta kokonaisturvallisuudenhallinnan tason nostamiseksi.

Kerätyllä tiedolla on myös kansallista merkitystä, sillä (HVK:n hallituksen 2023 linjausten mukaisesti) se vaikuttaa suunnittelutyöhön, jolla laaditaan alan toimintoja koskevat yleissuunnitelmat poikkeusolojen sekä niihin verrattavissa olevien vakavien häiriöiden varalle. Lisäksi sillä vaikutetaan Digipoolin toimintaan, jota ohjataan kyselyn painottamiin aiheisiin yritysten sparraamiseksi. Samalla myös arvioidaan valmiutta EU Direktiivien (NIS2, CER) ohjaaman kotimaisen lainsäädännön mahdollisille velvoitteille.

Kyselyn tuottamasta tiedosta tehdään analyysi ja tuotetaan raportti. Valmistuessaan raportti julkaistaan Digipoolin tapahtumassa ja sen sisällöstä viestitään julkisesti. Raporttia jaetaan ensisijaisesti siihen vastanneille ja muille HVO Digipoolin verkoston yrityksille. Tulosten kautta on mahdollista saada vertailutietoa yritysten tilasta. Raportti pyrkii esittämään koottuja suosituksia tavoitetasoksi tai kehitysaieiksi alalle.

*<https://ek.fi/hyotytietao-yrityksille/yritysturvallisuus/>

1. Aloita antamalla tähän pseudonyymi, jonka avulla tunnistat vastauksesi mahdollisesta raportista. (tunniste - kirjainsarja tai keksitty nimi) *


Pseudonyymi *

Seuraava



Huoltovarmuusorganisaatio
Digipooli

Selvitys Digipoolin yritysten kokonaisturvallisuuden hallinnan
tilasta

 Pakolliset kysymykset merkitty tähdellä (*)

2. Jäsentääkö yrityksenne kokonaisturvallisuutta jonkin mallin tai standardin mukaan (esim. ISO standardit)? *

- Ei
 Kyllä

3. Erittele ne standardit (esim. ISO 27001), joita sovellette toiminnassanne *

ISO27001

4. Onko yrityksenne sertifioitunut jonkin turvallisuudenhallinnan standardin osalta? *

- Kyllä
 Ei

5. Minkä turvallisuudenhallinnan standardin osalta olette sertifioituneet *

ISO27001

6. Mikä/mitkä seuraavista motivoivat ensisijaisesti yrityksen sertifioitumaan *

- Kaupallinen etu
 Oman kehityksen tukeminen
 Asiakasvaatimus
 Muu - mikä?

7. Sovellatteko EK:n yritysturvallisuusmallia (<https://ek.fi/hyotyietoayrityksille/yritysturvallisuus/>) *

- Kyllä
 Ei

Edellinen

Seuraava



Huoltovarmuusorganisaatio Digipooli

Selvitys Digipoolin yritysten kokonaisturvallisuuden hallinnan tilasta

Pakolliset kysymykset merkitty tähdeillä (*)

8. Arvioi yrityksesi (EK:n yritysturvallisuusmalli) turvallisuudenhallinnan kypsyyttä aiheittain asteikolla 1-4.

Arvio 0 = Prosesseja on hallitsemattomasti projekteissa tai muussa toiminnassa

Arvio 1 = Prosesseja ja perusohjausta on osassa organisaatiota

Arvio 2 = Prosessit on laadittu sekä käytössä koko organisaation tasolla

Arvio 3 = Prosesseja myös mitataan ja hallitaan

Arvio 4 = Prosesseja optimoidaan ja tapahtuu jatkuvaa parantamista *

	0	1	2	3	4
Henkilöstöturvallisuus *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Kiinteistö- ja toimitilaturvallisuus *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Pelastusturvallisuus *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tuotannon ja toiminnan turvallisuus *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ympäristöturvallisuus *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tietoturvallisuus *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Väärinkäytösten ja poikkeamien hallinta *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Varautuminen ja kriisinhallinta *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Työturvallisuus (työterveyshuolto ja työsuojelu) *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Yritysturvallisuuden standardien hyödyntäminen *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

9. Kuinka EK:n mallin aiheet painottuvat toiminnassanne? (järjestä aiheet painotuksen mukaiseen järjestykseen - huomioi painotuksessa se mihin aiheisiin käytetään eniten rahaa/resursseja/aikaa) *

Henkilöstöturvallisuus	Valitse -
Kiinteistö- ja toimitilaturvallisuus	Valitse -
Pelastusturvallisuus	Valitse -
Tuotannon ja toiminnan turvallisuus	Valitse -
Ympäristöturvallisuus	Valitse -
Tietoturvallisuus	Valitse -
Väärinkäytösten ja poikkeamien hallinta	Valitse -
Varautumisen ja kriisinhallinta	Valitse -
Työturvallisuus (työterveyshuolto ja työsuojelu)	Valitse -
Yritysturvallisuuden standardit	Valitse -

10. Minkä aiheen koet tarvitsevan kehitystä/panostuksia ja miksi? *


Edellinen

Seuraava



Huoltovarmuusorganisaatio
Digipooli

Selvitys Digipoolin yritysten kokonaisturvallisuuden hallinnan
tilasta

 Pakolliset kysymykset merkitty tähdellä (*)

11. Kuinka kokonaisturvallisuuden vastuut ovat organisoitu tai ohjattu yrityksessänne? (keskitetty vs. hajautettu tai hybridi - Avaa ketjua hallituksen ja johtoryhmän vastuista alkaen muutamalla lauseella.) *

12. Kuinka turvallisuuden tila (tilannekuva) kokonaisuutena kootaan? *

13. Onko turvallisuudelle asetettu/sovittu tavoitteet ja mitataanko niitä? *

- Kyllä, täsmennä
- Ei

14. Mitkä ovat johdolle tehtävän turvallisuuden tilan raportoinnin painopisteet? *

15. Mitä kokonaisturvallisuuden aiheita näkyy yrityksen voimassaolevassa Strategianssa ja miten (Valitse 1 tai useampi aihe)? *

- | | |
|---|----------------------|
| <input type="checkbox"/> Henkilöstöturvallisuus | <input type="text"/> |
| <input type="checkbox"/> Kiinteistö- ja toimintaturvallisuus | <input type="text"/> |
| <input type="checkbox"/> Pelastusturvallisuus | <input type="text"/> |
| <input type="checkbox"/> Tuotannon ja toiminnan turvallisuus | <input type="text"/> |
| <input type="checkbox"/> Ympäristöturvallisuus | <input type="text"/> |
| <input type="checkbox"/> Tietoturvallisuus | <input type="text"/> |
| <input type="checkbox"/> Väärinkäytösten ja poikkeamien hallinta | <input type="text"/> |
| <input type="checkbox"/> Varautumisen ja kriisinhallinta | <input type="text"/> |
| <input type="checkbox"/> Työturvallisuus (työterveyshuolto ja työsuojelu) | <input type="text"/> |
| <input type="checkbox"/> Yritysturvallisuuden standardit | <input type="text"/> |

16. Käsitelläänkö yrityksessä vastuullisuutta? *

- Kyllä
- Ei

Edellinen

Seuraava

16. Käsitelläänkö yrityksessä vastuullisuutta? *

- Kyllä
 Ei

17. Mitä kokonaisturvallisuuden aiheita yrityksessä käsitellään vastuullisuus otsikon alla? *

- Henkilöstöturvallisuus
 Kiinteistö- ja toimitilaturvallisuus
 Pelastusturvallisuus
 Tuotannon ja toiminnan turvallisuus
 Ympäristöturvallisuus
 Tietoturvallisuus
 Väärinkäytösten ja poikkeamien hallinta
 Varautumisen ja kriisinhallinta
 Työturvallisuus (työterveyshuolto ja työsuojelu)
 Yritysturvallisuuden standardit


Edellinen

Seuraava



Huoltovarmuusorganisaatio
Digipooli

Selvitys Digipoolin yritysten kokonaisturvallisuuden hallinnan
tilasta

 Pakolliset kysymykset merkitty tähdellä (*)

18. Onko yrityksenne CER Direktiivin (<https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX:32022L2557>) ja sen myötä kotimaisen lainsäädännön velvoitteiden piirissä? *

- Kyllä
 Ei
 En tiedä

19. Onko yrityksenne NIS2 Direktiivin (<https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX:32022L2555>) ja sen myötä kotimaisen lainsäädännön velvoitteiden piirissä? *

- Kyllä
 Ei
 En tiedä

20. Miten näette CER Direktiivin (<https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX:32022L2557>) vaikuttavan yrityksenne toimintaan? *

21. Miten näette NIS2 Direktiivin (<https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX:32022L2555>) vaikuttavan yrityksenne toimintaan? *

22. Oletteko käsitelleet direktiivien ja sitä seuraavan lainsäädännön vaikutukset toiminnallenne organisaatiossanne? *

- Kyllä - miten
 Ei

23. Ovatko direktiivit saaneet yrityksenne harkitsemaan turvallisuudenhallinnan standardien hyödyntämistä tai jopa sertifiointia? *

- Kyllä, miksi
 Ei

Edellinen

Lähetä

Lähtettäjä: Nyqvist Antti

Lähetetty: torstai 21. syyskuuta 2023 20.09

Aihe: Kysely - Digipoolin kokonaisturvallisuuden hallinnan selvitys

Arvon verkostomme yrityksen edustaja!

Toivomme että yrityksenne osallistuu kyselyyn, jonka avulla arvioidaan verkostomme yritysten kokonaisturvallisuudenhallinnan tilaa (kokonaisturvallisuuden ohjauksen ja hallinnan nykytila ja kehitystarpeet).

Kysely tehdään Elinkeinoelämänkeskusliiton EK:n [yritysturvallisuusmallia](#) mukaillen.

Kyselyssä on 23 kysymystä ja siihen vastaamiseen on hyvä varata n.30 minuuttia.

Kyselyssä ei kysytä vastaajan henkilöön tai yritykseen liittyviä tunnistetietoja.

Kyselyyn toivotaan **vastauksia viimeistään 13.10. aikana.**

Webropol järjestelmässä julkaistuun **kyselyyn pääset vastaamaan [tämän linkin kautta.](#)**

Toivomme kyselyyn vastauksia henkilöiltä, jotka vastaavat yrityksessänne kokonaisturvallisuudenhallinnasta tai osaavat muuten arvioida sen tilaa.

Välitäthän kyselyn siis sellaiselle henkilölle, jos et itse koe sellainen olevasi.

Voit myös ladata kyselyn kysymykset pdf tiedostona [täältä.](#)

Br,

Antti Nyqvist

Valmiuspäällikkö | Chief of Preparedness

Digipoolin pääsihteeri | General secretary of Digipool

tel. +358 40 8619446, [@Nyyrman](#)

antti.nyqvist@teknologiateollisuus.fi



Huoltovarmuusorganisaatio
Digipooli

Organisoituminen

1) Kokonaan hajautettu

2) Kokonaan keskitetty

3) Tiivis konsernitason yksikkö ja hands on -voimaa liiketoiminnoissa ja tukifunktioissa

Projekt	2023/2024	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	2037	2038	2039	2040	2041	2042	2043	2044	2045	2046	2047	2048	2049	2050																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																												
001	002	003	004	005	006	007	008	009	010	011	012	013	014	015	016	017	018	019	020	021	022	023	024	025	026	027	028	029	030	031	032	033	034	035	036	037	038	039	040	041	042	043	044	045	046	047	048	049	050	051	052	053	054	055	056	057	058	059	060	061	062	063	064	065	066	067	068	069	070	071	072	073	074	075	076	077	078	079	080	081	082	083	084	085	086	087	088	089	090	091	092	093	094	095	096	097	098	099	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256	257	258	259	260	261	262	263	264	265	266	267	268	269	270	271	272	273	274	275	276	277	278	279	280	281	282	283	284	285	286	287	288	289	290	291	292	293	294	295	296	297	298	299	300	301	302	303	304	305	306	307	308	309	310	311	312	313	314	315	316	317	318	319	320	321	322	323	324	325	326	327	328	329	330	331	332	333	334	335	336	337	338	339	340	341	342	343	344	345	346	347	348	349	350	351	352	353	354	355	356	357	358	359	360	361	362	363	364	365	366	367	368	369	370	371	372	373	374	375	376	377	378	379	380	381	382	383	384	385	386	387	388	389	390	391	392	393	394	395	396	397	398	399	400	401	402	403	404	405	406	407	408	409	410	411	412	413	414	415	416	417	418	419	420	421	422	423	424	425	426	427	428	429	430	431	432	433	434	435	436	437	438	439	440	441	442	443	444	445	446	447	448	449	450	451	452	453	454	455	456	457	458	459	460	461	462	463	464	465	466	467	468	469	470	471	472	473	474	475	476	477	478	479	480	481	482	483	484	485	486	487	488	489	490	491	492	493	494	495	496	497	498	499	500	501	502	503	504	505	506	507	508	509	510	511	512	513	514	515	516	517	518	519	520	521	522	523	524	525	526	527	528	529	530	531	532	533	534	535	536	537	538	539	540	541	542	543	544	545	546	547	548	549	550	551	552	553	554	555	556	557	558	559	560	561	562	563	564	565	566	567	568	569	570	571	572	573	574	575	576	577	578	579	580	581	582	583	584	585	586	587	588	589	590	591	592	593	594	595	596	597	598	599	600	601	602	603	604	605	606	607	608	609	610	611	612	613	614	615	616	617	618	619	620	621	622	623	624	625	626	627	628	629	630	631	632	633	634	635	636	637	638	639	640	641	642	643	644	645	646	647	648	649	650	651	652	653	654	655	656	657	658	659	660	661	662	663	664	665	666	667	668	669	670	671	672	673	674	675	676	677	678	679	680	681	682	683	684	685	686	687	688	689	690	691	692	693	694	695	696	697	698	699	700	701	702	703	704	705	706	707	708	709	710	711	712	713	714	715	716	717	718	719	720	721	722	723	724	725	726	727	728	729	730	731	732	733	734	735	736	737	738	739	740	741	742	743	744	745	746	747	748	749	750	751	752	753	754	755	756	757	758	759	760	761	762	763	764	765	766	767	768	769	770	771	772	773	774	775	776	777	778	779	780	781	782	783	784	785	786	787	788	789	790	791	792	793	794	795	796	797	798	799	800	801	802	803	804	805	806	807	808	809	810	811	812	813	814	815	816	817	818	819	820	821	822	823	824	825	826	827	828	829	830	831	832	833	834	835	836	837	838	839	840	841	842	843	844	845	846	847	848	849	850	851	852	853	854	855	856	857	858	859	860	861	862	863	864	865	866	867	868	869	870	871	872	873	874	875	876	877	878	879	880	881	882	883	884	885	886	887	888	889	890	891	892	893	894	895	896	897	898	899	900	901	902	903	904	905	906	907	908	909	910	911	912	913	914	915	916	917	918	919	920	921	922	923	924	925	926	927	928	929	930	931	932	933	934	935	936	937	938	939	940	941	942	943	944	945	946	947	948	949	950	951	952	953	954	955	956	957	958	959	960	961	962	963	964	965	966	967	968	969	970	971	972	973	974	975	976	977	978	979	980	981	982	983	984	985	986	987	988	989	990	991	992	993	994	995	996	997	998	999	1000

Organisoituminen

1) Kokonaan hajautettu

2) Kokonaan keskitetty

3) Tiivis konsernitason yksikkö ja hands on -voimaa liiketoiminnoissa ja tukifunktioissa

Selvitys Digipoolin kokonaisturvallisuuden hallinnan tilasta

Saate:

Arvon Digipoolin verkoston yrityksen edustaja – osallistut haastatteluun, jonka avulla arvioidaan verkostomme yritysten kokonaisturvallisuudenhallinnan tilaa (kokonaisturvallisuuden ohjauksen ja hallinnan nykytila ja kehitystarpeet). Kysely tehdään EK:n yritysturvallisuusmallin* aiheissa.

Kyselyyn kannattaa osallistua, sillä pyrimme löytämään aiheita, joissa yritysten kehityssuunnitelmia voitaisiin tukea kokonaisturvallisuudenhallinnan tason nostamiseksi. Sillä on myös kansallista merkitystä, sillä (HVK:n hallituksen 2023 linjausten mukaisesti) se ohjaa suunnittelutyötä, jolla laaditaan alan toimintoja koskevat yleissuunnitelmat poikkeusolojen sekä niihin verrattavissa olevien vakavien häiriöiden varalle. Lisäksi sillä vaikutetaan Digipoolin toimintaan, jota ohjataan kyselyn painottamiin aiheisiin yritysten sparraamiseksi. Samalla myös arvioidaan valmiutta EU Direktiivien (NIS2, CER) ohjaaman kotimaisen lainsäädännön mahdollisille velvoitteille.

Kyselyn tuottamasta tiedosta tehdään analyysi ja tuotetaan raportti. Valmistuessaan raportin sisällöstä viestitään julkisesti ja raporttia jaetaan ensisijaisesti HVO Digipoolin verkoston yrityksille. Tulosten kautta on mahdollista saada vertailutietoa yritysten tilasta. Raportti pyrkii esittämään koottuja suosituksia tavoitetasoksi tai kehityksaiheiksi alalle.

Vaikka yritykset ovat usein kansainvälisiä on tähän kyselyyn hyvä vastata lähinnä yrityksen suomen toimintojen näkökulmasta. Rajaamalla kyselyn kohdetta helpotetaan siihen vastaamista ja tuotetaan kuitenkin huoltovarmuustoiminnalle relevanttia tietoa.

Haastattelut tehdään tunnin kalenterivarauksin ja sovitaan etukäteen kohdeyritysten edustajien kanssa. Haastatteluihin haetaan osallistuvaksi Digipoolin aktiiviryhmien yritysten edustajia.

Toivomme haastatteluun osallistuvaksi vastauksia henkilöiltä, jotka vastaavat yrityksessänne kokonaisturvallisuudenhallinnasta tai osaavat muuten arvioida sen tilaa. Välitäthän kyselyn siis sellaiselle henkilölle, jos et itse koe sellainen olevasi.

Haastattelut tehdään luottamuksellisesti ja tulokset tallennetaan käyttäen haastateltavan määrittelemää pseudonyymiä – jonka avulla haastateltava voi tunnistaa tulokset myös jälkikäteen tuloksia vertailtaessa.

*<https://ek.fi/hyotytytieto-yrityksille/yritysturvallisuus/>

1. Aloitetaan antamalla tähän pseudonyymi, jonka avulla tunnistat vastauksesi mahdollisesta raportista. (tunniste - kirjainsarja tai keksitty nimi)

Pseudonyymi: _____

1. Yrityksen kokonaisturvallisuudenhallinta

Kerro kokonaisturvallisuudenhallinnasta yrityksessänne.

1.1. Kuinka kokonaisturvallisuuden vastuut ovat organisoitu tai ohjattu yrityksessänne?

1.2. Kuinka turvallisuuden tilasta (tilannekuva) raportoidaan johdolle?

1.3. Mitkä ovat johdolle tehtävän turvallisuuden tilan raportoinnin painopisteet?

1.4. Mitä kokonaisturvallisuuden aiheita näkyy yrityksen voimassa olevassa Strategiassa ja miten (1 tai useampi aihe)?

- Henkilöstöturvallisuus
- Kiinteistö- ja toimitilaturvallisuus
- Pelastusturvallisuus
- Tuotannon ja toiminnan turvallisuus
- Ympäristöturvallisuus
- Tietoturvallisuus
- Väärinkäytösten ja poikkeamien hallinta
- Varautumisen ja kriisinhallinta
- Työturvallisuus (työterveyshuolto ja työsuojelu)
- Yritysturvallisuuden standardit

1.5. Käsitelläänkö yrityksessä vastuullisuutta?

1.6. Mitä aiheita yrityksessä käsitellään vastuullisuus otsikon alla?

- Henkilöstöturvallisuus
- Kiinteistö- ja toimitilaturvallisuus
- Pelastusturvallisuus
- Tuotannon ja toiminnan turvallisuus
- Ympäristöturvallisuus
- Tietoturvallisuus
- Väärinkäytösten ja poikkeamien hallinta
- Varautumisen ja kriisinhallinta
- Työturvallisuus (työterveyshuolto ja työsuojelu)
- Yritysturvallisuuden standardit

1. Kokonaisturvallisuuden mallit ja standardit

1.1. Jäsentääkö yrityksenne kokonaisturvallisuutta jonkin mallin tai standardin mukaan?

1.2. Sovellatteko EK:n yritysturvallisuusmallia (<https://ek.fi/hyotytietao-yrityksille/yritysturvallisuus/>)

1.3. Sovellatteko ISO standardointimalleja? Erittele ne ISO Standardit, joita sovellatte toiminnassanne.

1.4. Onko yrityksenne sertifioitunut jonkin turvallisuudenhallinnan standardin osalta? Minkä turvallisuudenhallinnan standardin osalta olette sertifioituneet?

1.5. Kerro mitä muita malleja, standardeja tai sertifikaatteja pidät oleellisena ja miksi?

1.6. Mikä/mitkä aiheet motivoivat ensisijaisesti yrityksen sertifioitumaan? (esim. Kaupallinen etu, Oman kehityksen tukeminen, Asiakasvaatimus, Muu - mikä?)

1. Kypsyysarvio

1.7. Arvioi yrityksesi turvallisuudenhallinnan kypsyystä aiheittain (EK:n yritysturvallisuusmalli) asteikolla 1-5. Arvion 1 ollessa matala kypsyysaste ja arvion 5 ollen hyvin kypsä.

Henkilöstöturvallisuus

Kiinteistö- ja toimitilaturvallisuus

Pelastusturvallisuus

Tuotannon ja toiminnan turvallisuus

Ympäristöturvallisuus

Tietoturvallisuus

Väärinkäytösten ja poikkeamien hallinta

Varautuminen ja kriisinhallinta

Työturvallisuus (työterveyshuolto ja työsuojelu)

Yritysturvallisuuden standardien hyödyntäminen

1.8. Kuinka EK:n mallin aiheet painottuvat toiminnassanne? (järjestä EK yritysturvallisuusmallin aiheet painotuksen mukaiseen järjestykseen - huomioi painotuksessa se mihin aiheisiin käytetään eniten rahaa/resursseja/aikaa.)

1.9. Minkä aiheen koet tarvitsevan kehitystä/panostuksia ja miksi?

2. EU regulaatio ja direktiivien vaikutukset kokonaisturvallisuuteen

1.1. Onko yrityksenne tulevaisuudessa CER Direktiivin (CER Direktiivi) ja sen myötä kotimaisen lainsäädännön velvoitteiden piirissä?

1.1.1. Miten näette CER Direktiivin vaikuttavan yrityksenne toimintaan?

1.2. Onko yrityksenne tulevaisuudessa NIS2 Direktiivin (NIS Direktiivi) ja sen myötä kotimaisen lainsäädännön velvoitteiden piirissä?

1.2.1. Miten näette NIS2 Direktiivin vaikuttavan yrityksenne toimintaan?

1.3. Oletteko käsitelleet direktiivien ja sitä seuraavan lainsäädännön vaikutukset toiminnallenne organisaatiossanne?

1.4. Onko Direktiiveihin ja tulevaan lainsäädäntöön varautuminen aiheuttanut resursointitarpeita tai vastuuttamista?

Kiitos haastattelusta – projektissa tehdään seuraavaksi laajempi kysely ja sen vastausten ja haastatteluiden tuloksena tehdään raportti. Raportti jaellaan osallistuneille, mutta myös HVO Extranetissä Huoltovarmuusorganisaation nähtäville. Sen havainnoilla on merkitystä toimintamme ohjauksessa.

Tavoitetila yritysturvallisuuden osa-alueille

Tässä liitteessä kuvataan turvallisuudenhallinnan painopisteet selvityksen havaintoihin nojaten sanoiksi puetun yritysturvallisuuden osa-alueiden tavoitetila Digipoolin verkoston yrityksissä. Tätä tavoitetilan kuvausta vasten voidaan arvioida edistymistä jatkossa. Seuraavat kirjaukset tarkastelevat turvallisuuden osa-alueiden tilaa yrityksissä muutaman vuoden aikajänteellä.

1.1. Varautuminen ja kriisinhallinta

Digipoolin verkoston yrityksissä on tapahtunut merkittävää edistystä varautumisen ja kriisinhallinnan alueilla. Aiheen prioriteetti on noussut keskimääräiseltä kuudennelta sijalta korkeammalle. Tämä kehitys on seurausta Digipoolin onnistuneesta valistustehtävästä, joka on lisännyt yritysten tietoisuutta hyvästä ja riittävästä varautumisesta sekä yhteiskunnan odotuksista. Kaikilla Digipoolin verkoston yrityksillä on nyt selkeät toimintatavat ja vastuut kriisinhallinnassa. Näitä toimintatapoja harjoitellaan sekä teknisesti että hallinnollisesti, ja niitä kehitetään jatkuvasti. Yrityksissä on myös käytössä kriisinhallintamallit ja -suunnitelmat, ja henkilöstöä koulutetaan säännöllisesti niiden sisällöstä. Yhä useampi yritys harkitsee eri toimintojen kriisinhallinnan prosessien yhdenmukaistamista ja samojen prosessien käyttöönottoa. Lisäksi valmiussuunnittelua tarkastellaan yhä useammin osana jatkuvuudenhallintaa. Asiakassopimussuhteissa sovitaan yhä useammin myös varautumisen ja kriisinhallinnan aiheista ja toimintaa harjoitellaan yhdessä asiakkaiden kanssa.

1.2. Tuotannon ja toiminnan turvallisuus

Kun keskustellaan aiheesta, on nykyisin parempi ymmärrys siitä, mitä sisältyy tuotannon käsitteeseen. Ohjelmistokehityksen turvallisuus on yksi tärkeä osa tuotannon turvallisuutta, ja yritykset ovat ottaneet sen huomioon suunnitelmissaan ja käytännöissään, olipa kyse ohjelmistokehityksestä tai ei. Erityisesti kolmannen osapuolen ohjelmistojen turvallisuudesta vastataan asiakkaiden suuntaan. Nopea teknologinen kehitys on otettu huomioon yhä useamman yrityksen toiminnassa. Toimintatapoja on kehitetty niin, että turvallisuusaiheet eivät jää huomiotta. Sopimushallinnassa turvallisuus on nyt erottamaton osa prosessia, ja toimitusketjun turvallisuus on arvo, jota verkoston yritykset vaalivat. Lisäksi tuotannon ja toiminnan vakuuttamista hoidetaan osana kokonaisvaltaista turvallisuudenhallintaa.



1.3. Henkilöturvallisuus

Henkilöturvallisuus on yrityksissä korkealla prioriteetilla. Henkilöturvallisuus on strategia aiheena ja sitä mitataan tavoitteita vasten sekä kehitetään jatkuvasti. Yritykset jakavat aktiivisesti tietoa henkilöturvallisuuden hallintakeinoista – esim. paljon matkustavilta yrityksiltä vähemmän matkustaville. Yhä useampi yritys on määritellyt henkisen tuen palveluita henkilöstölle - psykologista tukea turvallisuustapahtumiin liittyen – tai on sopinut niiden järjestämisestä kumppaniyrityksen kanssa. Etätyön turvallisuus on lopulta määritelty yrityksessä ja on sovittu työnantajan vastuista, velvollisuuksista ja valtuuksista.

1.4. Väärinkäytösten ja poikkeamien hallinta

Väärinkäytösten ja poikkeamien hallinta on tunnettu ja erottamaton osa turvallisuudenhallintaa yrityksissä. Yhä useampi yritys käsittelee taloudelliset väärinkäytökset ja poikkeamat samoissa prosesseissa muiden turvallisuuspoikkeamien kanssa. Useimmilla yrityksillä on toteutettuna ilmoituskanavat ja sisäinen tarkastus toimii aktiivisesti turvallisuuden tukena.

1.5. Tietoturvallisuus

Tietoturvallisuus on edelleen ICT alan yritysten korkein prioriteetti, joka näkyy strategiassa, arvoissa ja joka saa arvoisensa huomion toiminnassa. Tietoturvallisuuden tasoa seurataan johdossa ja sille asetetaan tavoitteita. Jatkuva kehitys on ratkonut nousevia uhkia ja esim. ohjelmistokehityksen turvalliset tavat ovat erottamaton osa toimintaa, hankinnat tai toimitussopimukset huomioivat kattavasti tietoturvallisuuden. Henkilöstön osaamiseen ja tietoisuuteen panostetaan valtavasti ja osataan näin välttää henkilöstöstä aiheutuvat inhimilliset häiriöt. Asiakkaiden hankintaosaaminen on kehittynyttä ja toimintojen prioriteettia kommunikoidaan aktiivisesti sopimussuhteissa. Prioriteetti ohjaa sopimussuhteiden turvallisuuden tasoa. Turvallisuudesta ollaan valmiita maksamaan. Tietoturvallisuus on yrityksissä toteutettu tehokkaasti niin, että uusien asiakasvaatimusten kohtaaminen ei aiheuta ylimääräiseksi koettua työtä. Yritysten oma tietoturvallisuuden taso on niin korkea, että se täyttää direktiivien, lainsäädännön ja vaativimpien asiakkaidenkin vaatimukset lähtökohtaisesti.

1.6. Ympäristöturvallisuus

Ympäristöturvallisuus tarkoittaa ICT alan yrityksille muutakin kuin vain energiakulutuksen optimointia. Yritykset seuraavat laitteiden kierrätystä, konesalien hiilidioksidipäästöjä sekä



ohjelmistojen ja ohjelmistokehityksen hiilijalanjälkeä. Hiilijalanjälkeä myös kompensoidaan aktiivisesti. Ympäristöturvallisuuden edut – säästöt ja tehokkuus vaikuttavat yritysten arjessa. Aihe näkyy vastuullisuusteemana ja se ohjaa yritykset konkreettisiin toimenpiteisiin. Yritysten maturiteetti on niin hyvä, että se vetoaa valistuneisiin asiakkaisiin, jotka haluavat tehdä ympäristöturvallisuudessa kunnostautuneiden yritysten kanssa töitä – ja toisaalta valistuneen henkilöstön rekrytointi on helppoa ympäristöarvojen ollessa korkealla tasolla. Verkoston yritykset tukevat toisiaan ympäristötavoitteissa ja vaikuttavat myös yhdessä toimitusketjun ympäristöaiheisiin ja edellyttävät sitä muilta.

1.7. Kiinteistö- ja toimitilaturvallisuus

Alan toimijoita ohjaavat kiinteistö ja toimitilaturvallisuudessakin periaatteet, jotka nostavat kaikkien yritysten tasoa lähemmäs alan kärkeä. Yrityksillä on käytössään selkeät käyttötärpeen mukaan määrittävät tasomallit erilaisten tilojen ja kiinteistöjen turvallisuudelle. Liiketoiminnan ja asiakasvaatimusten ohjaavasta vaikutuksesta on tässäkin päästy siihen, että yrityksen oman toiminnan mallit kattavat useimmat. Kiinteistö ja toimitilaturvallisuutta arvioidaan ja kehitetään itsenäisesti ja säännöllisesti. Vuokratiloissa toimivat alan yritykset saavat sopimussuhteensa toimimaan kuten toimisivat omissa tiloissa- vastuut on selvästi määritelty ja sovittu ja turvallisuutta kehitetään yhteistyössä. Yksityisen turva-alan palveluita käytetään tottuneesti suorilla sopimussuhteilla tai saadaan vuokrasopimussuhteissa yhteistyö toimimaan kuten näin olisi. Sopimushallinta ja vakuuttaminen on turvallisuusprosesseissa erottamattomana osana.

1.8. Pelastusturvallisuus

Pelastusturvallisuudesta pidetään huoli kuten kiinteistö ja toimitilaturvallisuudesta. Kokonaisuudelle löytyy yrityksistä vastuu henkilöstöä. Henkilöstön koulutuksia järjestetään säännöllisesti ja poistumisharjoitukset ovat arkea kohdetyypistä huolimatta. Pelastussuunnitelmien laatu on noussut niiden sisällön kriittisen tarkastelun myötä. Tietoisuus lakisääteisistä palovakuutuksista on korkea ja hallittu muiden vakuutusten lailla turvallisuudenhallinnan kokonaisuudessa.

1.9. Työturvallisuus (työterveyshuolto ja työsuojelu)

Työsuojelu on edelleen korkealla tasolla alan yrityksissä. Aiheita seurataan ja mittaroidaan aktiivisesti ja toimenpiteitä toteutetaan tämän perusteella. Työsuojelua ja työterveydenhuoltoa tarkastellaan kokonaisuutena erottamattomasti henkilöstöturvallisuuden kanssa.



Työterveyshuollon ja työsuojelun sopimusten kattavuutta arvioidaan jatkuvasti ja toimintaa kehitetään yhteistyössä kumppanien kanssa. Henkilöstöturvallisuus, työterveyshuolto ja työsuojelu näkyvät esimiestyössä ja esimiestyötä kehitetään tämä tavoite mielessä.

Työterveyshuolto ja työsuojelu huomioivat nousevat ilmiöt ja tuo ratkaisuita arkeen.

Työsuojelun konsepti huomioi esim. etätyöolosuhteet, ergonomian ja työhyvinvoinnin sekä tukee kuntoilua.

1.10. Turvallisuusaiheet strategioissa

Kaikissa Digipoolin verkoston yrityksissä näkyvät turvallisuusaiheet strategiakirjauksissa.

Turvallisuus ylipäänsä sekä eritellen ne yritysturvallisuuden aiheet, jotka kulloinkin nähdään kaipaavan panostuksia. Tietoturvallisuus näkyy kaikilla yrityksillä strategian arvona tai vastuullisuuskysymyksenä ja tätä tuetaan mm. tuotannon ja toiminnan turvallisuusaiheilla.

1.11. Yritysten organisoituminen turvallisuudenhallinnan osalta

Turvallisuudenhallinnan organisoitumista tarkastellaan aktiivisesti ja kehitetään havaintojen perusteella. Kehityksessä on huomioitu se, että kokonaisturvallisuus ei eriydy missään aiheessa yksittäisten osastojen tehtäväksi yksinään vaan turvallisuuden kokonaisuudelle tunnustetaan kokonaisuutta käsittelevät vastuutoimijat. Liiketoiminnan riskit ja operatiiviset riskit kohtaavat organisaatiossa aktiivisesti. Fyysisen maailman turvallisuus, kyberturvallisuus, sopimukset, vakuutukset sekä talouden pitoon liittyvät turvallisuusaiheet ovat mukana kokonaisuuden tarkastelussa tavalla tai toisella ja tämä pystytään myös henkilöstön toimesta esittämään.