Toimialojen kyberkypsyyden selvitys 2022

Kansallinen koosteraportti

Huoltovarmuuskeskus

Huoltovarmuuskeskus

www.huoltovarmuuskeskus.fi

Huoltovarmuudella tarkoitetaan kykyä sellaisten yhteiskunnan taloudellisten perustoimintojen ylläpitämiseen, jotka ovat välttämättömiä väestön elinmahdollisuuksien, yhteiskunnan toimivuuden ja turvallisuuden sekä maanpuolustuksen materiaalisten edellytysten turvaamiseksi vakavissa häiriöissä ja poikkeusoloissa.

Huoltovarmuuskeskus (HVK) on työ- ja elinkeinoministeriön hallinnonalan laitos, jonka tehtävänä on maan huoltovarmuuden ylläpitämiseen liittyvä suunnittelu ja operatiivinen toiminta.

Huoltovarmuusorganisaatio (HVO) on verkosto, joka työskentelee yhdessä Suomen toimintakyvyn ja sen edellyttämän huoltovarmuuden hyväksi. Siihen kuuluvat Huoltovarmuuskeskus ja sen hallitus, huoltovarmuusneuvosto sekä eri toimialojen sektorit ja poolit. Lisäksi yhteistyötä tehdään alueellisten toimijoiden, kuten aluehallintovirastojen, kuntien ja kaupunkien sekä alueellisten toimikuntien kanssa.

Julkaisija: Huoltovarmuuskeskus
Laatinut: Laatinut Huoltovarmuusorganisaation Digipooli ja Accenture Oy
Kuvat: GettyImages
Taitto: LM Someco Oy
Julkaisuvuosi: 2023
ISBN: 978-952-7470-23-7

Sisältö

1 Johdanto

Toimialojen kyberselvitys oli jatkumoa aiemmalle selvitykselle, joka toteutettiin vuosina 2019–20. Selvitykset olivat osa Huoltovarmuuskeskuksen Digitaalinen Turvallisuus 2030 -ohjelmaa[1] (DT2030). Tavoitteena oli tuottaa keskeistä pohjatietoa ohjelman investointien suuntaamiseksi.

Selvitys toteutettiin arvioimalla 121 toimijan kyberkypsyys. Osallistuneiden toimijoiden valinnan tavoitteena oli tuottaa laaja otos eri toimialoista sekä erilaisista organisaatioista toimialojen sisällä. Toimialoja selvitykseen kertyi lopulta 12. Osallistujat valittiin toimialapoolien avustuksella ja otokseen kerättiin huoltovarmuusketjun toimijoita monipuolisesti eri profiileilla, organisaation koon, toimialueen ja liiketoimintamallin perusteella.

Toimialojen selvityksen ydinhavainto oli, että osallistuneiden yritysten ja organisaatioiden kypsyystaso oli hyvällä perustasolla (3,00), mutta sekä toimialojen että yritysten välillä oli paljon hajontaa. Samanaikaisesti havaittiin, että uhka- ja riskikenttä oli merkittävässä muutoksessa ja kybertoiminnan lisääntyminen oli havaittu lähes kaikissa osallistuneissa organisaatioissa.

Tämä raportti kokoaa yhteen keskeiset kehityskohteet ja päähavainnot toimialaraporteista, jotka valmistuivat selvityksen tuloksista vuoden 2022 aikana. Selvitykseen osallistuneet toimijat saivat omat ja toimialakohtaiset tulokset. Lisäksi toimialakohtaisia tuloksia jaettiin toiminnan kehityksestä vastaaville tahoille kuten Huoltovarmuusorganisaation poolien käyttöön.

Digipoolin toimeksiannosta Accenturen tietoturvakonsultit toteuttivat selvityksen vuoden 2022 aikana. Tukena työssä oli myös suuri määrä toimiala-asiantuntijoita.

Huoltovarmuusorganisaation eri toimialojen ja yritysten kyberkypsyyttä on selvitetty eri keinoin historiassa. Nyt tehty selvitys on toinen laatuaan. Tämän kaltaisia selvityksiä tullaan edelleen toteuttamaan säännöllisin väliajoin, jotta voidaan seurata kypsyyden kehitystä ja tarjota kehitystä edistävää tietoa kotimaisille organisaatioille.

[1] https://www.huoltovarmuuskeskus.fi/huoltovarmuusorganisaatio/huoltovarmuuskeskus/4962-2/digitaalinen-turvallisuus-2030

2 Johdon tiivistelmä

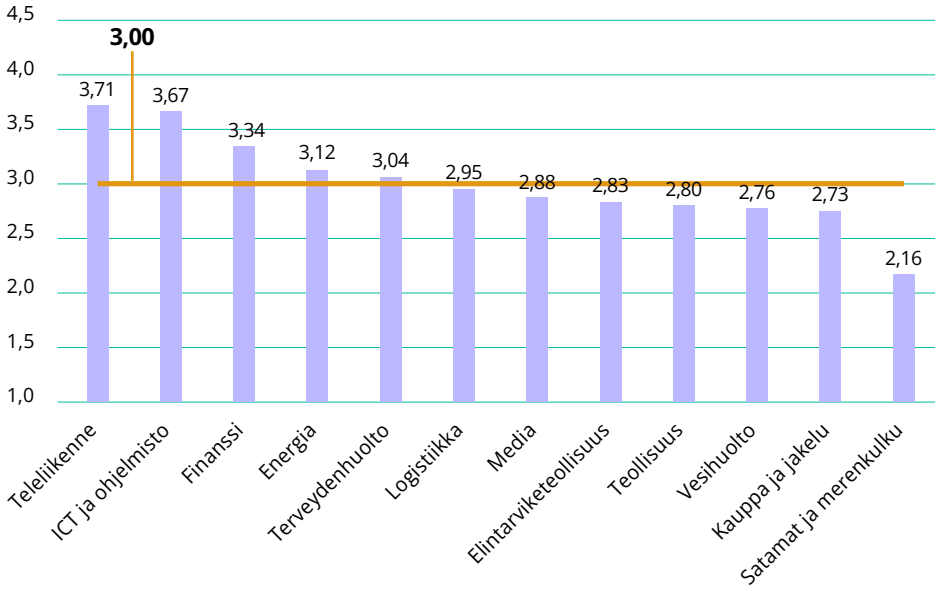
Toimialojen kyberselvitys 2022-raportti käsittää 12:sta toimialan kyberturvallisuuden kypsyysselvitysten tulokset ja analyysiin pohjautuvat suositukset sekä johtopäätökset. Päähavainnot olivat:

- Vuoden 2022 muutokset uhka- ja riskikentässä ovat tuoneet kyberturvallisuuden myös niiden johtoryhmien agendalle, jotka eivät aikaisemmin käsitelleet kyberturvallisuuden tilannekuvaa säännöllisesti
- Kypsyystasoa nostavia tekijöitä tunnistettiin olevan liiketoiminta- ja riskilähtöinen kyberturvallisuuden kehittäminen, standardeihin perustuvat johtamisjärjestelmät ja sujuva kommunikaatio kyberturvallisuusvastaavien ja organisaation ylimmän johdon välillä
- Kypsyyttä laskevia tekijöitä tunnistettiin olevan strategisen suunnittelun puute, reaktiivinen suhtautuminen kriittiseksi nousseisiin uhkiin ja riskeihin sekä riskienhallinnan käytäntöjen puute
- Kumppaniverkostojen, kokonaisketjujen ja riippuvuuksien tunnistaminen vaatii kehittämistä kaikilla toimialoilla
- Organisaatioiden kybervarautumiseen vaikuttaa käsitys oman organisaation houkuttelevuudesta kyberrikollisten silmissä
- Turvallisuusympäristöön merkittävästi vaikuttavat tapahtumat, kuten geopoliittiset muutokset lähialueilla tai suureen julkisuuteen nousseet kyberhyökkäykset, kuten psykoterapiakeskus Vastaamon tietomurto, nostavat hetkellisesti organisaatioiden kyberturvatietoisuutta, mutta pitkän aikavälin kehitys vaatii säännöllisiä johdon raportoinnin käytäntöjä
- Kyberturvallisuusalaa piinaava pula osaajista näkyy usean organisaation kohdalla. Haasteen ratkaisu vaatii toimenpiteitä monella tasolla
- Aktiivinen sidosryhmätoiminta ja uhkatiedon jakaminen eivät heijastele suoraan organisaatioiden kypsyysarvioihin. Uhkat ja riskit tiedostetaan nykytilassa aiempaa paremmin, mutta saatujen tietojen hyödyntäminen jää usein vajaaksi osaamisen, tekijöiden tai ajanpuutteen vuoksi

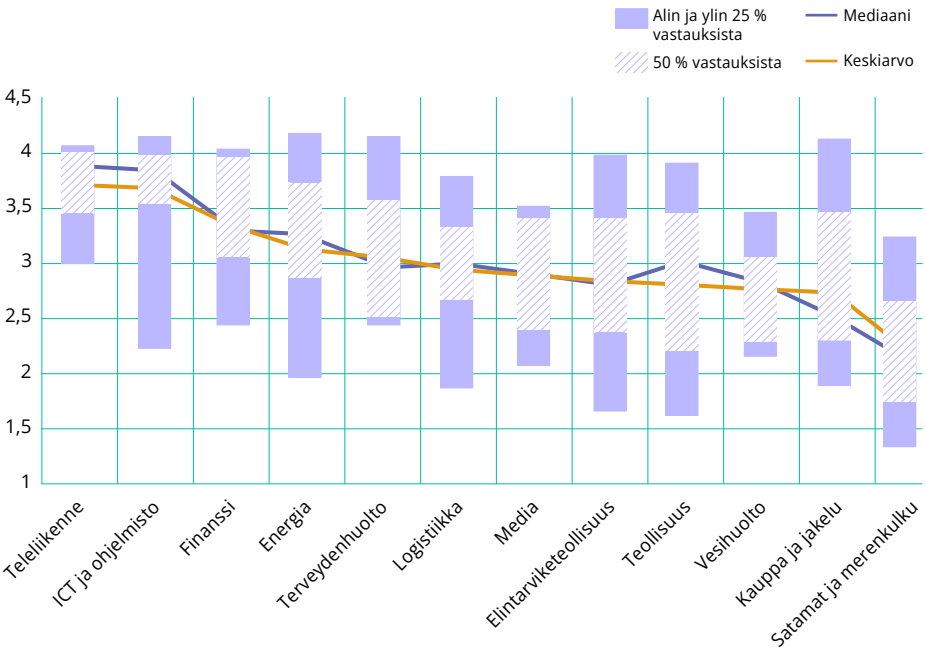
TOIMIALAA

Kaikkien toimialojen keskiarvoa 3,00 voidaan pitää **hyvänä perustasona**

YRITYSTÄ



Valtaosa selvityksessä tutkituista toimialoista on vähintään kohtuullisella kyberturvallisuuden tasolla.



Pienin hajonta oli Teleliikenteessä ja suurin Elintarviketeollisuudessa.

3 Suositukset

Tässä luvussa esitellään selvityksen tulosten perusteella laaditut suositukset kyberturvallisuuden kehittämiseksi. Toimialakohtaisista raporteista kerättiin toimialojen kehityssuositukset ja tähän raporttiin nostettiin niistä useimmin toistuvat. Alkuperäiset toimialakohtaiset suositukset olivat priorisoitu kypsyysselvitysten tulosten sekä toimialan uhka- ja riskikentän perusteella. Tässä kansallisessa raportissa kriittisimmät suositukset jaettiin kolmeen kategoriaan: kansallista varautumista edistävät, liiketoimintaa edistävät sekä kyberasiantuntijoille suunnatut suositukset.

Selvityksen havainnot ja suositukset jakautuvat kolmelle eri tasolle:

- Kansallisen raportin suositukset, jotka vastaavat kysymykseen: Mitä toimenpiteitä kansallisella tasolla selvitystulosten perusteella tulisi edistää?
- Toimialaraporttien suositukset, jotka vastaavat kysymykseen: Millaisia asioita toimialan tilanteen perusteella toimialalla yleisesti tulisi edistää?
- Yritysraporttien suositukset, jotka vastaavat kysymykseen: Mitä yksittäisen yrityksen tulisi huomioida omaa kypsyystilannetta kehittäessä?

3.1 Kansallista varautumista edistävät

Kolmansien osapuolten riskienhallinnan kehittäminen
Toimitusketjuista aiheutuvien kyberriskien tunnistaminen sekä niiden jatkuva arviointi on toimialoille kriittisen tärkeää monimutkaistuvassa toimintaympäristössä, jossa hyökkääjät usein pyrkivät iskemään ketjun heikoimpaan lenkkiin. Läpinäkyvyyttä verkostojen suuntaan voi lisätä yhteisillä riskien katselmoinneilla sekä molemminpuolisella vaatimusten asettamisella ja niiden toteutumisen seurannalla. Hankintoja tehdessä tieto- ja kyberturvallisuuteen liittyvien vähimmäisvaatimusten asettaminen sopimuksiin sekä kumppanuussuhteen koko elinkaaren aikainen hallinta vähentää verkostosta aiheutuvien uhkien todennäköisyyttä.

Kyberturvallisuustietoisuuden sekä -osaamisen kasvattaminen
Alati muuttuvassa ympäristössä kyberturvallisuustietoisuuden ja -osaamisen kehittäminen vaatii yrityksiltä jatkuvaa työtä niin koko henkilöstön kuin kyberturvallisuusasiantuntijoiden osalta. Osaamisen ja tietoisuuden ylläpitämiseksi on tarpeellista luoda jatkuvaa kehitystä tukevia malleja koko työsuhteen ajalle. Kansallisesta näkökulmasta osaajapulaan voidaan vastata erityisesti kyberturvallisuuteen tai teknisiin opintopolkuihin investoimisen jatkamisella sekä aloituspaikkojen lisäämisellä. Julkisten tahojen ja elinkeinoelämän yhteistyön lisääminen erityisesti uranvaihtajille suunnatuissa koulutuksissa vastaa myös omalta osaltaan alaan vaikuttavaan osaajapulaan. Osana poolitoimintaa on suositeltavaa tunnistaa toimenpiteitä ja toteuttaa koulutuksia, joiden avulla yritykset kykenevät lisäämään toimialaosaajien kyberturvatietoisuutta sekä mahdollisesti kehittämään toimialaa syvällisesti tuntevia kyberturvallisuusasiantuntijoita.

Kansallisen yhteistyön aktiivinen kehittäminen
Jotkin uhkat, kuten hybridivaikuttaminen tai valtiollisen tason kybervaikuttaminen ovat sellaisia joihin vastaaminen vaatii kansallisen tason yhteistyötä. Olemassa olevien hyvien jatkuvuusharjoittelu- ja tiedonvaihtomallien lisäksi on löydettävä keinoja harjoituttaa yksittäisiä organisaatioita tai kannustaa niitä itsenäiseen harjoitteluun. Erilaiset kansallisen tason kyberharjoitukset ovat hyviä kasvattamaan kyberasiantuntijoiden osaamista, mutta jatkossa on löydettävä tapoja kasvattaa kokonaisten organisaatioiden kybertietoisuutta ja -resilienssiä.

Tiedonvaihdon aktiivisuus vaihtelee toimialoittain. Esimerkiksi teleliikennealan organisaatiot vaihtavat aktiivisesti uhkatietoa keskenään alan kovasta kilpailusta huolimatta. Huoltovarmuusorganisaation poolitoiminta tai Kyberturvallisuuskeskuksen ISAC-tiedonvaihtoryhmien toimintaa on suositeltavaa laajentaa toimialoilla, joilla kyberturvallisuuden tilannekuvan ja uhkatiedon jakaminen ei vielä ole kattavaa.

Yhteisen tilannekuvan kehittäminen
Kansallisella tasolla on suositeltavaa jatkaa yhteisen tilannekuvan kehittämistä. Liikenne- ja viestintävirasto Traficomin toteuttama Kybersää sekä sen jatkokehitys on hyvä pohja yhteisen kansallisen tilannekuvan toteuttamisessa. Teknisen näkökulman edistäminen osana tapahtumien tunnistamiseen, analysointiin ja raportoimiseen lisäisi tilannekuvan hyödyllisyyttä. Mahdollisuus jakaa esimerkiksi kansallisesti relevanttia uhkatietoa tukisi Havaro-toiminnan nykyisellään tuottamaa näkyvyyttä.

3.2 Liiketoimintaa edistävät

Kyberturvallisuuden pitkän aikavälin liiketoimintalähtöinen suunnittelu ja kehittäminen
Kyberturvallisuuden pitkän aikavälin strateginen suunnittelu, joka huomioi liiketoiminnan riskit ja tavoitteet sekä ohjaa kyberturvallisuuteen liittyvissä päätöksissä ja investoinneissa toimii yrityksen koko kyberturvallisuuden perustana ja auttaa hallitun toiminnan ylläpitämistä. Liiketoimintalähtöisessä kyberturvallisuudessa tunnistetaan yrityksen toiminnan jatkuvuutta uhkaavat riskit sekä haasteet, jotka toteutuessaan saattavat vaikeuttaa strategisten tavoitteiden saavuttamista. Läpi kaikkien toimialojen havaittiin liiketoimintalähtöisyyden olevan merkittävä vaikutin korkean kypsyyden taustalla.

Kyberriskien nostaminen osaksi yrityksen kokonaisriskienhallintaa
Selvityksen perusteella riskienhallinnan toteutus organisaatioissa ei usein kata kyberriskejä. Kyberturvallisuusriskien ymmärtämiseksi ja arvioimiseksi niiden käsittely tulisi integroida osaksi organisaation muuta riskienhallintaa. Riskilähtöinen kyberturvallisuuden kehittäminen vaatii yhteistyötä organisaatioiden kyberturvallisuusvastaavien ja riskienhallintajohdon kanssa, jotta kyberturvallisuuden tekninen ymmärrys saadaan sovitettua mitattaviksi riskeiksi. Kyberriskien strukturoidumman arvioinnin lopputuloksena kriittisimmät kyberriskit tulee kommunikoida organisaation johdolle, jotta kehitystoimet ja investoinnit ovat riskilähtöisesti oikeansuuntaisia ja saavat tarvittavan tiedon taakseen.

OT-turvallisuuden kehittäminen, toimintojen yhtenäistäminen
Tuotannollisen teknologian (Operational Technology, OT) lisääntyvä liitettävyys, analytiikan hyödyntäminen seurannassa ja ohjauksessa sekä modernisointi lisää tarvetta kyberturvallisuuden hallinnalle. Selvityksen perusteella yritysten kyberturvallisuuden hallinta sekä OT-ympäristöjen hallinta ovat eriytyneet. Hallinnan hajautuminen ei sinänsä ole ongelma, mutta kokonaistilannekuvan tuottamisen osalta olisi tärkeä kyetä huomioimaan molemmat ympäristöt. Tämä vaatii yhteistyön määrittelyä ja toteutusta sekä tehokasta tiedonvaihtoa vastuullisten kesken. Näiden aikaansaaminen on tärkeä organisaation kokonaiskyberturvallisuuden varmistamiseksi.

Kyberturvallisuuden hallinnan kehittäminen ja johdon sitouttaminen
Johdon sitouttaminen varmistaa sen, että budjetit ja suunnitteluhorisontti ovat riittäviä riskeihin nähden. Yksi selvityksessä havaittu haaste oli kehityssuunnittelun ja budjettien reaktiivisuus sekä pitkän aikavälin näkemyksen puute sen ohjaamisessa. Tällöin organisaatiot tekevät kyberturvallisuuden investointipäätökset yksittäisinä ratkaisuina, joihin usein myös joudutaan perustelemaan budjetti hanke- tai projektikohtaisesti. Tämä lyhentää usein kehityssuunnittelun näköalaa ja ohjaa toimintaa reaktiiviseen suuntaan.

Oleellista on löytää yhteiset mittarit, joilla kyberturvallisuuden tilannekuvaa voidaan viestiä johdolle niin, että se on helposti ymmärrettävissä ja johto voi aktiivisesti osallistua tarvittavien toimenpiteiden suunnitteluun. Johdon sitouttamisen tärkeimpiä elementtejä ovat kyberaiheiden kommunikointi niin, että vaikutukset liiketoiminnalle ovat hyvin kuvattuja.

3.3 Kyberasiantuntijoille suunnatut

Tietoturvavalvonnan vahvempi integroiminen muuhun toimintaan
Varsinkin korkean kypsyystason toimialoilla nähdään tietoturvavalvomotoimintojen (Security Operations Centre, SOC) yleistyminen. Valvomoja on toteutettu niin sisäisinä toimintoina kuin ostopalveluina kumppaneilta. Haasteena valvomopalveluiden hyödyntämisen osalta havaittiin niiden rajoittuminen ainoastaan valvontaa toteuttaviksi toiminnoiksi. Tällöin SOC-toiminnon ainoa tehtävä on nostaa havainnot esiin muulle organisaatiolle selvitettäväksi. Tällöin valvomo täyttää vaatimustenmukaisuuden, mutta lisäarvo toiminnasta jää pieneksi. Tietoturvavalvomo tulisi integroida vahvemmin organisaation muuhun toimintaan, esimerkiksi omaisuuden-, haavoittuvuuksien- sekä uhkienhallintaan, jolloin se kykenee toimimaan keskeisenä päivittäisen, operatiivisen kyberturvatoiminnan solmukohtana, tukien myös kyberturvatapahtumien selvittämistä.

Sovellusturvallisuuden kehittäminen
Sovellustietoturvan tärkeys korostuu nykymaailman digitaalisessa toiminnassa organisaation toimialasta riippumatta. Erilaista kehitystä tehdään sekä itse että kumppaneiden toimesta, jolloin kehitysmallien tietoturvanhallinta sekä tuotosten tietoturvan varmistaminen on tärkeää. Modernien kehitysmallien osana esimerkiksi DevSecOps tai Security Champion -roolit kehittäjien tukena ovat tietoturvan varmistamisessa keskeisiä.

Sidonnaisuuksien tunnistamisen kehittäminen
Toimittajaverkostojen kehittyessä yhä kompleksisemmiksi on tärkeä laajentaa näkyvyyttä kattamaan myös suorien toimittajien alihankkijoita sekä muita sidonnaisuuksia (esimerkiksi riippuvuudet sovelluskomponenttien osalta). Kumppaninhallintaa tulee myös kehittää kattamaan palveluiden ja kumppanuussuhteiden koko elinkaaren. Nykyisellään selvityksen tulosten perusteella monet organisaatiot tuottavat hankintavaiheessa kyberturvavaatimukset, mutta jatkuvaa seurantaa, yhteydenpitoa ja vaatimusten toteutumisen varmistavia kontrolleja ei välttämättä hyödynnetä.

Proaktiivisen uhkien tunnistamisen kehittäminen
Uhka- ja riskikentän kehitys vaatii organisaatioilta yhä aktiivisempaa otetta kyberturvallisuuden osalta. Uhkien tunnistamisessa korostuu ymmärrys omaisuuden- ja haavoittuvuushallinnan kautta, joka muodostaa pohjan sille, miten valvontaa ja poikkeamiin vastaamisen resursseja kyetään suuntaamaan tehokkaasti. Kyvykkyyksien kehittäminen ja suojauksien toteutus täytyy olla jatkuvaa tekemistä, jonka osana seurataan ja arvioidaan kehittyvää uhkakenttää. Varautumisessa on tärkeää erilainen verkostoituminen ja tietolähteiden hyödyntäminen. Esimerkiksi Kyberturvallisuuskeskuksen fasilitoimat ISAC-tiedonvaihtoryhmät auttavat eri alojen varautumisessa, mahdollistamalla luottamuksellisen kokemusten jakamisen.

4 Johtopäätökset

Tässä luvussa nostetaan esiin selvityksen keskeiset johtopäätökset ja esitellään niiden taustalla olevia havaintoja. Johtopäätökset muodostettiin keräämällä toimialakohtaisista raporteista useimmin toistuvat havainnot, joiden perusteella tunnistettiin toimialoja yhdistäviä kyberturvallisuuteen vaikuttavia tekijöitä.

4.1 Kypsyystasoon vaikuttavat tekijät

Selvitystyössä havaittiin taustatekijöitä, jotka vaikuttivat kypsyystasoon nostaen tai laskien. Arvio tekijöiden vaikutuksesta perustui havainnoituun korrelaatioon, koska kausaliteetin toteaminen vaatisi tarkempaa selvitystä. Seuraavat tekijät olivat tämän selvityksen aineiston perusteella yhteisiä korkean ja matalan tason organisaatioilla toimialasta riippumatta.

Kypsyyttä nostavia:

- Liiketoiminta- ja riskilähtöinen kyberturvallisuuden kehittäminen
- Standardeihin tai muihin viitekehyksiin perustuvat johtamisjärjestelmät
- Sujuva kommunikaatio kyberturvallisuusvastaavien ja organisaation ylimmän johdon välillä

Kypsyyttä laskevia:

- Strategisen suunnittelun puute kyberturvallisuuden kehittämisessä ja hallinnassa
- Ennakoinnin sijaan reaktiivinen suhtautuminen kriittiseksi nousseisiin uhkiin ja riskeihin
- Riskienhallinnan käytäntöjen puute

4.2 Uhka- ja riskikentän muutokset

Kaksi merkittävintä tekijää uhka- ja riskikentän kehityksessä olivat viime vuosien aikana olleet COVID 19 -pandemia sekä geopoliittisen tilanteen muutos. Kyseiset asiat vaikuttivat laajasti niin liiketoimintaan kuin kyberturvallisuustilanteeseen kaikilla toimialoilla. Globaalit trendit vaikuttivat myös uhkatoimijoiden tapaan menetellä. On selvää, että erilaiset hyökkäykset olivat selvitykseen osallistuneiden organisaatioiden mukaan kasvussa. Tähän vaikuttivat muun muassa kasvanut tietoisuus uhkatilanteesta sekä parantunut kyvykkyys havaita normaalista poikkeavaa tai haitallista toimintaa.

Uhka- ja riskikentän muutoksiin liittyneiden työpajakeskustelujen pohjalta oli selvää, että kyberturvallisuuden kehittäminen on jatkuvaa kilpajuoksua uhkatoimijoita vastaan. Uhkatoimijat kehittävät omia kyvykkyyksiään (TTP, tools, tactics and procedures) tukemaan omia tavoitteittaan, jolloin organisaatioihin kohdistuvat uhkat kehittyvät ja muuttuvat.

Uhka, jota ei selvitystyöpajoissa juurikaan nostettu esiin, oli teollisuusvakoilu. Maailman muutos ja uhkatilanteen kehittyminen viimeisen kahden vuoden aikana on voinut laskea sen painoarvoa vähäiseksi, kun yritykset keskittyivät merkittävämpien asioiden hallintaan. Teollisuusvakoilu on ollut esillä viranomaisviestinnässä viime vuosina, joka eroaa selvitystyöpajoissa käydyistä uhka- ja riskikeskusteluista. Jatkossa teollisuusvakoilun ja tiedustelun uhka olisi hyvä muistaa riskien tunnistamisen ja arvioinnin yhteydessä.

4.3 Kolmansien osapuolten hallinta

Selvitystyöpajojen perusteella selvitykseen osallistuneet organisaatiot keskittävät kumppanihallinnan kontrollit suoriin kumppaneihin, joita hallitaan niin sopimustason vaatimuksien kuin jatkuvan yhteistyön ja valvonnan kautta. Toisaalta useat selvitykseen osallistuneet organisaatiot kertoivat luottavansa kumppaneihin hallinnan ja valvonnan osalta eikä varsinaisia valvontatoimenpiteitä toteuteta kumppanin raportoinnin lisäksi. Valvonnan laiminlyönti voi aiheuttaa merkittävän riskin, joka kannattaa tunnistaa.

Kumppaniverkostojen, kokonaisketjujen ja riippuvuuksien tunnistamisessa sekä niiden hallinnassa selvitykseen osallistuneilla tahoilla on edelleen kehitettävää. Pääosin kumppaniverkostoja hallitaan määrittämällä alihankkijat suorien kumppaneiden vastuulle. Kokonaisuuden hallinnan kannalta riippuvuuksien tunnistaminen olisi tärkeää, koska erilaiset kumppanit käytännössä laajentavat kokonaisriskiä. Erilaisten integraatioiden kautta kumppanit ja niiden alihankkijat voivat jopa laajentaa yrityksen verkkoa ja mikäli tällaiset riippuvuudet eivät ole tiedossa, on niiden aiheuttama potentiaalinen uhka merkittävä.

4.4 Viitekehysten ohjaama johtaminen yleistynyt

Kypsimmiksi arvioitujen yritysten toiminnan taustalta havaittiin tässä selvityksessä erilaisten viitekehysten käyttö tai niiden ohjaama johtamismalli. Toimialoista vahvimpien, kuten Teleliikenteen sekä ICT- ja ohjelmistoalan, organisaatioilla standardin mukaisesti toteutettu hallintamalli, sekä usean organisaation kohdalla myös sertifiointi, vaikuttivat positiivisesti järjestelmälliseen toimintaan. Myös muilla toimialoilla yksittäiset organisaatiot kokivat hyödylliseksi viitekehysten tai sertifiointien tuoman yhteisen kielen kommunikoidessaan sidosryhmien kanssa, vaikka esimerkiksi asiakkaat eivät varsinaisesti sertifiointia vaatisikaan. Lainsäädännön mukaisen toiminnan varmistamiseksi on viitekehysten mukainen toiminta hyödyllistä usealla toimialalla myös auditointien vuoksi. Esimerkiksi finanssialan toiminnan perustuminen toimilupaan vaatii organisaatioilta tietyt tietoturvallisuuteen liittyvät toimenpiteet sekä dokumentaation, jotta organisaatio voi osoittaa valvontaviranomaisille täyttävänsä toiminnalle asetetut vähimmäisvaatimukset.

4.5 Kyberturvallisuus johdon asialistalla

Uhka- ja riskikentän muutoksien myötä yhä useampi organisaatio oli aloittanut kyberturvallisuuteen liittyvien asioiden käsittelyn osana johdon agendaa. Muutos oli tapahtunut etenkin matalamman kypsyystason organisaatioissa, joilla ei entuudestaan ollut toimintamalleja johdon raportointiin esimerkiksi kyberriskeistä tai kyberturvallisuuden tilannekuvasta. Kypsemmän tason organisaatioissa kyberturvallisuus oli jo pidemmän aikaa ollut johdon agendalla. Näissä organisaatioissa oli varmistettu johdon tuki kyberturvallisuuden kehittämisohjelmalle ja tavoitteiden toteutumista seurattiin johdonmukaisesti.

Selvityksessä kävi ilmi, että turvallisuusympäristöön merkittävästi vaikuttavat tapahtumat, kuten geopoliittiset muutokset lähialueilla tai suureen julkisuuteen nousseet kyberhyökkäykset, kuten psykoterapiakeskus Vastaamon tietomurto, nostavat hetkellisesti organisaatioiden kyberturvatietoisuutta. Vaikka selvitystyön aikana kyberturvallisuus oli johdon asialistalla monessa organisaatiossa, näyttää siltä, ettei poikkeamien ja teknisluontoisten asioiden käsittely säilytä johdon kiinnostusta pitkällä tähtäimellä. Kyberturvallisuudesta vastaavien kannattaa keskittyä tunnistamaan asiat, joita johdon tasolla on tarkoituksenmukaista käsitellä ja seurata. Olennaista on löytää sellaiset mittarit ja tilannekuvan elementit, jotka ovat kohderyhmälle oikeita. Aihealueella menestyneet toimijat olivat löytäneet niin sanotun ”yhteisen kielen”, jolla kyberturvallisuuden tilannekuvasta viestitään johdolle liiketoimintapainotteisesti.

4.6 Liiketoimintalähtöinen kyberturvallisuus on kilpailuetu

Liiketoimintalähtöinen kyberturvallisuus näytti selvästi tukevan kypsyystason kehittymistä läpi kyvykkyysalueiden. Myös aloilla, joilla vahva sääntely on luonut pohjan perustason kyberturvallisuudelle, oli nähtävissä, että kyberturvallisuuden pitkäjänteisen kehittämisen integrointi organisaation liiketoimintastrategiaan ja tarpeisiin vaikutti kypsyyteen positiivisesti. Liiketoimintalähtöisyys auttoi ohjaamaan erityisesti pitkän aikavälin kehittämistä, jolloin kyberturvallisuuden tavoitteita kyettiin määrittämään organisaation tarpeista lähtöisin ja niiden kehittämistä oli helpompi seurata. Liiketoimintalähtöisyys toi etuja sisäisen kommunikaation suunnittelussa, kun kyberturvallisuudesta kyettiin puhumaan samaa kieltä liiketoiminnan edustajien kanssa.

Liiketoiminta- ja riskilähtöisyys näyttivät kulkevan käsi kädessä. Kun kyberturvallisuuden ohjausta kehitettiin liiketoimintaa tukevaksi, nousi riskilähtöisyys ohjaavaksi tekijäksi. Tämä vaikutti auttavan myös siilojen purkamisessa riskienhallinnan osalta, jossa havaittiin edelleen, että kyberriskejä ei käsitelty kokonaisriskienhallinnan osana, vaan ne oli eriytetty omille vastuutahoille. Kyberturvallisuuden asemoiminen liiketoiminnan mahdollistajana toi siis selvästi hyötyjä sekä liiketoiminnalle että kyberturvallisuudelle itselleen.

4.7 Pula kyberturvallisuuden osaajista

Julkisuudessa koko IT-alan osalta toisteltu osaajapula näkyi selvitystyössä kyberturvallisuusosaajien saatavuuden kohdalla. Selvitykseen osallistuneilla yrityksillä oli selkeitä tarpeita kehittää kyberturvallisuustekemistä useilla alueilla, mutta yhtenä pullonkaulana oli osaajien saatavuus. Tämä korostui erityisesti aloilla ja organisaatioissa, jotka eivät olleet vetovoimaltaan työnantajien kärjessä, kuten perusinfrastruktuurista vastaavissa yrityksissä ja organisaatiossa. Osaajien saatavuuteen vaikuttivat yrityksen ja toimialan imago, palkkataso sekä yrityksen kyky kehittää kyberturvallisuustoimintaa ja sitä myötä tarjota urakehitysmahdollisuuksia. Tosin on muistettava, että nykyisistä osaajista kilpaillessa jaetaan niukkuutta eri alojen kesken. Uusien osaajien kouluttamisen tulisi olla yksi toimenpide osaajapulaan vastaamiseksi sekä kansallisesti, toimialoittain, että yrityksille itselleen.

4.8 Tuotannollisten ympäristöjen hallinnan eriytyneisyys

OT-ympäristöt olivat perinteisesti kehittyneet osaksi tuotannollista toimintaa ja niiden ylläpito oli tuotannosta vastaavan liiketoiminnan vastuulla. Tämä vastuu ympäristöistä oli varmasti edelleen perusteltu, olihan näillä yksiköillä käytössään vuosien ajan kertynyt osaaminen ja asiantuntijuus. Haasteena oli kuitenkin ympäristöjen väliset integroinnit, esimerkiksi analytiikan tai vastaavien palveluiden toteutus, sekä kattavan tilannekuvan rakentaminen.

Hallinnan osalta selvityksessä havaittiin, että tietoisuus sekä tiedonvaihto IT- ja OT-ympäristöjen hallinnasta vastaavien tahojen välillä oli laajasti puutteellista. Kokonaiskyberturvallisuuden tilannekuvan tuottamiseksi vaaditaan myös OT-puolen tilanteen ja valvonnan ymmärtämistä. OT-järjestelmien hallinta tulisi integroida myös organisaation yleisiin prosesseihin, kuten omaisuuden-, haavoittuvuuksien sekä uhkienhallintaan. Selvityksen perusteella OT-ympäristöissä saattoi esimerkiksi esiintyä vanhoja käyttöjärjestelmiä, joiden kohdalla vaadittiin haavoittuvuuksien hallinnan osaamista.

Toisin kuin edellisessä, vuosina 2019–20 toteutetussa selvityksessä, tässä selvityksessä ei tarkasteltu tuotannollisten ympäristöjen eli ns. OT-ympäristöjen (Operational Technology) hallinnan tilaa erillisenä osana selvitystyötä. Tällä selvityskierroksella OT-ympäristöihin liittyvät tarkemmat havainnot nostettiin esiin toimialaraportoinnissa.

4.9 Hajonta

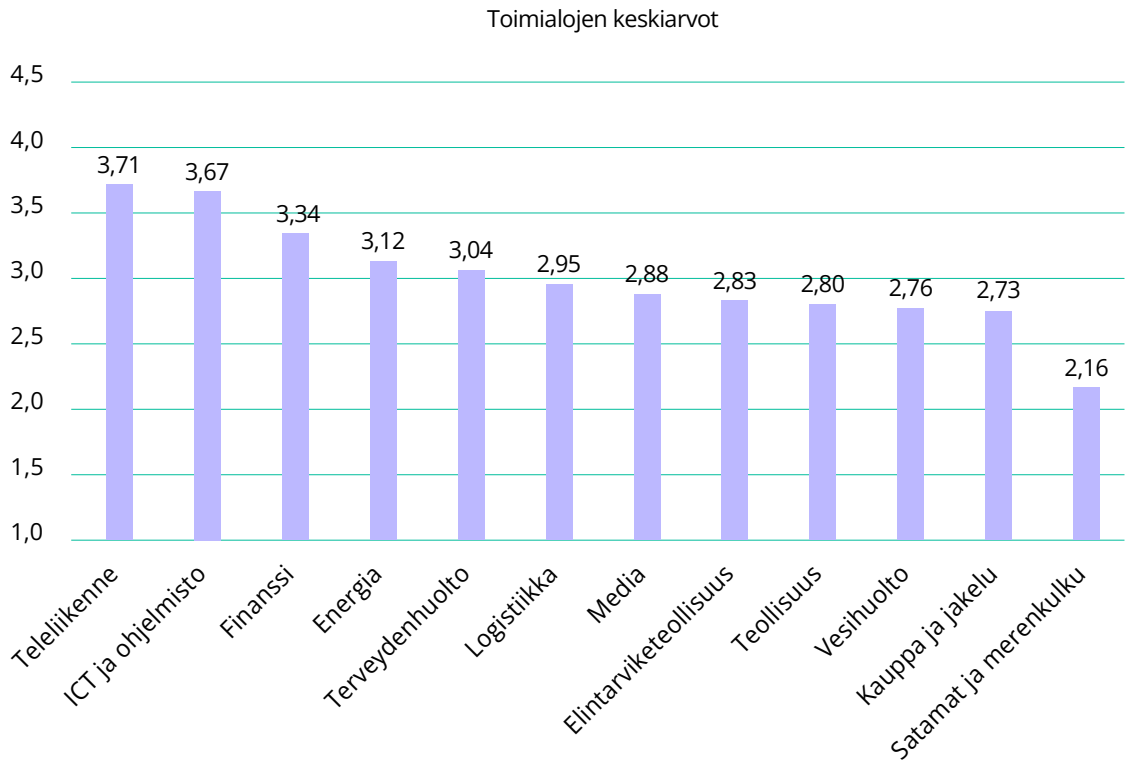
Useat toimialat näyttäytyivät selvityksessä kypsyystasojen osalta melko jakautuneina tai hyvin jakautuneina. Suurin toimialan matalimman ja korkeimman kypsyystuloksen välinen ero, eli vaihteluväli, oli 2,25 Elintarviketeollisuudessa. Pienin vaihteluväli taas oli Teleliikenteessä, jossa ero oli 1,06. Jos taas tarkastellaan sitä, millä toimialalla 50 % vastauksista sijoittui pienimmälle alueelle, ICT- ja ohjelmisto näyttäytyi tasaisimpana. Tarkemmin hajonta on kuvattu ja visuaalisesti esitetty luvussa 5.1.3.

Hajonnasta vedettyjen päätelmien kanssa oltiin tässä selvityksessä hyvin varovaisia muutaman eri muuttujan takia. Vaikka otannoissa pyrittiin mahdollisimman hyvään kattavuuteen, oli mahdollista, että selvityksen ulkopuolelle on jäänyt enemmän keskiarvoista merkittävästi poikkeavia toimijoita. Toiseksi toimialojen otannat vaihtelivat kooltaan kahdeksan ja kuudentoista osallistujan välillä, joten yksittäisten poikkeavien tulosten painoarvo toimialan keskiarvoon vaihteli aloittain.

Pienempi hajonta vaikutti olevan sellaisilla toimialoilla, joiden kyberturvallisuuden hallintaan vaikutti jokin yhteinen vaatimus tai lainalaisuus, ja jonka toimijat olivat jollain tapaa samanlaisia. Esimerkiksi Teleliikenteen yritykset toimivat pitkälti samankaltaisilla liiketoiminta-alueilla ja olivat pitkälti samojen lakisääteisten velvoitteiden alla. Toisessa päässä kypsyysasteikkoa vesihuoltoalan hajonta oli keskittynyt melko pienelle alueelle. Vesihuoltoalan kypsyystaso ei ollut korkea, mutta organisaatiot olivat samanlaisia toiminta-alueesta riippumatta. Lisäksi lähes kaikki olivat kaupunkien omistuksessa, jotka olivat myös usein merkittävimpiä IT-palveluntarjoajia. Näistä olosuhteista johtuen vesihuoltoalan toimijat kohtasivat samankaltaisia haasteita ja olivat kypsyydessään melko tasaisia. Kaksi toimialaa, joita koskettivat Teleliikenteen tavoin lainsäädännön vaatimukset, olivat Terveydenhuolto ja Finanssi. Ne olivat kuitenkin hieman enemmän jakautuneita, jonka merkittävimpänä syynä oli todennäköisesti erot pankki- ja vakuutustoimijoiden välillä sekä terveydenhuoltoalan otanta, joka koostui hyvin erilaisista toimijoista.

Suurimmat hajonnat taas nähtiin Elintarviketeollisuudessa ja Teollisuudessa, joiden otantoihin kuului merkittävän erilaisia yrityksiä erilaisine toimintaympäristöineen. Käytännössä oli mahdollista, että millä tahansa toimialalla olisi enemmän joko matalan tai korkean tason toimijoita, koska tämän selvityksen otannat olivat rajalliset. Verkottuneessa yhteiskunnassa tämä voi potentiaalisesti aiheuttaa riskikeskittymiä, joiden ketjuvaikutukset olisivat merkittäviä.

5 Kyberturvallisuuden tilannekuva vuonna 2022



Kuva 1: Toimialavertailu

5.1 Toimiala-analyysi

Toimialojen kypsyystasojen perusteella valtaosa selvityksessä tutkituista toimialoista oli vähintään kelvollisella kyberturvallisuuden tasolla. Mikäli hyvän perustason kypsyytenä pidettiin kypsyystasoa kolme, sen yli tai hieman alle osuu 11 toimialaa 12:sta. Näistä heikoin toimiala jäi hyvän perustason kypsyydestä 0,27 mittayksikköä. On kuitenkin tärkeä muistaa, että pelkkä keskiarvon tarkastelu ja siitä johtopäätösten vetäminen voi johtaa harhaan, jonka vuoksi toimialojen hajonta on esitetty luvussa 5.1.3.

Vahvasti säännellyt ja jo pitkään kyberrikollisuuden kohteena olevat alat Teleliikenne, ICT ja ohjelmisto sekä Finanssi eroittuivat selvästi kypsyyden osalta. Kaikki nämä alat olivat hyötyneet regulaation vaatimasta kehityksestä ja selvityksen perusteella ne kykenivät kehittämään kyberturvallisuutta ja kontrolleja liiketoiminta- ja riskilähtöisesti. Energia ja Terveydenhuolto ylittivät keskiarvokypsyydessä myös hyvän perustason kypsyyden kolme. Näiden alojen osalta uhka- ja riskitason vaikutus arvioitiin kuitenkin niin merkittäväksi, että alojen tulee tulevaisuudessa kehittää kypsyyttään sopeutuakseen kasvavan uhka- ja riskikentän aiheuttamiin haasteisiin.

Hieman hyvän perustason kypsyyden alle jäi kuusi toimialaa (Logistiikka, Media, Elintarviketeollisuus, Teollisuus, Vesihuolto sekä Kauppa ja jakelu). Ne olivat lähellä kelvollista tasoa, mutta vaativat kehitystä vastatakseen niihin kohdistuvaan uhka- ja riskitasoon. Alojen tavoitteiden arvioinnissa ja tavoitekypsyyden määrittelemisessä tulee kuitenkin katsoa tarkemmin kunkin alan erityispiirteitä. Keskiarvokypsyydellä mitattuna Satamat ja merenkulku jäi toimialana merkittävästi heikommaksi kuin muut toimialat. Tämän alan osalta onkin tärkeää kartoittaa ja toteuttaa pikaisesti toimenpiteitä kypsyyden kehittämiseksi.

Toimiala	Keskiarvokypsyys	Riski/uhkatason vaikutus	Arvo kyvykkyydestä vastata uhka/riskitasoon
Teleliikenne	**3,71**	Nouseva	Teleliikenneala osoittaa vahvaa kypsyystasoa ja kykenee varautumisen kautta vastaamaan toimialan riski- ja uhkakenttään.
ICT ja Ohjelmisto	**3,67**	Nouseva	ICT- ja ohjelmistoalan hyvä kypsyystaso ja riskitietoisuus tuottaa nykyisellään kyvyn vastata uhkiin.
Finanssi	**3,34**	Nouseva	Finanssiala kykenee vahvan kypsyystason ansiosta vastaamaan nykyiseen riski/uhkatilanteeseen.
Energia	**3,12**	Nouseva	Energia-alan kypsyystaso on yleisesti hyvä. Vahva varautumiskulttuuri edistää kyberturvallisuutta. Alaan kohdistuvat uhkat ovat niin merkittäviä, että yritysten oma varautuminen ei välttämättä riitä.
Terveydenhuolto	**3,04**	Nouseva	Toimialalla tietosuojakontrollit ja toimenpiteet ovat jo regulaationkin johdosta määrämuotoisesti hoidettu, mutta kyberturvallisuus vaatii usean toimijan osalta aiempaa järjestelmällisempiä toimenpiteitä.
Logistiikka	**2,95**	Nouseva	Ala on jatkuvasti kehittyvä, altis kilpailulle ja herkkä toimitusketjussa tapahtuville muutoksille, jolloin kyberturvallisuuden kokonaisvaltaiseen hallintaan tulee kiinnittää erityistä huomiota.

Toimiala	Keskiarvokypsyys	Riski/uhkatason vaikutus	Arvo kyvykkyydestä vastata uhka/riskitasoon
Media	**2,88**	Neutraali	Media-alan kehittynyt kypsyystaso tukee alan kykyä vastata uhkiin ja hallita riskejä. Alan asema keskeisenä kohteena sekä valtiotason vaikuttamiselle että rikollisille nostaa riskitasoa, jonka myötä riskilähtöinen kehitys on edelleen tarpeen.
Elintarviketeollisuus	**2,83**	Neutraali	Elintarviketeollisuusalan nykytilanne vaatii kehittämistä uhka- ja riskitilanteeseen vastaamiseksi.
Teollisuus	**2,80**	Neutraali	Teollisuuden hajanainen kypsyystilanne tekee varautumistilanteiden arvioinnin haastavaksi. Kypsyystaso on alle hyvän perustason, jolloin vastaaminen uhkiin ei ole kattavaa.
Vesihuolto	**2,76**	Nouseva	Vesihuoltotoimialan kokonaiskypsyys jää kypsyydessään vajaaksi hyvästä perustasosta, keskeinen rooli yhteiskunnan toimivuudessa vaatii investointeja myös kyberturvallisuuteen.
Kauppa ja jakelu	**2,73**	Neutraali	Kaupan ja jakelun toimialan kokonaiskypsyys jää hyvän perustason alle ja alan varautuminen kyberuhkiin ei ole kattavaa. Erityisesti suuri hajonta kypsyystasoissa voi indikoida riskikeskittymästä.
Satamat ja merenkulku	**2,16**	Neutraali	Satamat ja merenkulun toimialan kypsyystaso on matala ja vaatii merkittäviä toimenpiteitä.

Taulukko 1: Toimialojen kypsyys ja riskitason vaikutus siihen

Kypsyystason kehittämisen osalta on muistettava myös, että riski- ja uhkatilanne muuttuu ajan saatossa ja uhkatoimijat kehittävät omia kyvykkyyksiä sekä uusia hyökkäystapoja jatkuvasti. Tällöin kyberturvallisuuden jatkuva kehittäminen on keskeistä hyvän turva- ja suojautumistason ylläpitämiseksi. Jatkuvan kehityksen toteuttaminen on tärkeää nykyisestä kypsyydestä riippumatta. Vallalla olevat uhka- ja riskitilanteet arvioitiin vaikutuksiltaan suuriksi, jolloin niiden vaikutukset toimialojen varautumisen arviointiin määritettiin joko nousevaksi tai neutraaliksi.

Selvityksen tuloksista ei voitu suoraan vetää johtopäätöksiä organisaatiokoon vaikutuksesta kypsyystasoon. Vaikka organisaation investointikyky johti useimmin kyberturvallisuuden kypsyyden korkeampaan tasoon, organisaation kokoa tai liikevaihtoa tärkeämpi tekijä oli turvallisuusorientoituneisuus eli se, miten korkealla prioriteetilla organisaation johto näki kyberturvallisuuden ja oli valmis allokoimaan siihen resursseja. Pienillä organisaatioilla tai uudemman sukupolven yrityksillä oli etuna se, että kypsyyttä merkittävästi nostavat hallinnolliset toimenpiteet olivat helpompia jalkauttaa. Suuremmilla, monikansallisilla yrityksillä kehityksen tiellä olivat organisaation sisäiset epäjohdonmukaisuudet ja kehitystoimenpiteiden seurannan hankaluus. Toisaalta suurilla ja vakavaraisilla yrityksillä oli tyypillisesti enemmän investointikyvykkyyttä ja resursseja, jotka mahdollistavat esimerkiksi kyberturvallisuuteen liittyvän teknologian käytön ja kyberturvallisuushenkilöstön palkkauksen.

5.1.1 Korkeamman kypsyystason toimialoja yhdistävät asiat

Korkeamman kypsyystason toimialoilla kyberturvallisuustoiminta oli useammin liiketoiminta- ja riskilähtöistä. Kyberturvallisuuden tavoitteet tukivat liiketoiminnan strategisten tavoitteiden saavuttamista, eivätkä liiketoiminnan ja kyberturvallisuuden suunnittelu olleet liian erillään toisistaan. Kyberturvallisuuden hallinta ja tavoitteiden asettaminen oli lisäksi riskilähtöistä, eli päätöksien tukena käytettiin kyberriskien analysoinnin havaintoja ja arvioitiin niiden aiheuttamaa potentiaalista vaaraa liiketoiminnan tavoitteiden saavuttamiselle. Osalla korkeamman tason toimialoista riskienhallintaa ohjasi joko lainsäädäntö (esim. Finanssiala) tai käytössä olevat standardit ja viitekehykset (esim. ISO 27001), joita pidettiin tietyissä määrin hyvän perustason taustalla.

Lainsäädännön ja muiden asetusten asettamilla vaatimuksilla oli kiistämätön osa kypsimpien toimialojen kyberturvallisuuden hallinnassa. Regulaation asettamien vaatimusten täyttäminen takasi tietyn perustason, mutta kypsän ja todella kypsän tason arvioihin ei selvityksessä riittänyt vaatimustenmukaisuus, jos toimintaa ei pyritty kehittämään suhteessa vallitseviin riskeihin. Vastaavasti kyberturvallisuuden yleisiin standardeihin ja viitekehyksiin pohjautuvien johtamisjärjestelmien hyödyntäminen oli yleisempää korkeammalla kypsyystasolla. Useimmin kyberturvallisuuden hallinnan taustalla olivat ISO-standardit, NIST-viitekehys ja Katakri-kriteeristö.

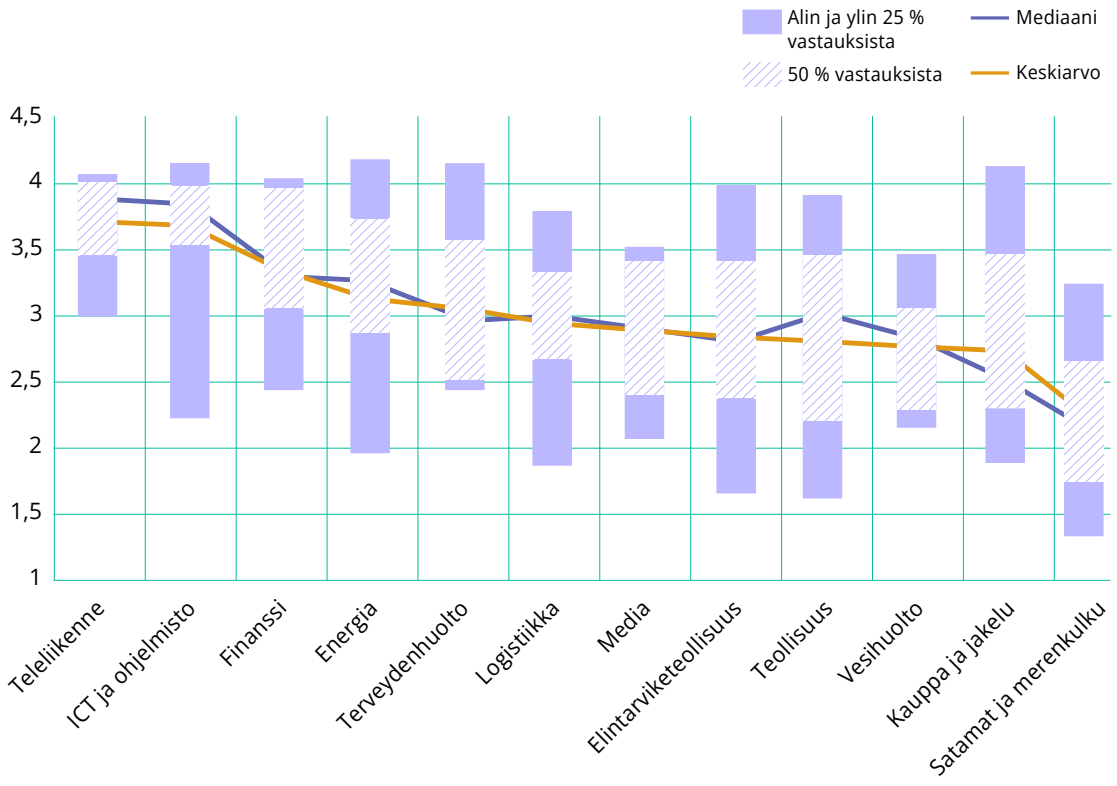
Korkeampien kypsyystasojen toimijat olivat liiketoimintalähtöisyyden ansiosta useammin onnistuneet kommunikoimaan kyberturvallisuuden merkityksen organisaation ylimmälle johdolle ja näin varmistaneet johdon tuen kehityshankkeille. Johdon tuella havaittiin olevan korrelaatio kyberturvallisuuden budjetoinnin ja investointien kanssa. Johdon tuki oli kypsimmissä organisaatioissa varmistettu muun muassa kyberturvallisuuden kehittämisohjelman hyväksyttämisellä, tilannekuvan säännöllisellä jakamisella sekä jatkuvuusharjoituksiin osallistumalla.

5.1.2 Matalamman kypsyystason toimialoja yhdistävät asiat

Matalamman kypsyystasojen toimialoja yhdistäväksi tekijäksi havaittiin kyberturvallisuuden strategisen suunnittelun ja hallinnan puutteet. Matalamman kypsyystason organisaatiot harvemmin asettivat pitkän aikavälin riskilähtöisiä suunnitelmia kyberturvallisuuden kypsyystason kestävän kehityksen tueksi. Kehitys oli matalammilla kypsyystasoilla useammin reaktiivista eli kehitys tapahtui vastauksena kriittiseksi nousseisiin uhkiin tai realisoituneisiin riskeihin. Matalammilla tasoilla kyberturvallisuuden johtamisjärjestelmän puuttuminen oli myös yleisempää kuin korkeamman kypsyystason toimialoilla. Tällöin kypsyystasoa laskivat muun muassa prosessien henkilösidonnaisuus, dokumentoinnin puutteet ja toistettavuuden haasteet.

Ennakoivan kyberturvallisuuden kehittämisen haasteista kertoi myös kyberriskienhallinnan heikompi taso. Riskienhallintakäytäntöjä oli harvemmin määritelty ja organisaatiot olivat harvemmin tunnistaneet toimintaa uhkaavat kyberriskit. Vaikka joillain toimialoilla liiketoimintariskien hallinta oli kyberriskejä aktiivisempaa, tyypillisintä oli, että riskikulttuuri oli kokonaisuudessaan heikolla tasolla. Matalamman kypsyystason toimialoilla oli esimerkiksi toistuvaa se, ettei organisaation johto ollut tietoinen kriittisimmistä kyberriskeistä.

Matalilla toimialoilla uhkatiedon kerääminen ja uhkien torjunta olivat riskienhallintaa kypsemmällä tasolla. Tyypillisesti uhkatiedon keräämisessä ja jakamisessa esimerkiksi sidosryhmien kesken oltiin hyvin aktiivisia, mutta tietoa ei hyödynnetty kyberriskien arvioinnissa tai tilannekuvan muodostamisessa. Toisin sanoen uhkatiedon vaikuttavuutta omalle toiminnalle ei kyetty tunnistamaan.



Kuva 2: Toimialayritysten hajonta[2]

5.1.3 Toimialojen hajonta

Toimialojen hajontaa voitiin tarkastella kahdesta näkökulmasta; kuinka suuri toimialan vaihteluväli, eli matalimman ja korkeimman tuloksen välinen ero oli, tai kuinka suurelle alueelle 50 % tuloksista sijoittui. Vaihteluväli osoitti sen, että lähes jokaiselta toimialalta löytyy matalan ja korkean kypsyyden toimijoita, kun taas 50 % jakautumista tarkastelemalla voitiin arvioida sitä, miten tasaisena toimialan kypsyyttä voitiin pitää. Neljällä toimialalla (Teleliikenne-, Logistiikka-, Vesihuolto- sekä ICT- ja ohjelmistoalalla) 50 % vastauksista jakautui alle yhden tason väliselle alueelle.

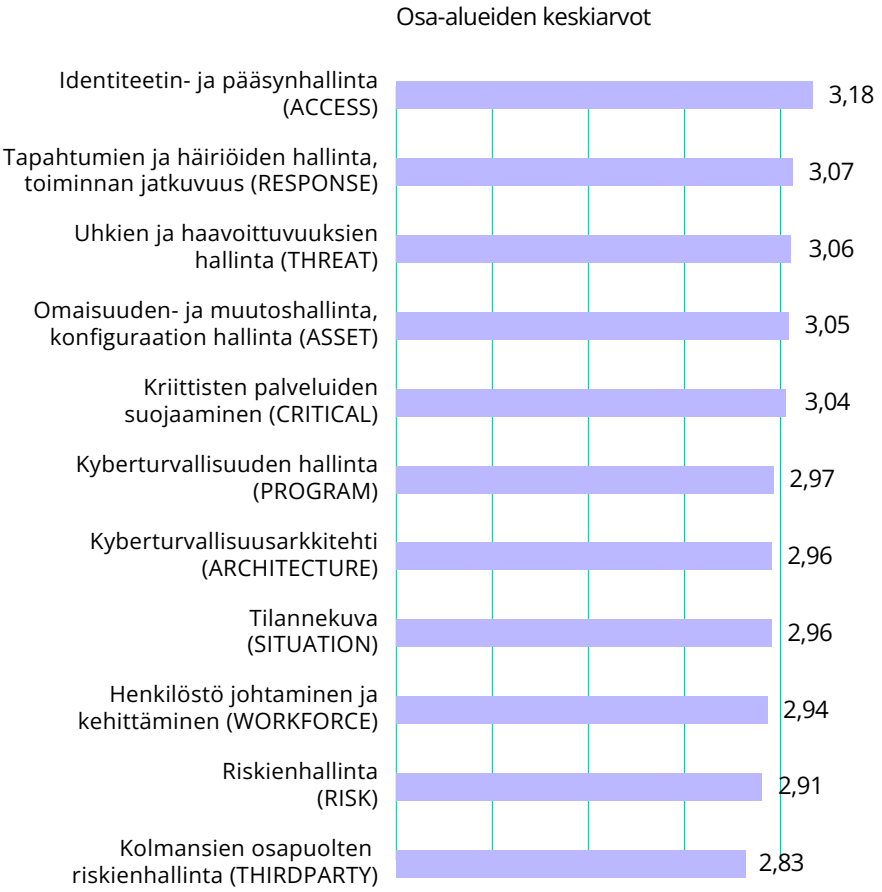
Toimialojen jakaumaa tarkastellessa voitiin havaita, että pienin vaihteluväli oli Teleliikennealalla ja pienin 50 % vastausten keskittymä oli ICT- ja ohjelmistoalalla. Vaikka ICT-alan 50 % tulosten hajonta oli pienempi ja sen ylin 25 % oli korkeampi, Teleliikenneala sijoittui toimialalistauksen kärkeen. Tähän vaikutti se, että Teleliikennealan 50 % jakautui asteikolla hieman korkeammalle ja ICT-alan keskiarvoa veti alaspäin alin 25 %. ICT- ja ohjelmisto alan otanta oli kuitenkin yli puolet Teleliikennettä suurempi, jonka valossa ICT-alan hyvä kypsyysarvio vaikutti alinta 25 % lukuun ottamatta kertovan alan tasaisen vahvasta kyberturvallisuuden nykytilasta.

[2]Kuvan ylin ja alin viiva osoittaa tulosten vaihteluvälin. Laatikon sisälle sijoittuu 50 % tuloksista. Ylimpään neljännekseen sijoittuvat tulokset näkyvät kuvaajassa laatikon ja ylimmän viivan välissä. Alimpaan neljännekseen sijoittuvat tulokset näkyvät laatikon ja alimman viivan välissä. Ylin viiva puuttuu, mikäli ylempi neljännes saa yhtä suuren arvon kuin mitä laatikon sisällä oleva maksimiarvo on. Vastaavasti alin viiva puuttuu, mikäli alempi neljännes on yhtä pieni kuin laatikon pienin arvo. Vaakatasossa oleva viiva kuvaa keskilukua eli mediaania ja rasti keskiarvoa.

Suurin hajonta oli Elintarviketeollisuusalalla (2,25) ja toiseksi suurimmat Kaupan ja jakelun sekä Energian aloilla (2,19). Näillä aloilla hajontaan vaikuttivat ainakin toimialan yritysten merkittävästi eriävät investointikyvykkyydet ja resurssit kyberturvallisuudelle. Vaikka koko selvityksen osalta havaittiin, että pienemmät organisaatiot kykenevät pienemmistä budjeteista huolimatta hyvään kypsyystasoon ja hyötyvät esimerkiksi organisaatioiden ketteryydestä, hajonnan taustalla vaikuttavat organisaatioiden koko, investointikyky, alueellisuus ja työntekijöiden määrä. Suuret monikansalliset yritykset pystyivät lähtökohtaisesti investoimaan kyberturvallisuuden kehittämiseen ja henkilöstöön enemmän, mutta poikkeuksia löytyi eikä yrityksen kokoa voitu pitää selvänä indikaattorina kypsyydestä. Yhtenä kypsyyteen vaikuttavana tekijänä havaittiin se, miten todennäköisenä kyberhyökkäyksen kohteena organisaatiot näkivät itsensä. Tämän johdosta esimerkiksi Energia-alalla suuremmalla maantieteellisellä alueella toimivat organisaatiot olivat investoineet kyberturvallisuuteen paikkakuntakohtaisia toimijoita enemmän.

Kuva 2 osoittaa hajonnan lisäksi keskiluvun eli mediaanin, jonka mukainen toimialalistaus erosi keskiarvolistauksesta muutaman toimialan osalta. Koska toimialojen yritysotannat vaihtelivat kooltaan, yksittäisten osallistujien kypsyystasoilla oli vaihtelevan suuria vaikutuksia toimialojen keskiarvoihin. Mediaaneja tarkastellessa Teollisuus sijoittui viidennelle sijalle, Logistiikka kuudennelle sijalle ja Terveydenhuolto seitsemännelle sijalle. Sen sijaan keskiarvovertailussa Teollisuus sijoittui neljänneksi viimeiseksi eli yhdeksänneksi, koska toimialan alin 25 % veti keskiarvoa merkittävästi alaspäin. Teollisuusalan mediaanin ja keskiarvon suhteessa isompaan eroon vaikuttaa Teollisuusalan otanta, joka on jopa kaksinkertainen pienimpiin toimialoihin verrattuna.

Yleisesti hajontakuvaajaa ja lukuja tarkastellessa oli hyvä ottaa huomioon, että toimialojen otannat eivät olleet samankokoisia ja on mahdollista, että toimialojen otannan ulkopuolelle jäi enemmän matalan tai korkean tason toimijoita.

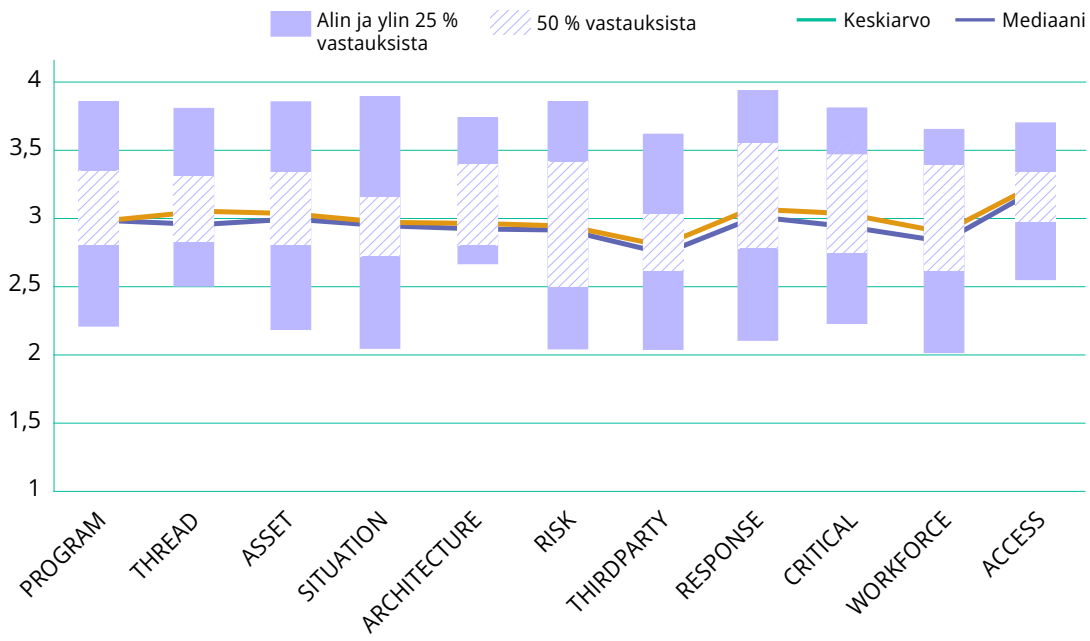


Kuva 3: Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen Kybermittarin mukaisten osa-alueiden tulokset

5.1.4 Selvityksen osa-alueittaiset tulokset

Kaikkia toimialoja yhdistävänä heikkoutena voitiin pitää kolmansien osapuolten riskienhallintaa, joka jää osa-alueista heikoimmaksi koko selvityksen skaalassa. Haasteita oli toimialasta riippuen joko omien pääasiallisten kumppaneiden hallinnassa tai toimitusketjujen kokonaisuuden ymmärtämisessä. Esimerkiksi Vesihuoltoalalla kriittiseksi kehityskohteeksi tunnistettiin kommunikaatio- ja vastuunjakohaasteet kuntien ja kaupunkien kanssa, jotka olivat usein vesilaitosten omistajia sekä suurimpia IT-palveluntuottajia. Usein toistuva haaste läpi toimialojen liittyi juuri epäselvyyksiin omien ja toimittajien vastuiden välillä. ICT- ja ohjelmistoalalla taas suorien kumppaneiden hallinta oli useammin strukturoitua, mutta alan toimijat kokivat kompleksisten toimitusketjujen kokonaisvaltaisen hallinnan haastavaksi. Tämän myötä toimitusketjujen kautta realisoituvia kyberuhkia pidettiin yhtenä kriittisimmistä riskeistä monella toimialalla, koska organisaatiot tiedostavat, ettei kaikkia riippuvuuksia ja riskiskenaarioita oltu tunnistettu.

Lähes kaikkia toimialoja yhdistävänä vahvuutena taas voitiin pitää identiteetin- ja pääsynhallintaa (ACCESS), jossa 75 % toimialoista sijoittuu hyvälle perustasolle kolme tai sen yli. Identiteetin- ja pääsynhallinnan (IAM) yleisin vahvuus oli fyysinen pääsynhallinta, joka oli keskimäärin hyvin hoidettu myös matalan kypsyystason toimialoilla. Fyysisen turvallisuuden ulottuvuudet olivat perinteisesti ymmärretty kyberturvallisuutta aiemmin ja paremmin, jonka johdosta prosessit, kontrollit ja vastuut olivat tarkemmin määriteltyjä. Lisäksi identiteetin- ja pääsynhallinnassa pärjäsivät myös pienet organisaatiot, joiden kypsyystaso oli muuten matala. Henkilöstömääriltään pienissä organisaatioissa identiteettien ja pääsyoikeuksien ylläpito oli realistista toteuttaa manuaalisesti, kun toisaalta resursseiltaan vahvemmilla organisaatioilla keskitetty IAM-järjestelmä oli usein investointiprioriteettien kärjessä.



Kuva 4: Osa-alueiden hajonta[3]

Suurin vaihteluväli oli tapahtumien ja häiriöiden ja toiminnan jatkuvuuden (RESPONSE) osa-alueessa. Merkittävää hajontaa selitti osittain se, että esimerkiksi Teleliikennealalla varautuminen oli yritysten lakisääteinen velvoite ja ICT- sekä ohjelmistoalalla palveluiden häiriöt tuottaisivat alan toimijoille merkittäviä kustannuksia mm. asiakkaiden korvausten muodossa. Toisessa päässä oli toimialoja, joiden jatkuvuussuunnittelu on tähän mennessä keskittynyt tuotannon jatkuvuuden varmistamiseen, eikä kyberturvallisuus ole ollut ajattelun keskiössä. Osittain osa-alueen haasteet nivoutuivat aiemmin käsiteltyihin epäselvyyksiin organisaatioiden ja toimittajien välisissä vastuunjaoissa. Selvityksessä ilmeni esimerkiksi, että jotkin toimijat tukeutuivat kyberhäiriöiden hallinnassa täysin kumppaniin, eli useimmiten tietoturvavalvomopalveluntarjoajaan (SOC, Security Operations Centre) ja olivat jättäneet laatimatta omia, organisaation sisäisiä jatkuvuussuunnitelmia. Useimmiten SOC-palvelut olivat kuitenkin ulkoistettu, jolloin tietyt teknisen häiriönhallinnan tehtävät olivat sopimuksellisesti kumppanin vastuulla, mutta muita toimia, kuten mahdollista kommunikointia asiakkaiden tai sidosryhmien suuntaan kyberhäiriötilanteessa ei ollut suunnitelmissa.

Selvityksessä havaittiin, että monella kypsemmän tason toimijalla oli käytössään joko sisäinen tai ulkoistettu SOC-palvelu ja matalamman tason toimijoillakin palvelun hankinta oli suunnitelmissa. Oman hallinnan tärkeyttä kybertilannekuvan osalta ei kuitenkaan aina ymmärretty riittävällä tasolla, joka ilmenee ylempänä kuvatusta epäselvyydestä häiriönhallinnan vastuunjakoon liittyen. Vaikka tietoturvamonitorointipalvelut olivat yleistyneet, niiden kattavuus ei välttämättä ollut riskilähtöisesti riittävä eikä ollut ymmärrystä siitä, miten asiakkaan ja toimittajan väliset vastuut olivat jaettu. Selvityksen perusteella monella organisaatiolla SOC toimi roolissa, jossa se havaitessaan tapahtumia ainoastaan välitti tiedon havainnosta asiakasorganisaatiolle selvitettäväksi. Tämä rajallinen toiminta täyttää SOC:n minimivaatimuksen, mutta siinä ei hyödynnetty kaikkia tietoturvavalvomotoiminnassa syntyviä synergioita, mm. tilannekuvan osalta.

Jos tarkastellaan hajontaa siitä näkökulmasta, minkä osa-alueen 50 % vastauksista sijoittui laajimmalle alueelle, riskienhallinta oli jakautunein. Tähän vaikuttaa aiemmin korkeamman ja matalamman kypsyystason toimialojen erityispiirteissä käsitellyt seikat, kuten sääntelyvaatimukset ja viitekehyksiin perustuvien johtamisjärjestelmien kriteerit. Kypsemmillä toimialoilla liiketoiminnan riskienhallinta oli usein hyvinkin määrämuotoista, mutta kyberriskit eivät olleet osana kokonaisuutta. Matalammilla toimialoilla organisaatioilla ei välttämättä ollut minkäänlaista riskikulttuuria. Kaikilta toimialoilta löytyi organisaatioita, joiden haasteena oli sovittaa riskienhallintamenetelmät ja kyberturvallisuuden tekninen osaaminen yhteen. Kyberturvallisuuden asiantuntijat mielsivät riskienhallinnan usein tekniseksi uhkienhallinnaksi, kun taas riskienhallintavastaavat ovat tottuneet arvioimaan riskiskenaarioita taloudellisten ja kvantitatiivisten mittareiden avulla.

[3] Kuvan ylin ja alin viiva osoittaa tulosten vaihteluvälin. Laatikon sisälle sijoittuu 50 % tuloksista. Ylimpään neljännekseen sijoittuvat tulokset näkyvät kuvaajassa laatikon ja ylimmän viivan välissä. Alimpaan neljännekseen sijoittuvat tulokset näkyvät laatikon ja alimman viivan välissä. Ylin viiva puuttuu, mikäli ylempi neljännes saa yhtä suuren arvon kuin mitä laatikon sisällä oleva maksimiarvo on. Vastaavasti alin viiva puuttuu, mikäli alempi neljännes on yhtä pieni kuin laatikon pienin arvo. Vaakatasossa oleva viiva kuvaa keskilukua eli mediaania ja rasti keskiarvoa. Jos otannassa on yksittäinen muista merkittävästi eroava arvo, sitä ei osoiteta kuvaajassa.

5.2 Vertailu 2019–2020 selvitykseen

Vuosina 2019–2020 tehtyyn selvitykseen verrattuna toimialojen tilanne oli keskimääräisesti pysynyt nykyselvityksen perusteella hyvällä perustasolla tai sen läheisyydessä (kypsyystaso kolme), vaikka organisaatioiden välillä havaittiin edellisen selvityksen tavoin merkittävää hajontaa. Selvityksiä vertaillessa on hyvä ottaa huomioon, että osallistujaotanta muuttui 2019–2020 selvityksen ja 2022 selvityksen välillä. Kypsyystason muutoksia ei voitu suoraan vertailla kypsyysarvioiden numeraalisten tulosten pohjalta, johtuen arvioinnissa hyödynnetyn Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen Kybermittarin sekä arviointikriteerien muutoksista.

Merkittävimmät yhteiset kehityskohteet edellisessä selvityksessä liittyivät huoltovarmuus näkökulmasta yhteisen tilannekuvan muodostamiseen, turvalliseen ohjelmistokehitykseen sekä henkilöstön osaamisen kehittämiseen. Liiketoiminnan näkökulmasta edellisessä selvityksessä merkittävimmät kehityskohteet olivat yrityksen kyberturvallisuusstrategia, kyberturvallisuusarkkitehtuuri sekä tekninen jäljitettävyys. Vaikka kiihtynyt digitalisaatio, koronapandemia sekä geopoliittisen tilanteen muutokset vauhdittivat organisaatioiden tarvetta huomioida kyberturvallisuus aiempaa kokonaisvaltaisemmin, merkittävimmät kehityskohteet säilyivät pitkälti samoina. Syitä sille, miksi tilanne oli kehityskohteiden osalta pysynyt samanlaisena, on useita. Sillä numeraalisia tuloksia ei ollut mielekästä vertailla arviointiasteikon muutoksien takia, paneuduimme tässä tekstissä laadullisen analyysin vertailuun. Huomionarvoista oli, että yrityskohtaiset merkittävimmät kehityskohteet saattoivat hajonnan vuoksi vaihdella suuresti.

Edellisessä selvityksessä toimialojen sekä yritysten tuloksissa esiintyi tarve yhtenäiselle kyberturvallisuuden tilannekuvan kehittämiselle. Toisaalta yhteisen kansallisen ja toimialakohtaisen tilannekuvan muodostamiseen oli jo aiemmin tehty investointeja, joista esimerkkeinä ISAC- tiedonvaihtoryhmät sekä HAVARO-toiminta. Vaikka tässä selvityksessä havaittiin, että usea toimiala oli aktiivinen sidosryhmätoiminnassa ja etenkin uhkatiedon jakamisessa, eivät nämä toiminteet heijastelleet suoraan organisaatioiden kypsyysarvioihin. Selvityksen perusteella mahdolliset uhkat ja riskit tiedostettiin nykytilassa aiempaa paremmin, mutta saatujen tietojen hyödyntäminen jäi usein vajaaksi osaamisen, tekijöiden tai ajanpuutteen vuoksi.

Turvallinen ohjelmistokehitys oli mainittu edellisessä selvityksessä jokaisen toimialan yhtenä tärkeimmistä kehityskohteista. Edellisessä selvityksessä havaittu tarve yhteisille, ohjelmistokehityksen tietoturvallisuutta varmentaville minimivaatimus suosituksille eli yhä. Nykyselvityksen perusteella kypsyystasoja laski usealla toimialalla osaamisen ja ajan puutteen lisäksi myös puutteet elinkaarenhallinnassa. Edellä mainitut näkyivät niin tilanteissa, joissa ohjelmistokehitystä tehdään organisaation itsensä toimesta kuin myös silloin, kun organisaatio toimii palvelun ostajana. Toimenpiteet ohjelmisto- ja sovelluskehityksen sekä hankintojen turvallisuuden vaatimiseksi ja varmistamiseksi tuottivat haasteita läpi toimialojen. Aiemmin mainittujen lisäksi yhtenä merkittävänä syynä turvallisuuden varmistamisen puutteille oli myös luottamus, joka etenkin suurten ja tunnettujen palveluntarjoajien suuntaan vaikutti olevan tekijä, jonka varaan lasketaan paljon.

Elinkaarenhallinnan haasteet näkyivät nykyselvityksen usealla eri osa-alueella. Yksi niistä oli henkilöstön ja johtaminen kehittäminen, jossa yhtäläisyyksiä aiemmin tehtyyn selvitykseen havaittiin osaamisen jatkuvan kehittämisen puutteissa henkilöstön työsuhteen aikana. Henkilöstön yleisen kyberturvallisuustietoisuuden tunnistettiin kasvaneen viimeisen muutaman vuoden aikana, vaikka nykyselvityksen tulokset kertoivat jatkuneista haasteista toteuttaa koko työsuhteen elinkaaren aikaista henkilöstön kehittämistä, koulutuksien painottuessa työsuhteen alkupäähän. Kyberturvallisuusasiantuntijoiden vaihtuvuus- ja saatavuushaasteet vaikuttivat edelleen organisaatioiden jatkuvuuteen ja resilienssiin. Toisaalta suuressa kuvassa havaittiin muutoksia organisaatioiden liiketoiminta-johdon ja kyberturvavastaavien näkökulmien eron kaventumisessa. Yhä useamman organisaation johto käsitteli kyberturvallisuuteen liittyviä aiheita ja oli ottanut riskipainotteisemman lähestymistavan johtamiseen, jossa kyberturvallisuus huomioitiin aiempaa kattavammin. Edellisessä selvityksessä havaittiin, että erittäin useissa organisaatioissa ylin johto ei käsittellyt kyberturvallisuusasioita säännöllisesti. Suurin vaikuttaja muutoksiin oli vuoden sisäiset geopoliittiset tapahtumat, joiden myötä organisaatiot ymmärsivät laajamittaisen valtiollisen kybervaikuttamisen uhkan, jonka kohteena saattavat olla suoraan tai välillisesti kaikki huoltovarmuuskriittisen ketjun toimijat.

Vaikka välillisesti organisaation toimintaa koettelevien kyberuhkien mahdollisuus oli tunnistettu, oli valtaosalla toimijoista vielä paljon parannettavaa kolmansiin osapuoliin liittyvässä riskienhallinnassa. Edellisessä selvityksessä toimitusketjun ja ulkoisten riippuvuuksien hallinnan koettiin olevan hyvällä tasolla, mutta hajontaa toimialojen välillä havaittiin riippuvuusriskienhallinnassa, joita vain neljännes edellisen selvityksen organisaatioista hallitsi hyvin. Kolmansien osapuolten riskienhallinta oli tämän selvityksen yksi tärkeimmistä havaituista kehityskohteista. Tämän selvityksen perusteella voitiin katsoa, että kolmasosa toimialoista hallitsi toimitusketjujaan, sidonnaisuuksiaan ja riippuvuuksia hyvän perustason saavuttavalla tavalla, vaikka myös kyseiseen

kolmannekseen kuuluvien toimialojen keskuudessa havaittiin haasteita kompleksisten toimitusketjujen hallinnassa sekä riippuvuuksien kattavassa tunnistamisessa. Pääasiallisten kumppaneiden osalta nykyselvityksessä merkittäväksi riskivektoriksi nousi pitkäaikaiset sopimukset ja kumppanuussuhteet, joiden seuranta saattaa pitkän yhteistyön luoman luottamuksen vuoksi jäädä puutteelliseksi. Yhteisenä haasteena olivat monimutkaistuneet toimittaja- ja alihankintaketjut, joista usein tunnistetaan ja hallitaan ensimmäinen linkki, kokonaisvaltaisen riskienhallinnan jäädessä usein vajaaksi. Yleisesti kyberriskien hallinnan voitiin todeta olevan usealla toimialalla asia, jota ei nykytilassa otettu tarpeeksi kattavasti huomioon osana liiketoiminnan muuta riskienhallintaa. Riskienhallinta oli tässä selvityksessä toiseksi matalimman keskiarvon saanut osa-alue. Edellisen selvityksen tapaan osa-alueessa organisaatioiden välillä havaittiin kuitenkin merkittävää hajontaa.

Yksi tämän selvityksen havainnoista liittyi IT- ja OT-ympäristöjen kyberturvallisuuden eri tasoiseen hallintaan, jonka osalta toiminnan yhdenmukaistamisessa ei edelliseen selvitykseen verrattuna nähty juurikaan edistystä. OT-puolen heikko tai jopa olematon näkyvyys aiheutti edellisessä selvityksessä huomattavan eron ympäristöjen kyberturvallisuuden kypsyyksissä. Digitalisaation myötä esille noussut yhteinen liiketoimintateknologian hallinta tunnistettiin jo edellisen selvityksen aikaan toiminteeksi, jonka avulla IT- ja OT- ympäristöjen synergiaa ja hallintaa pyrittiin syventämään, vaikka erityistä kehitystä ei nykyselvityksessä tästäkään huolimatta havaittu. Yksi tekijä oli myös perinteisen kyberturvallisuusorganisaation osittainen tietämättömyys OT-ympäristöjen tilanteesta, joka on seurausta hallinnan jakautumisesta eri organisaatioihin.

Numeraalisten arvioiden perusteella nykytilanne ei aiempaan selvitykseen verrattuna ollut merkittävästi muuttunut. Kuitenkin organisaatioiden kyberturvallisuuteen liittyvässä tietoisuudessa oli havaittavissa huomattavaa kehitystä. Nykyselvityksen perusteella voitiin todeta usean organisaation olevan kyberturvallisuuden osalta murroksessa, joka ohjaa tulevaisuudessa suunnittelemaan liiketoiminnan jatkuvuutta kyberturvallisuus sen keskiössä. Tiivistettynä nykytilanne kyberturvallisuuden osalta nähtiin selkeänä ja ymmärrys sen merkityksestä toimintavarmuuden takaajana oli jo usean organisaation kehityksen taustalla. Nyt ensiarvoisen tärkeää on varmistaa, että organisaatioita tuetaan eri tavoin viranomaistahojen toimesta. Menestymisen edellytys vaikuttaa olevan kyky investoida sekä kyberturvallisuuden kehittämiseen että osaamiseen.

6 Toimialakohtaiset yhteenvedot

6.1 Teleliikenne

Toimialalle ominaista

Toimiala on olennainen osa kriittistä infrastruktuuria ja keskeinen toimija kansallisen kyberturvallisuuden varmistamisessa. Toimiala on myös historiallisesti toiminut aktiivisesti digitaalisuuden edistämisessä ja varautumisen etulinjassa:

- Vahva regulaatio rajaa liikkumavaraa niin liiketoiminnan- kuin riskienhallinnan ratkaisuissa
- Avainasemassa muiden toimialojen digitaalisen toiminnan mahdollistajana
- Vahva yhteistyö toimialan sisällä varautumisen osalta

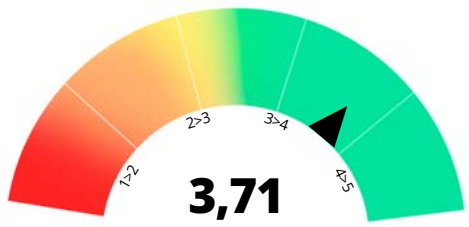
Suositukset toimialalle

Teleliikenneala osoittaa vahvaa kypsyystasoa ja kykenee varautumisen kautta vastaamaan toimialan riski- ja uhkakenttään. Alan asema keskeisenä digitaalisen kyvykkyyksien tuottajana nostaa sen houkuttelevuutta kohteena, jolloin jatkuva kehitys ja parantaminen kyberturvallisuuden osalta on ratkaisevan tärkeää.

Varautumistason kehittämiseksi nousevat seuraavat asiat esiin:

- Toimiala- ja viranomaisyhteistyön aktiivinen jatkaminen ja edelleen syventäminen
- Uhka- ja riskilähtöisen kyberturvallisuuden kehittämisen jatkaminen edelleen
- Toimitusketjujen riippuvuuksien ja kyberturvallisuuden hallinta

Toimialan kokonaiskypsyys



Toimialan vahvuudet

Toimialan vahva kokonaiskypsyys näkyy erityisesti seuraavissa osa-alueissa:

- Hyvä kypsyystaso läpi toimialan osoittaa alan varautumiskyvyn olevan korkea
- Liiketoiminta- ja riskilähtöinen kyberturvallisuuden hallinta, jolla vahva johdon tuki
- Keskeiset toiminnan turvaamisen liittyvät kyvykkyydet vahvoja kautta linjan

Toimialan riskit ja uhkat

Merkittävimmät toimialan tunnistamat riskit ja uhkat:

- Digitalisaatio ja teknologiariski, ml. pilvipalveluiden laajentuva käyttö
- Osaamisriski mm. ulkoistusten ja edelleen käytössä olevan legacy-infrastruktuurin osalta
- Kyberrikollisuuden ja -vaikuttamisen jatkuva kehittyminen ja monimuotoistuminen

Toimialan heikkoudet

Toimialan heikoimmatkin kyvykkyydet ovat yli hyvän perustaso kolmen. Kriittisimmiksi kehitystoimiksi tunnistettiin:

- Kolmansien osapuolten kyberturvallisuuden hallinta
- Vaihteleva kyvykkyys kyberturvallisuuden tilannekuvan muodostamisessa toimialayritysten välillä

Vertailu selvityksen 2019–2020 ja 2022 välillä

Vuoden 2019-20 ja 2022 selvitysten välillä Teleliikenneala on edelleen kyennyt kehittämään kypsyystasoaan. Vahvuudet edellisestä selvityksestä on kyetty säilyttämään ja erityisesti muutamia heikkouksina vuonna 19-20 mainittuja kyvykkyyksiä on parannettu, osaa merkittävästi.

Kehittyneet kyvykkyydet:

- Henkilöstön johtaminen ja kehittäminen, erityisesti kyberturvallisuushenkilöstön osaamisen kehittäminen
- Tilannekuvan kehittäminen, tietoturvavalvomo laajasti käytössä alan yrityksillä
- Omaisuudenhallinnan kehittyminen

Muut havainnot:

- Toimialan merkitys osana kansallista kyberturvallisuutta ja varautumista kohonnut geopolitiikan tapahtumien vuoksi

6.2 ICT ja ohjelmisto

Toimialalle ominaista

Toimiala olennainen toimija kansallisen digitaalisen infrastruktuurin ja kyvykkyyksien tuottamisessa, toimijuus sekä oman että asiakkaiden kyberturvallisuuden varmistamisessa.

- Kyberturvallisuus on luottamustekijä asiakastyössä, mutta hankintojen kustannusfokus jättää usein turvallisuuden vähälle huomiolle laatuvaatimuksissa
- Asiakkaiden varovaisuus ja palveluiden hankintakulttuuri hidastavat palveluiden modernisointia (esim. pilvisiirtymä ja legacy-haasteet)

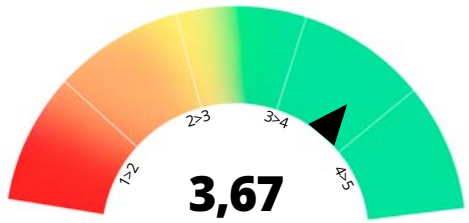
Suositukset toimialalle

ICT- ja ohjelmistoalan hyvä kypsyystaso ja riskitietoisuus tuottaa nykyisellään kyvyn vastata uhkiin. Alan asema huoltovarmuuskriittisessä kokonaisketjussa ja datan käsittelijänä kuitenkin nostaa sen houkuttelevuutta kohteena ja asettaa vaatimuksen jatkuvasta kyvykkyyksien kehittämisestä.

Kypsyystason kehittämiseksi suositellaan seuraavia:

- Toimitusketjujen sidonnaisuuksien tunnistaminen ja kumppanuuksien riskienhallinta laajemmin kuin suorien palveluntarjoajien osalta
- Toimialan sisäinen tiedonvaihto ja yhteinen jatkuvuusharjoittelu valtiollisten toimijoiden kyber- ja hybridiuhkien havaitsemisen ja torjumisen tueksi

Toimialan kokonaiskypsyys



Toimialan vahvuudet

Toimialan vahva kokonaiskypsyys näkyy erityisesti seuraavissa osa-alueissa:

- Kyberturvallisuuden kehittämisen priorisointi liiketoiminnan strategioissa, joka korreloi johdon tuen ja investointien kanssa
- ISO 27000 - tietoturvastandardiin pohjautuvien tietoturvallisuuden hallintamallien yleisyys

Toimialan riskit ja uhkat

Merkittävimmät toimialalle tunnistetut riskit ja uhkat:

- Henkilöstöön liittyvät riskit, kuten inhimilliset virheet, sisäpiiriuhkat, henkilöstön vaihtuvuus sekä osaavien kyberturvallisuusasiantuntijoiden saatavuushaasteet
- Toimitusketjuihin kohdistuvat uhkat
- Valtiollisten toimijoiden aiheuttamat kyber- ja hybridiuhkat

Toimialan heikkoudet

Toimialan hyvästä kypsyystasosta huolimatta kehityskohteiksi tunnistettiin seuraavat:

- Asiakasympäristöjen priorisointi ja sisäisten järjestelmien heikompi huomioiminen
- Legacy-järjestelmien suuri osuus sekä pilvisiirtymän hitaus johtuen epäselvyyksistä datan käsittelyyn liittyvästä regulaatiosta ja asiakkaiden varovaisuudesta

Vertailu selvityksen 2019–2020 ja 2022 välillä

ICT- ja ohjelmistoalan toimijoiden kehittyneet riskienhallinnan käytännöt ja jatkuvuusharjoittelu ovat vahvistaneet alan yritysten varautumisen tasoa. Toisaalta uhkatilanne on kehittynyt tai lähinnä konkretisoitunut, eli erilaiset, seuratut riskit ovat toteutuneet. Kypsyystaso on edelleen korkealla tasolla, mutta uhkaympäristön kehitys asettaa haasteita kaikille toimialayrityksille myös tulevaisuudessa.

Kehittyneet kyvykkyydet:

- Kyberriskienhallinta
- Kolmansien osapuolten riskienhallinta
- Käytännön jatkuvuusharjoittelu

Kyberriskienhallinnan käytännöt ja liiketoimintalähtöinen kyberturvallisuuden huomioiminen ovat selvästi kehittyneet edellisestä selvityksestä. Kolmansien osapuolten hallinta rajattuna suoriin kumppaneihin on myös parantunut, tosin kokonaisketjujen osalta havaittiin heikkouksia.

6.3 Finanssi

Toimialalle ominaista

Toimiala on osa kriittistä kansallista infrastruktuuria, joka on integroitunut osaksi Euroopan laajuisia rahoitusmarkkinoita. Sen tilannetta leimaa nopea tekninen kehitys, uudet teknologiat sekä pandemian luoma asiakasodotusten muutos.

Lisäksi varautumiseen vaikuttavat seuraavat asiat:

- Laajasti pakottavaa regulaatiota
- Pitkä historia kyberrikollisuuden kohteena
- Vahva yhteistyö toimialan sisällä

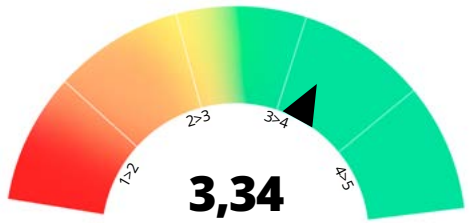
Suositukset toimialalle

Finanssitoimiala osoittaa vahvaa kypsyystasoa kautta linjan ja kykenee vastaamaan toimialan moninaiseen uhka- ja riskikenttään. Alan asema keskeisenä yhteiskunnan rahoittajana ja vakuuttajana sekä asiakasdatan hallinnoijana nostaa sen houkuttelevuutta kohteena, jolloin palveluiden jatkuva kehitys, turvaaminen ja parantaminen kyberturvallisuuden osalta on ratkaisevan tärkeää.

Kypsyystason kehittämiseksi nousevat seuraavat asiat esiin:

- Strategisen ohjauksen ja liiketoiminalähtöisyyden edelleen kehittäminen osaksi kyberturvallisuuden ohjausta
- Toimittajaketjujen tunnistamisen ja hallinnan kehittäminen
- Henkilöstön osaamisen ja tietoisuuden jatkuva kehittäminen vastaamaan kehittyvään uhkaympäristöön

Toimialan kokonaiskypsyys



Toimialan vahvuudet

Toimialan vahva kokonaiskypsyys näkyy erityisesti seuraavissa osa-alueissa:

- Vahva riskienhallinnan kulttuuri
- Kyberturvallisuuden tilannekuvan kattava kyvykkyys
- Kriittisten palveluiden ja häiriöiden hallinnan korkea taso

Toimialan riskit ja uhkat

Merkittävimmät toimialan tunnistamat riskit ja uhkat:

- Digitalisaatio ja teknologiariski, ml. pilvipalveluiden laajentuva käyttö
- Osaamisriski mm. ulkoistusten ja edelleen käytössä olevan legacy-infrastruktuurin osalta
- Kyberrikollisuuden jatkuva kehittyminen ja monimuotoistuminen

Toimialan heikkoudet

Toimialan heikoimmatkin kyvykkyydet ovat lähellä hyvän perustason kyvykkyyttä kolme. Kriittisimmiksi kehitystoimiksi tunnistettiin:

- Kolmansien osapuolten kyberturvallisuuden hallinta
- Sidonnaisuuksien laaja-alainen tunnistaminen esimerkiksi monimutkaisten alihankintaketjujen osalta

Vertailu selvityksen 2019–2020 ja 2022 välillä

Vuoden 2020 ja nykyisen selvityksen tulokset ovat säilyneet samanlaisina. Kypsyystaso on tasainen ja johdonmukainen läpi toimialan. Molemmissa selvityksissä sääntelyn vaikutus näyttäytyy selvästi kyvykkyyksien ja valmiuksien tasossa.

Erityisesti kriittisten palveluiden hallintaan liittyvät kyvykkyydet ovat olleet ja säilyneet korkealla tasolla.

Haasteina koetaan edelleen kolmansien osapuolten hallinta, laajempien riippuvuuksien tunnistaminen sekä hallinta. Hallinnan kehittäminen kohti ekosysteemi- ja kokonaisketjuajattelua on vielä kesken.

Kehittyneet kyvykkyydet:

- Sisäinen tiedonvaihto ja yhteistyön kehitys, erityisesti liiketoimintojen välillä
- Kyberturvan tietoisuustyö ja siihen liittyvät toimenpiteet
- Kumppanien hallintaan liittyvien resurssien vähäisyys vaikuttaisi helpottaneen

Muut havainnot:

- Kumppanihallinta edelleen haastavaa, tosin kehitystä sopimusteknisten kontrollien ja kriittisten kumppanien kyberturvan varmistamisen osalta on tapahtunut.

6.4 Energia

Toimialalle ominaista

Toimiala on keskeinen toimija yhteiskunnan huoltovarmuusketjussa. Uusiutuvien energiamuotojen kehitys sekä vaadittujen investointien suuruus ovat alan keskeisiä haasteita.

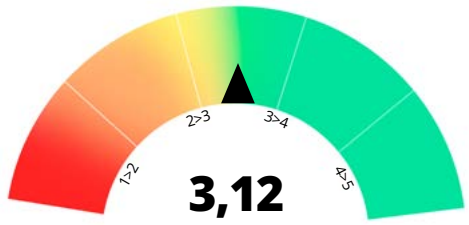
- Siirtymä uusiutuviin energiamuotoihin ajaa digitalisaatiota ja yritysten liiketoiminnan uusiutumista
- Valtiolla merkittävä rooli liiketoiminnallisesti olosuhteiden luomisessa ja merkittävimpien riskien hallinnassa

Suositukset toimialalle

Energia-alan kypsyystaso on yleisesti hyvä. Vahva varautumiskulttuuri edistää kyberturvallisuutta. Alaan kohdistuvat uhkat ovat niin merkittäviä, että yritysten oma varautuminen ei välttämättä riitä, jolloin valtiotason ja sen ylittävien toimenpiteiden merkitys on suuri.

- OT-ympäristöjen kyberturvallisuuden hallinnan integroiminen osaksi johtamisjärjestelmää
- Kypsyystasojen hajonnan aiheuttaman riskin arviointi laajemmin toimialalla

Toimialan kokonaiskypsyys



Toimialan vahvuudet

Toimialan hyvä kokonaiskypsyys näkyy erityisesti seuraavissa osa-alueissa:

- Järjestelmällinen ja hallittu tietoturvan johtaminen, jota ohjaa liiketoiminta- ja riskitietoisuus
- Vahva kulttuuri varautumisen osalta sekä kattava jatkuvuussuunnittelu, jota tukee alan tiedonvaihto
- Pääsynhallinta, sekä fyysisten että loogisten oikeuksien osalta

Toimialan riskit ja uhkat

Merkittävimmät toimialalle tunnistetut riskit ja uhkat:

- Toimiala keskeinen vaikutusväline valtioiden välisessä vaikuttamisessa ja konflikteissa, kaikki riskit eivät yritysten hallittavissa
- Teknologian kehitys avaa integraatioita ja uhkavektoreita IT- ja OT-ympäristöjen välillä

Toimialan heikkoudet

Toimialan hyvästä kypsyystasosta huolimatta kehityskohteiksi tunnistettiin seuraavat:

- Alan vahva jakautuminen korkean ja matalan kypsyystason toimijoihin
- Tietoturvakulttuurin vaihteleva taso toimijoiden välillä
- Elinkaariajattelun puutteet niin kumppani- kuin identiteetinhallinnassa

Vertailu selvityksen 2019–2020 ja 2022 välillä

Energia-ala näyttäytyy edellisen selvityksen tavoin vahvasti jakautuneena yritysten kyberturvallisuuskyvykkyyksien sijoittuessa kypsyysasteikon kumpaankin päähän. Yhtenäistä selvityskierrosten tuloksissa on haasteet OT-turvallisuuden huomioimisessa.

Kehittyneet kyvykkyydet:

- Kyberturvallisuuden hallinta ja johtaminen
- Uhkatiedon jakaminen

Varautumiskulttuuri on perinteisesti keskittynyt tuotanto- ja jakeluhäiriöiden estämiseen ja esimerkiksi kyberturvallisuuden hallinta on jäänyt vähemmälle huomiolle. Edelliseen selvitykseen nähden tilanne on kehittynyt ja etenkin alan kypsät yritykset suhtautuvat kyberturvallisuuden kehittämiseen strategisesti ja entistä laaja-alaisemmin. Yhä useampi alan toimija kerää uhkatietoa, mutta haavoittuvuuksien hallinnassa nähdään edellisen selvityksen tavoin kehitysvaraa, etenkin matalamman kypsyyden yrityksissä.

6.5 Terveydenhuolto

Toimialalle ominaista

Terveydenhuollon tavoitteena on edistää ja ylläpitää väestön terveyttä, hyvinvointia, työ- ja toimintakykyä ja sosiaalista turvallisuutta sekä kaventaa terveyseroja. Perustana ovat hyvin toimivat, koko väestön saatavilla olevat ehkäisevät, korjaavat ja kuntouttavat terveyspalvelut.

- Erilaiset tietosuojakontrollit, laatustandardit, määräykset ja regulaatio
- Alan toimijoilla vastuu asiakkaiden tietosuojasta ja tietoturvasta
- Palveluntuottajia, jotka hyödyntävät teknologiaa liiketoiminnan kehittämiseen

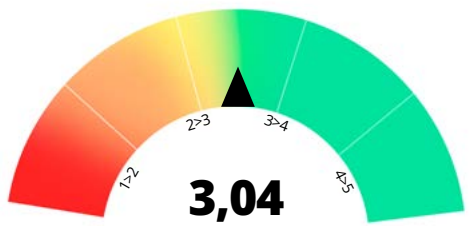
Suositukset toimialalle

Terveydenhuollon toimiala osoittaa hyvää perustason kypsyyttä pystyen mm. erilaisin tietosuojakontrollein ja laatustandardien tukemana hoitamaan kyberturvallisuutta määrämuotoisesti. Alan asema keskeisenä väestön terveyden ja hyvinvoinnin mahdollistajana nostaa sen houkuttelevuutta kohteena, jolloin jatkuva kehitys ja parantaminen kyberturvallisuuden osalta on ratkaisevan tärkeää.

Kypsyystason kehittämiseksi suositellaan seuraavia:

- Henkilöstön vaihtuvuudesta johtuen toimijoiden on erityisen tärkeää huolehtia henkilöstön ymmärryksestä omasta roolistaan organisaation kyberturvallisuuden toteutumisessa.
- Laajentaa toimitusketjujen sekä sidonnaisuuksien tunnistamista pidemmälle toimitusketjuja.
- Tietoturvan huomioiminen kattavasti koko sovelluskehitysprosessin ajan ns. DevSecOps -lähestymistavan mukaisesti.

Toimialan kokonaiskypsyys



Toimialan vahvuudet

Toimialan hyvä kokonaiskypsyys näkyy erityisesti seuraavissa osa-alueissa:

- Johdonmukainen, jatkuvan kehityksen toimintatavoitteet
- ISO 27000 – tietoturvastandardiin pohjautuvien tietoturvallisuuden hallintamallien yleisyys
- Riskienhallinta, viestien toimijoiden tiedostaneen huoltovarmuuskriittisen asemansa.

Toimialan riskit ja uhkat

Merkittävimmät toimialalle tunnistetut riskit ja uhkat:

- Hajanaiset legacy-järjestelmät
- Työvoimapula ja sijaisuudet, luoden osaamisen tasoeroja, nostaen riskiä kyberturvan laadukkaassa varmistamisessa sekä tietoisuudessa
- Toimittajariski, joka nykyselvityksessä noussut edelliseen selvitykseen nähden vaikutuksiltaan vähäisestä kohtuulliseksi

Toimialan heikkoudet

Toimialan hyvästä kypsyystasosta huolimatta kehityskohteiksi tunnistettiin seuraavat:

- Toimitusketjut, joissa palveluntarjoajien kyberturvallisuuden tason seuraaminen ja sopimusvelvoitteiden asettaminen ovat terveydenhuoltoalalla heikolla tasolla
- Kriittisten palveluiden suojaaminen, muodostuen kolmansien osapuolten riskienhallinnan heikoista käytännöistä
- Hybridiuhkiin varautuminen osana jatkuvuussuunnittelua sekä säännöllistä harjoittelua

Vertailu selvityksen 2019–2020 ja 2022 välillä

Alueittaisten tulosten hajonta on pysynyt samankaltaisena edelliseen selvitykseen nähden. Keskiarvoltaan heikoimman ja korkeimman selvityksen osa-alueen välillä eroa on alle yhden tason verran.

Kehittyneet kyvykkyydet:

- Kyberturvallisuuden hallinta ja johtaminen
- Lokienhallinta ja ympäristöjen monitorointi

Organisaatiokohtaisesta hajonnasta huolimatta kyberturvallisuuden hallinta on kypsyydeltään kolmanneksi korkein osa-alue. Etenkin kyberturvallisuuden hallintamallia koskeva osakohta osoittaa, että alan toimijat ovat edelliseen selvitykseen nähden kehittäneet kyberturvallisuuden johtamisjärjestelmiään.

6.6 Logistiikka

Toimialalle ominaista

Toimialalle tyypillisen tavarankuljetuksen sujuvuudesta on moni muu toimiala riippuvainen. Logistiikka-alan toimijat toteuttavat toimintaansa niin pyörillä, raiteilla kuin ilmassa. Asiakasodotukset virtaviivaisemmalle ja läpinäkyvälle palvelulle yli logistiikkaketjujen. Kriittinen ala, josta toiset toimialat riippuvaisia. Alan toimijoiden välillä suuria eroavaisuuksia vaihdellen yhden henkilön kuljetusyrityksistä globaaleihin logistiikkajätteihin.

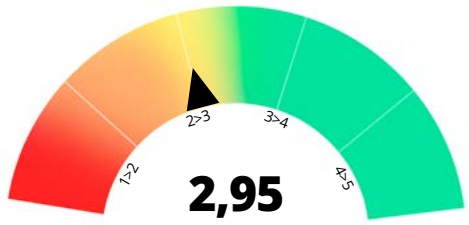
- Toimitusketjujen digitalisoituminen
- Globaali kilpailu, jossa investointikyvykkyys elinehto
- Kriittistä toimintaa, jossa palvellaan myös erilaisia, korkean turvatason toimijoita

Suositukset toimialalle

Ala on jatkuvasti kehittyvä, altis kilpailulle ja herkkä toimitusketjussa tapahtuville muutoksille, jolloin kyberturvallisuuden kokonaisvaltaiseen hallintaan tulee kiinnittää erityistä huomiota.

- Tarve kokonaisvaltaiselle kyberturvallisuuden hallinnan kehittämiselle
- Tilannekuvan kehittäminen tukemaan ajantasaisen tilannekuvan muodostamista
- Tietoturvallisuuden huomioiminen kattavasti koko sovelluskehitysprosessin ajan ns. DevSecOps -mallin mukaisesti

Toimialan kokonaiskypsyys



Toimialan vahvuudet

Toimialan kokonaiskypsyys näkyy seuraavissa osa-alueissa:

- Kyberturvallisuuden vaikutusten huomioiminen liiketoimintastrategiassa
- Ymmärrys kriittisistä palveluista sekä niiden jatkuvuuden varmistaminen

Toimialan riskit ja uhkat

Merkittävimmät toimialalle tunnistetut riskit ja uhkat:

- Erilaiset, maailmantilanteen muutoksen johdosta syntyvät uhkat näyttäytyen mm. kybertoiminnan ja hybridivaikuttamisen kasvuna
- Logistiikkaketjujen monimutkaisuus hankaloittaa niihin kohdistuvien riskien tunnistamista ja hallintaa
- Digitaalisten toimitusketjujen kasvu, altistaen uusille uhkavektoreille toimitusketjuissa

Toimialan heikkoudet

Toimialan heikkoudeksi tunnistettiin seuraavat:

- Puutteet lokienhallinnan politiikkojen tai linjausten määrityksessä ja jalkautuksessa
- Järjestelmätason sekä OT-ympäristöjen valvonnan kattavuus ja varmistaminen
- Kolmansien osapuolten ja toimintojen välisten riippuvuuksien tunnistaminen

Vertailu selvityksen 2019–2020 ja 2022 välillä

Edellisestä selvityksestä poiketen vaihtelua osa-aluekohtaisissa kyvykkyyksissä nähdään merkittävästi vähemmän. Toimialan kyvykkyyserojen ollen lähinnä toimijoiden välisiä, ei osa-alueita myöskään voida järjestää vahvuuksiin ja heikkouksiin kaikkien ollessa lähes samalla tasolla.

Kehittyneet kyvykkyydet:

- Henkilöstön johtamisen ja kehittämisen osa-alue on kehittynyt tietoturvakoulutusten osalta, jotka olivat edellisen selvityksen aikaan entistä heikommin toteutettu.

6.7 Media

Toimialalle ominaista

Toimiala keskeinen osa tietoyhteiskuntaa. Keskiössä sananvapaus, vapaa ja luotettava tiedonvälitys sekä demokraattisen yhteiskunnan puolustaminen.

- Kehittämisen ajurina modernin teknologian hyödyntäminen (mm. pilvipalvelut)
- Toimiala aktiivinen yritysostojen osalta, joissa haltuun voidaan saada sekä IT- että OT-ympäristöjä ja legacy-teknologiaa
- Alalla hyödynnetään kumppaneita, joiden laaja kirjo suurista yrityksistä yksittäisiin asiantuntijoihin aiheuttaa riskejä

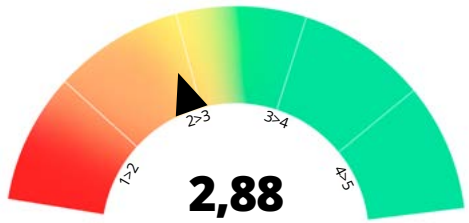
Suositukset toimialalle

Media-alan kehittynyt kypsyystaso tukee alan kykyä vastata uhkiin ja hallita riskejä. Alan asema keskeisenä kohteena sekä valtiotason vaikuttamiselle että rikollisille nostaa riskitasoa, jonka myötä riskilähtöinen kehitys on edelleen tarpeen.

Kypsyystason kehittämiseksi suositellaan seuraavia:

- Riskienhallinnan ja riskilähtöisen kyberturvallisuuden kehittäminen
- Toimitusketjujen hallinnan kehittäminen ja kumppanien kyberturvallisuuden varmistaminen, myös osana yritysostoja
- Alan kyberturvallisuuskulttuurin kehittäminen

Toimialan kokonaiskypsyys



Toimialan vahvuudet

Toimialan kehittynyt kokonaiskypsyys näkyy erityisesti seuraavissa osa-alueissa:

- Modernin teknologian hyödyntäminen ja tietoisuus suojattavista kohteista parantaa lähtökohtia kehittää kyberturvallisuutta
- Kyky valvoa omia ympäristöjä ja reagoida poikkeamiin

Toimialan riskit ja uhkat

Merkittävimmät toimialalle tunnistetut riskit ja uhkat:

- Toimialan rooli niin valtiollisten kuin kyberrikollisten kohteena
- Henkilöriskit, niin osaamisen, inhimillisten virheiden kuin henkilöihin kohdistuvan vaikuttamisen kautta
- Yritysostojen osalta puutteelliset due diligence-menettelyt, erityisesti kyberturvallisuuden osalta

Toimialan heikkoudet

Toimialan hyvästä kehityksestä huolimatta kehityskohteiksi tunnistettiin seuraavat:

- Riskienhallintakulttuurin puutteet
- Turvallisuusajattelun puute osana kehittämistä
- Kyberturvallisuuskulttuurin ja henkilöstön tietoisuuden heikko taso

Vertailu selvityksen 2019–2020 ja 2022 välillä

Media-alan kehittynyt kypsyystaso tukee uhka- ja riskikentän muutoksiin varautumista. Aiemman selvityksen jälkeen erityisesti uhkatilanteen kehittyminen, alalle kohdistuneet kyberhyökkäykset sekä alan liiketoiminnan kehittyminen on ajanut investointeja erityisesti teknisiin tietoturvaratkaisuihin, jotka näkyvät kypsyystasoissa.

Kehittyneet kyvykkyydet:

- Kyberriskienhallinta
- Kolmansien osapuolten riskienhallinta
- Käytännön jatkuvuusharjoittelu

Kyberriskienhallinnan käytännöt ja liiketoimintalähtöinen kyberturvallisuuden huomioiminen ovat selvästi kehittyneet edellisestä selvityksestä. Kolmansien osapuolten hallinta rajattuna suoriin kumppaneihin on myös parantunut, tosin kokonaisketjujen osalta havaittiin heikkouksia.

6.8 Elintarviketeollisuus

Toimialalle ominaista

Elintarviketeollisuus on teollisuuden ala, joka tuottaa elintarvikkeita tai elintarvikkeiden raaka-aineita. Lisäksi se on yhteiskunnan tukijalkana pidetty toimiala, jonka huoltovarmuuskriittinen rooli on turvata väestön ja tuotannollisten kotieläinten ravinto häiriötilanteissa ja poikkeusoloissa.

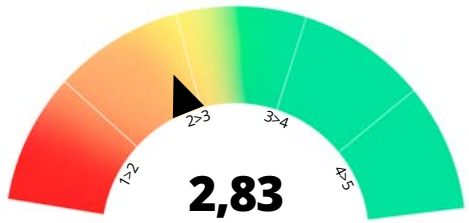
- Laaja, monimutkainen toimittajakenttä
- Toiminnan jatkuvuus riippuvainen tuotantopanosten saatavuudesta
- Tuoteturvallisuuden merkitys keskeinen toiminnan turvaamisessa

Suositukset toimialalle

Elintarviketeollisuuden yritysten on suositeltavaa kiinnittää huomioita toimenpiteisiin, jotka kasvattavat kypsyystasoa pitkällä aikavälillä. Reaktiiviset toimenpiteet voivat hetkellisesti nostaa kyberpuolustuskykyä tiettyjä uhkia vastaan, mutta eivät auta ennakoimaan nousevia uhkia tai kasvattamaan organisaation kokonaisvaltaista resilienssiä. Varautumistason kehittämiseksi suositellaan seuraavia:

- Kyberturvallisuuden pitkän aikavälin tavoitteiden linjaaminen ja kehittämissuunnitelman laatiminen sitouttaen organisaation ylimmän johdon yhteisiin tavoitteisiin
- Kyberriskien hallinnan kehittäminen tukemaan riskilähtöistä päätöksentekoa

Toimialan kokonaiskypsyys



Toimialan vahvuudet

Toimialan keskimääräisesti kypsimmät käytännöt nähdään seuraavissa:

- Identiteetin- ja pääsynhallinta toteutuu alan organisaatioissa pääosin sovitun prosessin mukaisesti
- Omaisuudenhallinnan vahvuutena on etenkin keskitetty rekisteri IT- ja OT-omaisuudesta sekä parhaillaan niiden konfiguraatioista. Lisäksi tietovarantojen hallinta on alan organisaatioissa keskimääräisesti hyvin hallussa.

Toimialan riskit ja uhkat

Merkittävimmät toimialan tunnistamat riskit ja uhkat:

- Globaalin pandemian aiheuttamat, moniulotteiset vaikutukset liiketoimintaan
- Sosiaalisen manipuloinnin hyödyntäminen kyberhyökkäyksissä

Toimialan heikkoudet

Kriittisimmiksi kehitystoimiksi toimialalla tunnistettiin:

- Kyberriskien hallinnan prosessien puutteet ja sen vaikutukset päätöksenteon riskilähtöisyyteen
- Kyberturvallisuuden tilannekuvan puutteet esimerkiksi lokitietojen hyödyntämisen osalta

Vertailu selvityksen 2019–2020 ja 2022 välillä

Elintarviketeollisuusalan hajonta matalimman ja korkeimman kypsyystason organisaatioiden välillä on hieman kasvanut edelliseen selvitykseen nähden. Monen edellisen selvityksen kehityskohteen tila on pysynyt samanlaisena selvitysten välillä. Kehitystä nähdään kuitenkin kahdella alueella.

Kehittyneet kyvykkyydet:

- Omaisuudenhallinta, etenkin IT- ja OT-omaisuuksien keskitetyn järjestelmän kautta
- Uhkatiedon jakaminen

Varautumiskulttuuri on perinteisesti keskittynyt tuoteturvallisuuden varmistamiseen ja esimerkiksi kyberturvallisuuden hallinta on jäänyt vähemmälle huomiolle. Nykytilassa ala on hyvin jakautunut matalimman kypsyystason toimijoiden tehdessä lähes kaiken kyberturvallisuuteen liittyvän reaktiivisesti tai ilman strukturoituja prosesseja, kypsimpien tehdessä strategisia suunnitelmia pitkälle aikavälille.

6.9 Teollisuus

Toimialalle ominaista

Teollisuuden toimialaraportin otantaan kuuluu yrityksiä metsä-, rakennus-, kemia-, suunnittelu-, konepaja- ja puolustusteollisuudesta. Laajasta otannasta huolimatta toimialalta löytyy seuraavia, yhdistäviä piirteitä:

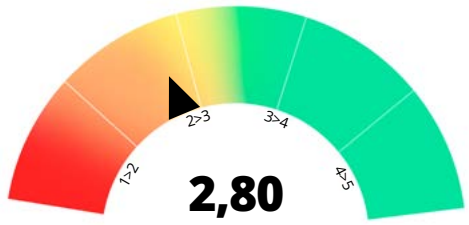
- Riippuvuus toimitusketjujen häiriöttömyydestä
- Herkkä suhdannevaihteluille ja ympäröivän maailman muutoksille
- Merkittävien investointien synnyttämät, taloudelliset riskit

Suositukset toimialalle

Teollisuuden hajanainen kypsyystilanne tekee varautumistilanteet arvioinnin haastavaksi. Kypsyystaso on alle hyvän perustason, jolloin vastaaminen uhkiin ei ole kattavaa. Teollisuuden toimialalla tunnistettiin seuraavat kehityskohteet:

- Toimitusketjujen sekä sidonnaisuuksien tunnistamisen laajentaminen mahdollisimman pitkälle toimitusketjussa.
- Teollisuusalan laajempi tarkastelu, eri teollisuudenalojen erottaminen omiksi kokonaisuuksiksi
- OT ja IT-ympäristöjen hallinnan integroiminen, tietoisuuden ja näkyvyyden rakentaminen molemmin puolin kokonaisvaltaisen tilannekuvan mahdollistamiseksi.

Toimialan kokonaiskypsyys



Toimialan vahvuudet

Toimialan hyvä kypsyys näkyy seuraavissa osa-alueissa:

- Uhkien ja haavoittuvuuksien hallinta
- Identiteetin- ja pääsynhallinta
- Tapahtumien ja häiriöiden hallinta, toiminnan jatkuvuus

Toimialan riskit ja uhkat

Merkittävimmät toimialalle tunnistetut riskit ja uhkat:

- Toimitusketjujen digitalisoituminen
- Vaikutukset geopoliittisen tilanteen muutoksissa

Erityisesti rakennusalalla esiintyvä, harmaan talouden riski

Toimialan heikkoudet

Toimialan kehityskohteiksi tunnistettiin seuraavat:

- Toimittajahallinnan kehittäminen ja sidonnaisuuksien tunnistaminen
- Riskienhallinta, jossa puutteita havaittiin erityisesti kyberriskien strukturoidussa hallintamallissa
- Kyberturvallisuuden hallinta osa-alueella erityisesti johdon tuen ja kiinnostuksen puutteen vaikutukset

Vertailu selvityksen 2019–2020 ja 2022 välillä

Edellisessä selvityksessä havaitut osa-alueet ovat sittemmin kehittyneet, niiden ollessa nykyselvityksessä arvioitu kypsyydessään kolmeksi korkeimmaksi osa-alueeksi. Edelleen haasteena on siiloutuminen IT- ja OT-ympäristöjen hallinnan välillä.

Kehittyneet kyvykkyydet:

- Uhkien- ja haavoittuvuuksienhallinta
- Uhkatiedon jakaminen
- Jatkuvuuden suunnitteluun liittyvät toimenpiteet

Edelleen matalalla tasolla on kolmansien osapuolten riskienhallinta, erityisesti kokonaisketjujen hallinnan sekä sidonnaisuuksien tunnistamisen näkökulmasta.

6.10 Vesihuolto

Toimialalle ominaista

Tärkeänä toimijana päivittäisen infrastruktuurin ylläpidossa sekä yhteiskunnan toiminnan kannalta kriittinen palvelu. Vesihuolto on toimintaa, jonka asiakkaat helposti olettavat tapahtuvaksi. Suuremmat poikkeustapahtumat eskaloituvat helposti paikallisiksi katastrofeiksi.

- Toiminnan keskiössä operatiivisen toiminnan ja järjestelmien ylläpito ja toimintavarmuus
- Usea vesihuollon toimija luottaa ICT:n osalta taustalla olevan kaupungin tai kunnan palveluihin
- Laaja palvelutoimittajakenttä, luoden haasteita kolmansien osapuolten hallintaan läpinäkyvyyden osalta

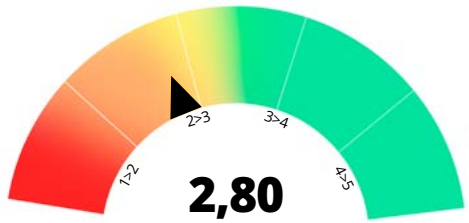
Suositukset toimialalle

Vesihuoltotoimialan kokonaiskypsyys jää kypsyydessään vajaaksi hyvästä perustasosta. Keskeinen rooli yhteiskunnan toimivuudessa vaatii investointeja myös kyberturvallisuuteen alan vastatakseen kattavasti siihen kohdistuviin kyberuhkiin. Alan kriittinen, yhteiskunnallinen rooli korostaa kriittisten palveluiden ylläpitoa ja kehittämistä.

Kypsyystason kehittämiseksi suositellaan seuraavia:

- Kyberturvallisuuden hallinnan ja yhteistyön rakentaminen omistajatahojen sekä IT-toimittajien kanssa
- Kolmansien osapuolten riskienhallinnan kehittäminen ja toimitusketjujen kyberturvallisuuden varmistaminen sidonnaisuuksien tunnistamisen ja läpinäkyvyyden kautta.
- Ajantasaisen ja kattavan tilannekuvan mahdollistavien prosessien ja käytänteiden kehittäminen

Toimialan kokonaiskypsyys



Toimialan vahvuudet

Toimialan kypsimmät käytännöt näkyvät seuraavissa osa-alueissa:

- Ymmärrys omista, toimintavarmuuden kannalta kriittisimmistä toiminnoista
- Kyberturvallisuuden hallinnan taustalla ohjaavat suunnitelmat tai politiikat, joita vasten kyberturvallisuuden kehittäminen tapahtuu
- Sellaiset omaisuuden, muutosten ja konfiguraation hallintaan liittyvät käytänteet, jotka mahdollistavat muun muassa haavoittuvuustietoihin nopean reagoinnin

Toimialan riskit ja uhkat

Merkittävimmät toimialalle tunnistetut riskit ja uhkat:

- Toimialan rooli niin kyber- tai hybridivaikuttamisen kohteena
- Raaka-aineiden ja materiaalien saatavuuteen liittyvät riskit etenkin poikkeusoloissa
- Haasteet ajantasaisen tai oikean tiedon saamisessa tilannekuvan muodostamiseksi

Toimialan heikkoudet

Toimialan kriittisimmiksi kehityskohteiksi tunnistettiin seuraavat:

- Kyberturvallisuuden kokonaishallinnan puutteet, erityisesti IT-toimittajien suuntaan
- Heikko näkyvyys kumppanien toimintaan kehitystyössä
- Korkea riippuvuussuhde IT-palveluntoimittajiin

Vertailu selvityksen 2019–2020 ja 2022 välillä

Alueittainen keskiarvojen vaihtelu on pysynyt melko samanlaisena edelliseen selvityskierrokseen nähden. Edellisen selvityksen tavoin suurempaa vaihtelua nähdään organisaatiokohtaisissa tuloksissa.

Kehittyneet kyvykkyydet:

- Henkilöstön johtaminen ja kehittäminen
- Kyberturvallisuuden kehitystyötä ohjaavat politiikat
- Omaa sovelluskehitystä tekevien toimijoiden kypsyystason nousu tietoturvallisessa sovelluskehitystyössä

Kenties merkittävin kehitys selvitysten välillä liittyy uhka- ja riskitilanteen kehitykseen, jossa vesihuolto alana on noussut potentiaalisten kohteiden joukkoon. Monet niistä riskeistä, joita on arvioitu todennäköisyydeltään pieneksi, onkin nyt nousemassa seurantalistoille. Tämä kehitys puoltaa myös investointeja kyberturvallisuuden kypsyyteen.

6.11 Kauppa ja jakelu

Toimialalle ominaista

Kaupan ja jakelun yritykset toimivat laajojen materiaalivirtojen päätepisteenä ja ovat elintarvikeketjun asiakasrajapinnassa hyvin häiriöherkkä alue.

- Vahvasti riippuvainen toimitusketjuista ja niiden toimintavarmuudesta (Elintarvike ja Logistiikka)
- Automatisoinnilla suuri merkitys niin toimitusketjujen kuin verkkokaupan operatiivisessa toiminnassa
- Koronapandemian poikkeukselliset vaikutukset kaupan ja jakelun toimijoille, sekä viranomaisrajoitukset että pandemian pitkäaikaiset asiakaskäyttäytymisen muutokset

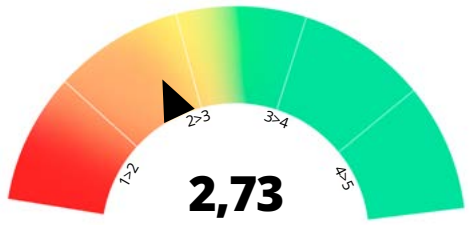
Suositukset toimialalle

Kaupan ja jakelun kokonaiskypsyys jää hyvän perustason alle ja alan varautuminen kyberuhkiin ei ole kattavaa. Suuri hajonta kypsyystasoissa voi indikoida riskikeskittymästä, erityisesti pienempien ja paikallisten toimijoiden keskuudessa.

Kypsyystason kehittämiseksi suositellaan seuraavia:

- Kyberriskienhallinnan käytäntöjen kehittäminen riskilähtöisen päätöksenteon varmistamiseksi
- Kyberturvallisuuden integrointi osaksi liiketoiminnan ja palveluiden kehittämistä

Toimialan kokonaiskypsyys



Toimialan vahvuudet

Toimialan kypsimmät käytännöt ovat seuraavissa aiheissa:

- Identiteetin- ja pääsynhallinnan vahvuus on etenkin fyysisten pääsyoikeuksien hallinta, mutta osa toimijoista hallitsee myös digitaalisia identiteettejä ja loogisia pääsyoikeuksia kypsällä tasolla
- Operatiivisen toiminnan varmistamisen pitkä kulttuuri, jonka parhaita käytäntöjä voidaan hyödyntää myös kyberturvallisuuden varmistuksessa

Toimialan riskit ja uhkat

Merkittävimmät toimialalle tunnistetut riskit ja uhkat:

- Liiketoimintamallin digitalisoitumisen tuomat vaikutukset suojattavaan tietoon sekä tiedon suojauksen mekanismeihin ja kontrolleihin
- Toimitusketjuihin kohdistuvat kyberuhkat
- Rikollisuuden vaikutukset niin kyberrikoksissa kuin esimerkiksi inflaation vaikutuksesta myymälärikollisuudessa

Toimialan heikkoudet

Toimialan kriittisimmiksi kehityskohteiksi tunnistettiin seuraavat:

- Kyberturvallisuusnäkökulman heikompi huomioiminen operatiiviseen jatkuvuuteen verrattuna mm. osa-alueissa: tapahtumien ja häiriöiden hallinta, haavoittuvuuksien hallinta, omaisuudenhallinta ja kriittisten palveluiden suojaaminen
- Kyberriskienhallintakulttuurin puute useimmissa otannan organisaatioissa ja sen vaikutus riskilähtöisen päätöksenteon haasteisiin

Vertailu selvityksen 2019–2020 ja 2022 välillä

Edelliseen selvityskierrokseen verrattuna vaikuttaisi siltä, että tällä kertaa Kauppa ja Jakelu alojen otannassa on mukana enemmän matalan tason toimijoita. Tämä osaltaan on tuonut esiin alan toimijoiden polarisoituneisuutta eri osa-alueiden kypsyyksissä.

Kehittyneet kyvykkyydet:

- Kyberuhkatietoisuuden nousu ja kyberturvallisuuden käsittelyn hienoinen lisääntyminen yritysten johtoryhmien tasolla

Kaupan ja jakelun yritykset näyttäytyvät edellistä selvitystä jakautuneempina kypsyystasoissaan. Otannan muutoksista johtuen ei voida varmuudella arvioida, onko ala ollut jo pitkään yhtä jakautunut kypsyydessään, vai onko kypsyystasojen erot kehittyneet erityisesti selvityskierrosten välisinä vuosina.

6.12 Satamat ja merenkulku

Toimialalle ominaista

Kustannustehokas ja ympäristöystävällinen toimiala. Korvaamaton kuljetusmuoto erityisesti suurille tonnistomäärille.

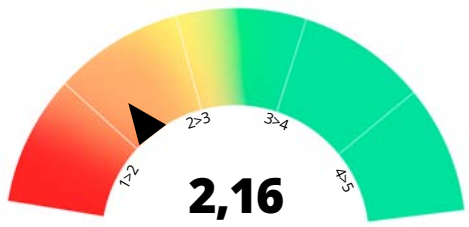
- Toimialan korostunut rooli kansallisen huoltovarmuuden ylläpidossa poikkeustilanteissa
- Toimialalla kiristyvä GDPR-regulaatio ja NIS2-direktiivin vaikutukset digitaalisen kehittymisen myötä
- Kasvavat ympäristövaatimukset

Suositukset toimialalle

Satamat ja merenkulun toimialan kypsyystaso on matala. Erityisesti havaittu puute johdon tuessa estää mahdollisten kehitystarpeiden ja investointien tehokkaan edistämisen, joilla kyberturvallisuuden kokonaisuutta on mahdollista nostaa nykyisestä kypsyystasosta.

- Kyberturvallisuuden hallinnan kehittäminen pidemmän aikavälin strategialla, huomioiden liiketoimintalähtöisen kyberturvallisuusstrategian
- Johdon tuen lisääminen varmistamaan strategiaan pohjautuvien ja asetettujen kyberturvallisuuden tavoitteiden läpiviennin
- Kyberturvallisuusarkkitehtuuri osa-alueen kehittäminen huomioiden erityisesti selvityksessä havaitut puutteet tiedonsuojauksen prosesseihin liittyen

Toimialan kokonaiskypsyys



Toimialan vahvuudet

Toimialan matalan kokonaiskypsyyden huomioon ottaen voidaan kuitenkin havaita osa-alueita, jotka laadukkaasti kehitettyinä voivat nostaa osa-alueiden kypsyyttä seuraavalle kypsyystasolle:

- Identiteetin- ja pääsynhallinta
- Uhkien- ja haavoittuvuuksienhallinta

Yrityksillä on matalasta kokonaiskypsyydestä huolimatta hyviä käytäntöjä, joita jatkokehittämällä kokonaismaturiteettitasoa saadaan tulevaisuudessa nostettua.

Toimialan riskit ja uhkat

Merkittävimmät toimialalle tunnistetut riskit ja uhkat:

- Kyberturvallisuuteen osoitettujen resurssien vähäisyys altistaa monivaikutteisille uhkille ja riskeille
- Liikenteen ja satamien häirintänä Ukrainan sodan seurauksena

Toimialan heikkoudet

Toimialan kypsyystasossa tunnistettiin seuraavat heikkoudet:

- Johdon tuen puute, estäen kehittämistarpeiden läpiviennin
- Puutteet kyberturvallisuuden hallinnan perustason määrittelyssä ja asetannassa

Vertailu selvityksen 2019–2020 ja 2022 välillä

Satamat ja merenkulun toimialan kyberturvallisuuden tilanne ei ole merkittävästi muuttunut edellisestä, vuosina 2019-2020 toteutetusta toimialojen kyberturvallisuuden tilannekuvan selvittämishankkeesta.

Kehittyneet kyvykkyydet:

- Havaittavissa muutos tietoisuudessa ja suhtautumisessa tieto- ja kyberturvallisuuden pitkäjänteiseen kehittämiseen

Toimialaa koskettavat edelleen samat haasteet, kuten resurssoinnin vähäisyys, johdon sitoutumattomuus ja IT-palveluntuottajien kommunikoinnin puutteet. Toimialan kehittämistä tukee toimijoiden vahva sitoutuneisuus huoltovarmuusorganisaatioon. Toimialalle tämä linkki tarjoaa mahdollisuuden kehittää kyberturvallisuuden tilaa lisäämällä yhteistä tilannekuvaa ja organisoimalla yhteisiä tapoja kehittää kyvykkyyksiä.

7 Liitteet

Tässä luvussa esitellään toimialojen kyberturvallisuusselvityksen tausta ja käytetyt menetelmät. Luvussa 7.1 esitetään selvityksen tausta ja jatkumo edellisestä, vuosina 2019-2020 toteutetusta, selvityksestä. Luvussa 7.2 kerrotaan tämänkertaisen, vuoden 2022, selvityksen toteutuksesta. Käytetty menetelmä, työkalu ja arviointikriteeristö esitellään luvussa 7.3. Lopuksi esitetään huomiot selvitysten vertailusta.

7.1 Selvityksen tausta

Toimialojen kyberturvallisuusselvitys on jatkumoa 2019-2020 toteutetulle selvitykselle ja nyt toimialojen tilannetta tarkasteltiin uudelleen. Vuonna 2022 toteutetussa selvityksessä arvioitiin 121:n suomalaisen yrityksen kyberturvallisuuden nykytilaa eri toimialoilta hyödyntäen Kybermittarista aihealueittain johdettua versiota. Työpajoissa käsiteltiin kybermittarin aihealueiden lisäksi toimialoille tyypillisimmät, identifioidut riskit, jotka ovat jatkumoa edelliskerran selvityksestä. Riskien kautta yrityksen nykytilaa ja valmiutta vastata toimialan uhka- ja riskikenttään on myös arvioitu. Lisäksi vuoden 2022 selvityksessä selvitettiin pilvipalveluiden käyttöä ja niihin liittyvien riskien tunnistamista sekä kokonaisketjuun liittyvien riskien tunnistamista.

Selvityksen tuloksia hyödynnetään määritettäessä toimia kriittisen infrastruktuurin ja kansallisen kyberturvallisuuden kehittämiseksi. Selvitys toteutettiin osana Huoltovarmuuskeskuksen Digitaalinen Turvallisuus 2030 -ohjelmaa, joka pyrkii vahvistamaan elinkeinoelämän ja yhteiskunnan keskeisten toimijoiden kykyä torjua kyberuhkia ja selvitä kyberhäiriötilanteista.
Vuosina 2019-2020 toteutetun selvityksen raportti on nähtävissä täällä:
Kyberturvallisuuden nykytila eri toimialoilla[1]

7.1.1 Selvityksen toteutus

Vuonna 2022 toteutettuun selvitykseen osallistui yhteensä 121 suomalaista yritystä. Yritykset jakautuivat 12 toimialueelle. Haastattelujen tuloksia hyödynnetään laajassa kansallisen tason raportissa, johon koostetaan kokonaisnäkemys yli toimialojen. Lisäksi kustakin toimialasta tuotettiin erillinen raportti. Yrityskohtaiset tulokset ovat anonymisoituja; yrityksiä käsitellään raportoinnissa yrityskoodeilla. Yrityskoodien avulla yritykset voivat tunnistaa itsensä ja omat tuloksensa raporteista.

Tutkimuksen mittarina hyödynnettiin Kybermittarista aihealueittain johdettua versiota – Kybermittaria sellaisenaan ei kuitenkaan käytetty. Mittariin oli lisäksi otettu tämän hetken merkittävimmät kyberriskit toimialoittain, joiden kautta yrityksen nykytilaa ja valmiutta arvioitiin. Lisäksi haluttiin selvittää pilvipalveluiden käyttöä, niihin suhtautumista ja niihin liittyvien riskien tunnistamista.

Selvitykseen osallistuneille yritykselle lähetettiin etukäteistietopaketti, joka opasti yritystä löytämään oikeat tahot mukaan haastatteluun. Itse haastattelut toteutettiin keskustelevina työpajoina. Mittaustuloksien ja riskikartan myötä organisaatioille luotiin näkymä omasta valmiustasostaan toimialan suuriin muutoksiin kyberturvan näkökulmasta sekä kyberturvan eri osakohtien onnistumisista ja kehityskohteista. Selvitys tuotti työpajoihin osallistuneille yrityksille tietoa yritysten omasta tilanteesta kyberuhkiin varautumisessa sekä laajempia toimialakohtaista näkemystä. Loppuraportissa käsitellään myös toimialat ylittävä näkymä kansalliseen kyberturvallisuuden tilaan ja kehityskohteisiin.

7.1.2 Mittaristo ja arviointikriteeristö

Kypsyysarvioiden mittaristo pohjaa yleiseen 5-tasoiseen kypsyysmalliin, kuten esimerkiksi CMM-mallissa. Eri kypsyystasojen yleisvaatimukset on kuvattu alla taulukossa 2.

Kypsyystaso	Kuvaus / yleisvaatimukset tasolle
1	Toiminta reaktiivista, prosesseja ei kuvattu tai ne ovat vakiintumattomia.
2	Prosessit ovat suunniteltuja, valvottuja ja ne toteutuvat sovittujen menettelytapojen mukaisesti. Dokumentaatio ei ole kattavaa, eikä prosessien taustalla ole johtamisjärjestelmää.
3	Johtamisjärjestelmä määritelty ja käytössä, prosessit perustuvat organisaation yhteisiin standardeihin ja linjauksiin. Ei jatkuvaa arviointia/auditointia, dokumentaation päivittäminen on puutteellista.
4	Johtamisjärjestelmä toteuttaa jatkuvan parantamisen mallia, prosessien laadulle ja suorituskyvylle on asetettu vaatimukset, joita seurataan. Toiminta on systemaattista.
5	Jatkuvan parantamisen malli, jota tuetaan teknologisilla kyvykkyyksillä ja niiden kehittämisellä (mm. automatisointi, modernit ratkaisut). Prosessit kattavat koko organisaation ja linkittyvät organisaation strategiseen tasoon.

Taulukko2: Kypsyystasojen kuvaus

Kypsyystasoista voidaan yleisesti mainita, että hyvä perustason kyvykkyys vaatii tason 3 kypsyyden. Tällöin voidaan sanoa alueen riskien olevan hallinnassa. Kypsyysarvion perusteella on kuitenkin vaarallista tehdä johtopäätöksiä kyberturvallisuuden kyvykkyydestä suojata organisaatiota. Arvioinnin pohjalta voidaan tehdä arvio miten kyvykkyysaluetta hallitaan, mutta todellisen kyvykkyyden toteamiseksi on syytä käyttää myös muita testauskeinoja. Näihin kuuluvat esimerkiksi erilaiset tietoturvan valmiusharjoitukset, erilaiset tietoturvatestaukset sekä erilaisia hyökkäyssimulaatioita (esim. ns. red teaming -harjoitukset).

Arviointiskaala on sinällään vastaava viisiportainen kuin edellisessä selvityksessä. Muutoksia arviointiin on tullut kahtaalta: työkalun kyberturvallisuuden alueet ovat päivittyneet verrattuna edelliseen selvitykseen ja tämän lisäksi arviointiskaalaa on uudelleenkalibroitu ja maturiteettitasojen sisältöjä tarkennettu. Skaalan kalibrointi merkitsee sitä, että kypsyysarvion tulokset eivät ole numeraalisesti suoraan verrannollisia. Tästä johtuen vertailu selvitysten välillä perustuu enemmän kvalitatiiviseen arvioon, eli on katsottu enemmän maturiteettitasojen sisällä olevia kyvykkyyksiä ja niiden kehittymistä, kuin pelkkää numeraalista vertailua.

Työkaluna selvityksessä on hyödynnetty Traficomin Kybermittari-työkalua[2]. Kybermittari on organisaatioiden johdolle ja tietoturva-ammattilaisille suunnattu konkreettinen väline kyberturvallisuuden hallintaan, toimialakohtaiseen vertailuun ja kehityspanostusten ohjaamiseen.

Arviointityökalun avulla organisaatio voi mitata kypsyystasonsa kyberturvallisuuden hallinnan eri osa-alueilla. Kybermittari kertoo saavutetun kypsyystason ja esittää seuraavalle tasolle vaadittavat kehitysalueet. Mittarin käyttöä tukee mittauksista saatavat vertailukelpoiset tulokset.

Kybermittarin kohteena liiketoiminnalle ja yhteiskunnalle kriittiset toiminnot ja kattaa yleisimmät kyberturvallisuuden riskienhallinnan osa-alueet. Työkalun pohjana on toiminut olemassa olevat NIST ja C2M2 -mallit ja parhaat käytännöt. Työkalun avulla voidaan raportoida myös NIST CFT-mallin kyvykkyyksien näkökulmasta. Kyberselvityksessä ei toteutettu Kybermittari-arviointeja kokonaisuudessaan, vaan hyödynnettiin osajoukkoa työkalun kyvykkyyksistä. Selvityksessä arvioidut kyvykkyydet ovat listattu alla taulukossa 3.

Käsitellyt osa-alueet

Työpajoissa käytiin yhteensä läpi 11 eri osa-aluetta. Arviointi toteutettiin osa-aluekohtaisesti työpajoissa osallistujien antamien tietojen perusteella.

Osajoukon määrittelyn tavoitteena on ollut kohdentaa selvityksen työpajat organisaatioiden kyberturvallisuuden johtamisen ja hallinnan arviointiin.

Osa-alue	Kuvaus
PROGRAM	**Kyberturvallisuuden hallinta** osa-alueessa arvioidaan organisaation kykyä hallita ja ylläpitää organisaationlaajuista kyberturvallisuusohjelmaa.
ARCHITECTURE	**Kyberturvallisuusarkkitehtuuri** osa-alueessa arvioidaan organisaation kykyä hallita ja ylläpitää kyberturvallisuustoimintaansa.
RISK	**Riskienhallinta** osa-alueessa arvioidaan organisaation tieto- ja kyberturvallisuuteen liittyvien riskien (kyberriskit) tunnistamisen ja hallinnan valmiuksia.
CRITICAL	**Kriittisten palveluiden suojaaminen** osa-alueessa arvioidaan organisaation kykyä tunnistaa oma roolinsa yhteiskunnan kannalta kriittisten palveluiden tuottamisessa ja sen myötä suojaamisessa.
THREAT	**Uhkien ja haavoittuvuuksien hallinta** osa-alueessa arvioidaan organisaation kykyä määritellä ja ylläpitää suunnitelmia, prosesseja ja tekniikoita kyberuhkien ja -haavoittuvuuksien havainnointiin, tunnistamiseen, analysointiin, hallintaan ja niihin puuttumiseen.
ASSET	**Omaisuuden, muutosten ja konfiguraation hallinta** osa-alueessa arvioidaan organisaation kykyä hallita laite-, ohjelmisto- ja tieto-omaisuuttaan suhteessa organisaatioon kohdistuviin riskeihin ja organisaation tavoitteisiin.
WORKFORCE	**Henkilöstön johtaminen ja kehittäminen** osa-alueessa henkilöstön johtaminen ja kehittäminen arvioidaan henkilöstön kyberturvallisuustietoisuutta, -osaamista, sekä valmiutta reagoida erilaisiin kyberhäiriötilanteisiin.
THIRDPARTYE	**Kolmansien osapuolten riskienhallinta** osa-alueessa arvioidaan organisaation kykyä tunnistaa sekä hallinnoida toimitusketjuihin ja kolmansiin osapuoliin liittyviä riskejä.
SITUATION	**Tilannekuva** osa-alueessa arvioidaan organisaation kykyä ylläpitää kyberturvallisuuden tilannekuvaa.
RESPONSE	**Tapahtumien ja häiriöiden hallinta, toiminnan jatkuvuus** osa-alueessa arvioidaan organisaatioiden kykyjä hallinnoida, reagoida sekä palautua kyberhäiriötilanteista
ACCESS	**Identiteetin- ja pääsynhallinta** osa-alueessa arvioidaan organisaation kykyä hallinnoida ja rajoittaa loogisia ja fyysisiä pääsyoikeuksia yrityksen suojattavaan omaisuuteen.

Taulukko 3: Selvityksessä arvioidut kyvykkyydet

Toimialariskiarvio

Osana työpajoja toteutettiin myös toimialariskiarvio. Toimialariskilistat perustuvat edelliseen selvitykseen, joiden lisäksi mukaan uutena riskinä nykyselvitykseen on otettu globaali pandemia.

Riskiluvut määräytyivät osallistuneiden yritysten itsearvion pohjalta. Yritykset arvioivat riskien todennäköisyyttä ja vaikutusta omasta näkökulmastaan sekä osana toimialan kokonaisketjua. Toimialariskejä arvioitiin laskukaavalla todennäköisyys x vaikutus. Todennäköisyyttä ja vaikutusta arvioitiin viisitasoisen arviointiasteikon mukaan, joka esitetty alla taulukossa 4.

Todennäköisyys		Vaikutus	
1	Harvinainen	**1**	Merkityksetön
2	Epätodennäköinen	**2**	Vähäinen
3	Mahdollinen	**3**	Kohtuullinen
4	Todennäköinen	**4**	Merkittävä
5	Erittäin todennäköinen	**5**	Erittäin merkittävä

Taulukko 4: Riskien arviointiasteikko

7.1.3 Selvitysten tulosten vertailu

Vuoden 2019-2020 selvitys ja vuoden 2022 selvitys eivät ole suoraan vertailukelpoisia muuttuneen työkalun sekä tarkennetun arviointikriteeristön vuoksi.

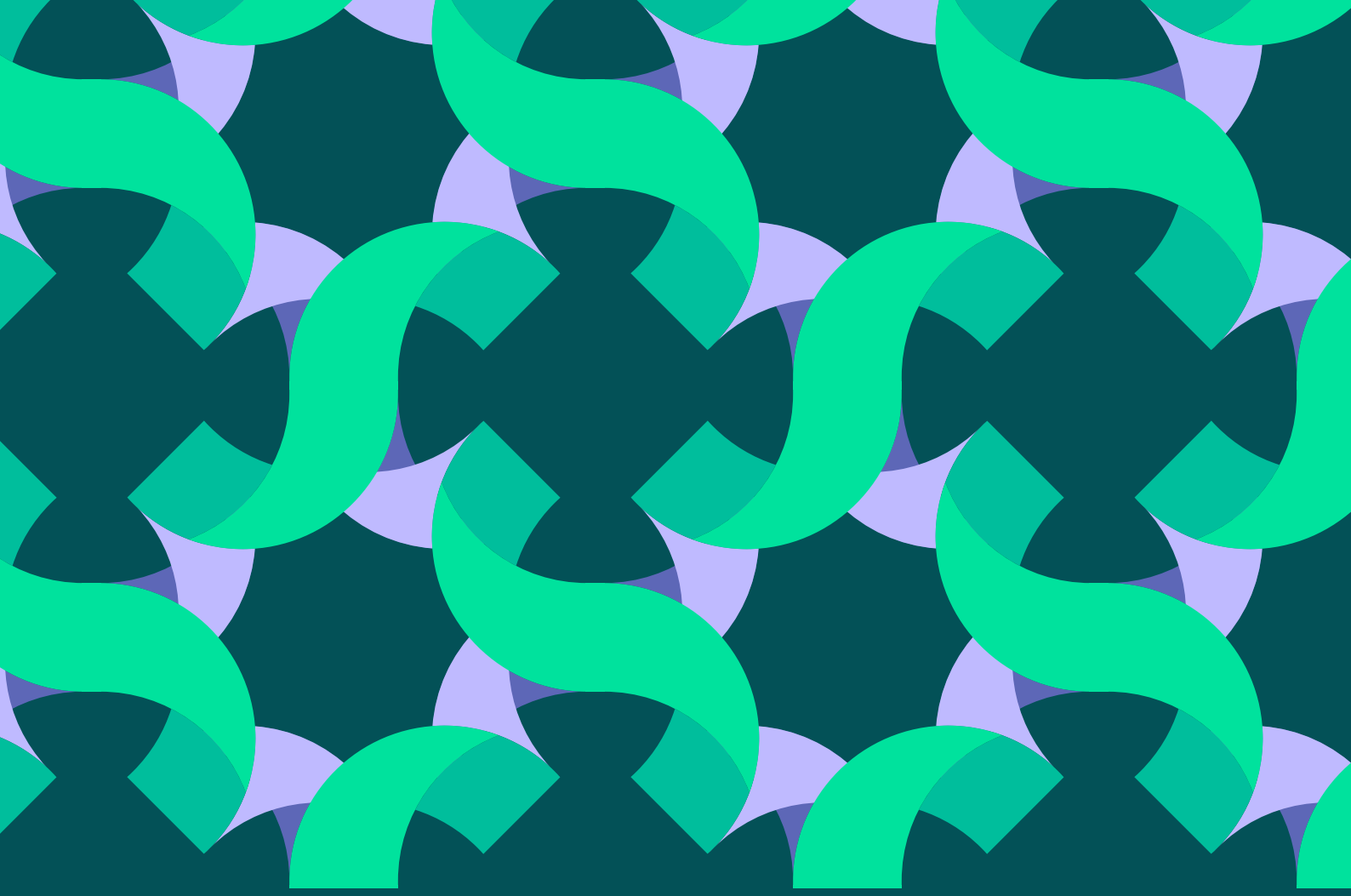
Johtopäätökset selvitysten vertailu osiossa on pyritty numeroarvioiden sijaan ymmärtämään kypsyysarvioiden pohjana olevia kyvykkyyksiä ja prosesseja. Vertailussa on pyritty arvioimaan kehitystä vuosien 2020 ja 2022 välillä, peilaamaan sitä uhka- ja riskitilannearvioihin sekä toimialariskiarvioon.

Huomioitavaa on myös otannan merkitys tulosten vertailussa. Ensimmäisen selvityksen tarkka otanta ei ole ollut käytössä tätä selvitystä toteutettaessa. Luottamuksellisuuden varmistamiseksi tarkkaa otantaa ei myöskään raportoida tämän selvityksen osalta. Tällöin otannan vaikutuksia kypsyysarvioihin on mahdotonta arvioida tai ottaa huomioon analyysissä. Tässä selvityksessä toimialojen määrä on eriävä edellisestä, kuin myös toimialojen yritysmäärät.

Yllä mainituista syistä selvitysten välinen vertailu on tehty varoivaisuusperiaatetta noudattaen. Johtopäätökset on pyritty hakemaan alueilta, joissa niiden pohjalla on edes jonkin verran luotettavaa dataa. Niiden osalta epävarmuus on kuitenkin merkittävä ja luotettavuutta on syytä pitää heikkona.

[1]https://www.huoltovarmuuskeskus.fi/files/b3671ecb5d0b5b431174fec9350e0251b75227ba/kyberturvallisuuden-nykytila-eri-toimialoilla2-verkkosivuille.pdf

[2]https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostot/kybermittari



Huoltovarmuuskeskus