Kyberkypsyys toimialoilla 2025

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
Tilaaja: Digipooli
Toteuttaja: Accenture Oy
Kansikuva: pexels
Julkaisuvuosi: 2026
ISBN: 978-952-7470-45-9

Esipuhe

Digitalisaatio ja turvallisuusympäristön muutos haastavat huoltovarmuuden

Huoltovarmuus ja digitaalinen turvallisuus ovat kietoutuneet erottamattomasti toisiinsa. Yhteiskunnan kriittiset toiminnot kuten energiahuolto, logistiikka, finanssiala ja elintarvikehuolto nojaavat yhä vahvemmin digitaalisiin järjestelmiin ja verkottuneisiin toimitusketjuihin. Ilman luotettavia digitaalisia ratkaisuja ei ole myöskään yhteiskunnan toimintakykyä häiriö- tai poikkeusoloissa.

Viimeisen kahden vuoden aikana turvallisuusympäristö on myös muuttunut poikkeuksellisen nopeasti. Geopoliittinen vastakkainasettelu, sotilaallinen painostus ja taloudelliset häiriöt ovat korostaneet digitaalisen resilienssin merkitystä entisestään. Digitalisaatio etenee vauhdilla, mutta kyberturvallisuuden kehitys ei ole pysynyt tämän muutoksen tahdissa. Pilvipalvelujen, automaation, tekoälyn ja verkottuneiden laitteiden nopea käyttöönotto ovat laajentaneet hyökkäyspinta-alaa nopeammin kuin suojaus- ja hallintakäytännöt ovat kehittyneet.

Sotilaallisen painostuksen kasvu on tuonut kybertoimintaympäristöön uudenlaisen operatiivisen ulottuvuuden. Euroopassa kriittiseen infrastruktuuriin kohdistuvat kyberoperaatiot ovat lisääntyneet ja muuttuneet aiempaa määrätietoisemmiksi. Suomi on osa tätä laajempaa kehityskulkua osana eurooppalaisia energia-, tele- ja logistiikkajärjestelmiä. Samanaikaisesti laaja-alainen vaikuttaminen on voimistunut. Kyberhyökkäykset, disinformaatio ja poliittinen painostus muodostavat toisiaan tukevan kokonaisuuden, jossa digitaalisesta ympäristöstä on tullut keskeinen yhteiskunnallisen vaikuttamisen alusta. Luottamus instituutioihin ja päätöksentekoon on entistä useammin vaikuttamisen kohteena. Myös geotalouden merkitys on kasvanut. Toimitusketjujen haavoittuvuudet, teknologinen riippuvuus ja kyberuhkien kytkeytyminen taloudelliseen kilpailuun korostavat huoltovarmuuden ja kyberturvallisuuden keskinäisriippuvuutta.

Huolimatta nopeasti muuttuneesta turvallisuustilanteesta kansallinen kyberkypsyyden taso Suomessa on noussut vuodesta 2022 vain maltillisesti. Kärjessä ovat edelleen vahvasti säännellyt toimialat, kuten finanssi-, teleliikenne- ja ICT-ala, joilla kyberturvallisuus on liiketoiminnan edellytys tai merkittävä kilpailuetu. Heikommalle tasolle jäävät elintarvikehuolto, satamat, telakat ja operaattorit sekä liikenne ja logistiikka – juuri ne toimialat, jotka ovat huoltovarmuuden kannalta erityisen kriittisiä.

Viimeiset kaksi vuotta ovat siis olleet kyberturvallisuuden murrosvaihetta. Kehitys ei ole kuitenkaan ollut suhteessa turvallisuusympäristön muutoksen nopeuteen: teknologinen murros ja uudentyyppiset kyberuhkat etenevät nopeammin kuin organisaatioiden ja toimialojen varautuminen. Suomelle tämä tarkoittaa tarvetta yhtenäiseen ja pitkäjänteiseen kyberturvallisuuden kehittämiseen ja panostuksiin, joissa kyberturvallisuus nähdään huoltovarmuuden ja taloudellisen resilienssin perusrakenteena – ei irrallisena teknisenä kysymyksenä. On olemassa riski, että ilman selkeää kehitystoimenpiteiden tason nostoa näennäinen kehitys peittää alleen tosiasiallisen taantumisen suhteessa muuttuvaan uhkaympäristöön.

Maailma muuttuu nopeasti. Jos kyberturvallisuuden kehitys ei ota harppauksia eteenpäin, liikumme todellisuudessa taaksepäin.

Juha Ilkka, Huoltovarmuuskeskus
Ohjelmajohtaja, Digitaalinen turvallisuus 2030

Johdon tiivistelmä

Selvitys osoittaa, että kansallinen kyberkypsyyden taso on kehittynyt vuodesta 2022 vain maltillisesti. Samalla teknologian ja uhkakentän murros etenee merkittävästi nopeammin kuin organisaatioiden kyky uudistua ja investoida kyberturvallisuuteen.

Kehityksen hitaudesta kertoo se, että parannuskohteet ovat edelleen samoja, kuin kolme vuotta sitten tehdyssä selvityksessä. Samalla viidennes otannan yrityksistä jää matalalle kypsyystasolle.

Pienet ja keskisuuret yritykset sijoittuvat korostuneesti alemmille kypsyystasoille, eikä ilmiö selity yksinomaan resurssien rajallisuudella. Selkein puuttuva tekijä on ylimmän johdon tuki. Korkeamman tason yrityksissä johtoryhmä on tehnyt tietoisen päätöksen nostaa kyberturvallisuuden prioriteettia.

Verkostoituneessa yhteiskunnassa oma korkea kypsyystaso ei riitä suojaamaan uhkilta. Yhdistettynä toimitusketjujen riskienhallinnan heikkouksiin, altistuvat myös korkean kyberkypsyystason toimialat ja yritykset verkostojen kautta kyberuhkille. Riski korostuu entisestään, mikäli suomalaisten yritysten valmiustaso pääsee eriytymään liikaa.

Kyberuhkatietoisuus lisääntyy, mutta konkreettiset toimet jäävät jälkeen

Organisaatioiden kyberuhkatietoisuus on kasvanut ja johdon tietoisuus uhkista vahvistunut. Kuitenkin erityisesti matalamman kypsyystason yrityksissä kehitystä hidastavat resurssi- ja rakenteelliset puutteet sekä kyberturvallisuuden eriytyminen liiketoiminnasta.

Kyberriskienhallinnan kehitys on epätasaista, eikä sen tuottamaa tietoa kyetä hyödyntämään päätöksenteossa

Kyberriskienhallinnan taso vaihtelee merkittävästi eri toimialojen ja yritysten välillä. Korkeammalla tasolla se on liiketoimintalähtöistä ja aktiivista, kun taas erityisesti PK-sektorilla riskienhallinta on useammin satunnaista tai reaktiivista.

Häiriötilanteisiin varautuminen on ottanut harppauksen eteenpäin

Valtaosa yrityksistä on laatinut varautumissuunnitelman ainakin kriittisille palveluille ja monissa yrityksissä suunnitelmien laatiminen on myös johtanut konkreettisiin toimenpiteisiin. Kehitys on kuitenkin usein reaktiivista, ei ennakoivaa, ja harjoittelua tehdään edelleen vain vähän.

Suositukset

Suositukset perustuvat toimialoja läpileikkaaviin kehityskohteisiin ja ne ovat esitetty kriittisyysjärjestyksessä suhteessa selvityksessä tunnistettuihin kyberuhkiin. Yrityksille kohdistetut suositukset ovat koostettu toimiala-kohtaisiin raportteihin.

Yhteiskunnan kybervarautumista edistävät suositukset:

Toimitusketjujen kyberturvallisuus huomioitava laajemmin
Kansallinen kyberkypsyyden hidas kehitys ja yritysten valmiustason eriytyminen voi uhata kaikkia kokonaisketjun yrityksiä kypsyystasosta riippumatta. Toimitusketjujen riskien- ja kyberturvallisuuden hallinta on keskeinen kehitettävä kyvykkyys yrityksen kyberkypsyystasosta riippumatta.

Yhteisharjoittelu yhteiskunnallisesti ja toimialoittain on tärkeää
Yhteisharjoitukset ovat monille pk-yrityksille ainoa tapa harjoitella jatkuvuuden hallintaa. Siksi ne ovat tärkeitä paitsi näille yrityksille, myös korkeamman kypsyystason organisaatioille, jotka voivat altistua toimitusketjun kyberturvapoikkeamille.

Kyberturvallisuuslain toimeenpano
NIS2-direktiivin kansallisen toimeenpanon valvonnassa tulee painottaa käytännön toteutusta. Yrityksiltä on vaadittava konkreettisia todisteita kyberturvatoimien jalkautumisesta, jotta laki nostaa todellista eikä näennäistä kypsyyttä.

Liiketoimintajohtajille suunnattu kyberturvallisuuskoulutus
Johdon kyberuhkatietoisuuden heijastuminen käytännön kyberkypsyyteen vaatii koulutusta, joka puhuttelee kohderyhmää ja kytkee kyberturvallisuuden suoraan liiketoiminnan jatkuvuuteen ja taloudelliseen menestykseen.

Liiketoiminnan jatkuvuutta edistävät suositukset:

Johdon osallistuminen avain kyberkypsyystason nostoon
Tukea voi edistää aktiivisella yhteistyöllä ja seurattavilla mittareilla sekä kehittämällä johdon kyberturvallisuusosaamista kohdennetuin koulutuksin.

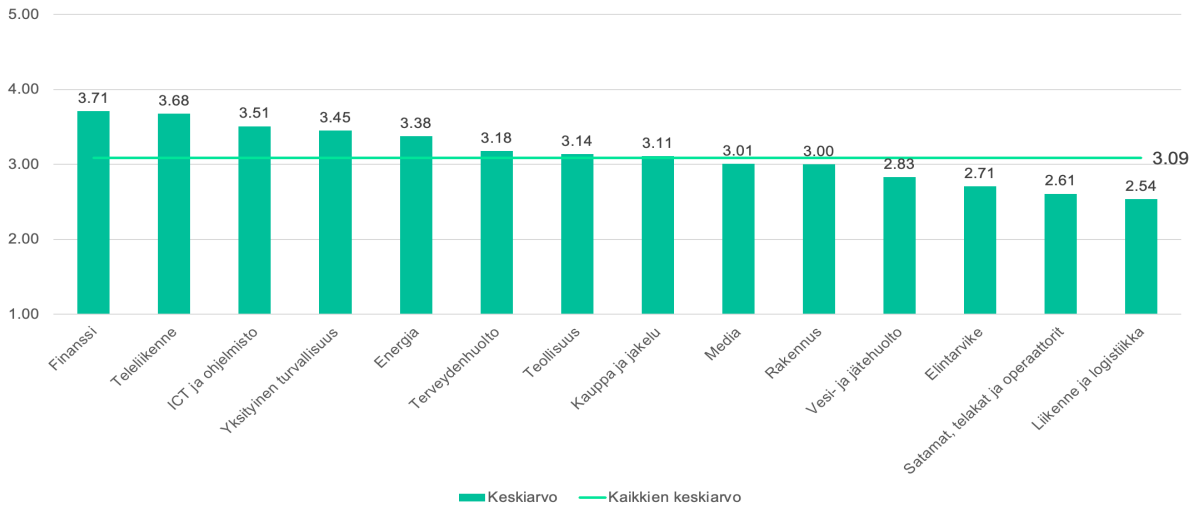
Kyberturvallisuusosaamisen kehittäminen
Yritysten tulisi organisaation koosta ja toimialasta riippuen varmistaa riittävä kyberturvallisuusosaamisen taso palkkaamalla asiantuntijoita, hyödyntämällä kumppaneita sekä tukemalla työntekijöiden uudelleenkouluttautumista.

Kokonaisvaltainen turvallisuusjohtaminen
Monissa organisaatioissa kyberturvallisuus, teollisuus- ja tuotantojärjestelmien (OT) turvallisuus sekä fyysinen turvallisuus johdetaan erillisinä kokonaisuuksina. Yhtenäinen tilannekuva parantaa kyberriskien ja resurssien priorisointia sekä auttaa tunnistamaan laajempia vaikuttamisyrityksiä.

Operatiivisen kyberriskienhallinnan sisällyttäminen osaksi liiketoiminnan kokonaisvaltaista riskienhallintaa
Erityisesti pienissä ja keskisuurissa yrityksissä kyberriskienhallinta on vähäistä, reaktiivista ja irrallista muusta liiketoiminnan riskienhallinnasta.

Tulokset

Kansallinen kyberkypsyys kehittyy hitaasti eikä yritysten kyky uudistua ja investoida kyberturvallisuuteen pysy uhkakentän ja teknologisen murroksen perässä. Kansallisesti tarkasteltuna suurin osa ylittää perustasona pidetyn 3.00, mutta osa kriittisistä toimialoista jää kyberkypsyydessään kohtuulliselle tasolle.



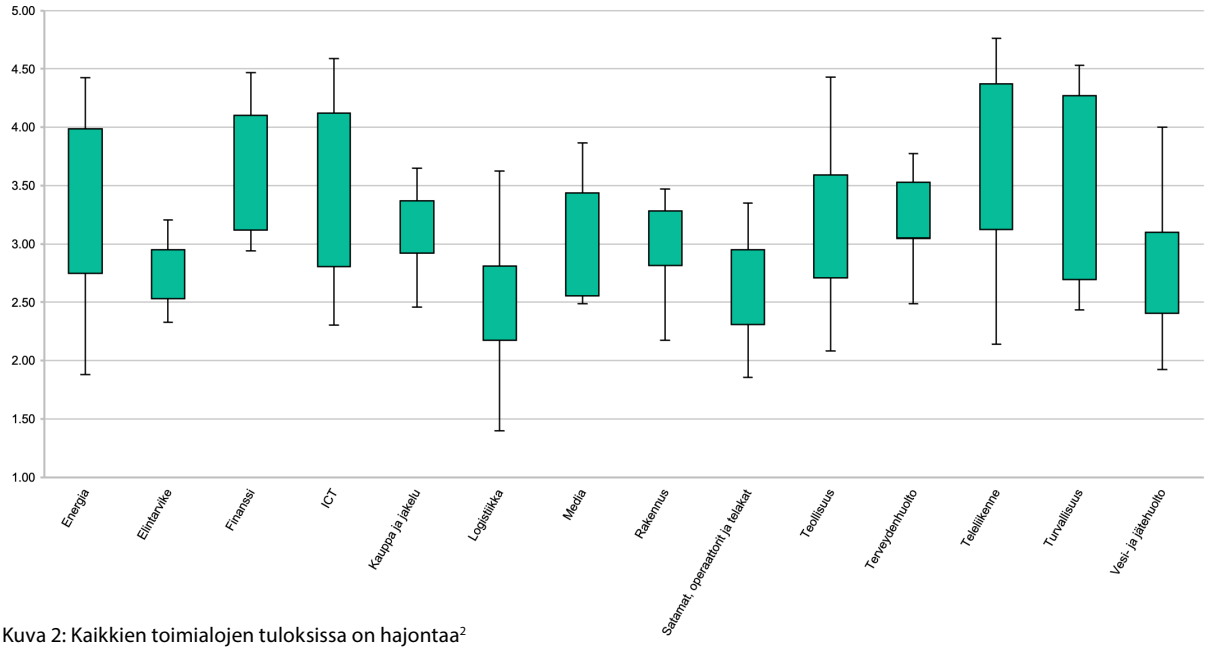
Kuva 1: Toimialavertailu keskiarvoittain*[1]

Vahvasti kyberturvallisuuden osalta säännellyt toimialat, kuten finanssi-, teleliikenne- ja ICT-alat ovat toimialavertailun kärjessä. Näillä toimialoilla kyberturvallisuutta on kehitetty liiketoimintalähtöisesti ja tavoitteellisesti jo pitkään. Yrityksillä on ollut mahdollisuus määritellä kyberturvallisuuden johtamisen ja hallinnan malleja sekä mitata ja arvioida niiden vaikuttavuutta pitkällä aikavälillä. Toimialavertailun loppupäässä on aloja, joilla digitalisaation eteneminen on ollut perinteisesti hitaampaa ja kyberturvallisuus on jäänyt vahvemmin liiketoiminnasta erilliseksi tukitoiminnoksi.

Merkittävimpänä kybertilannekuvaan vaikuttavana tekijänä nousi haastatteluissa NIS2-direktiivi ja sen kansallinen toimeenpano kyberturvallisuuslakina. Kansallinen lainsäädäntö tuli voimaan selvityksen ollessa jo käynnissä. Valtaosassa yrityksiä lainsäädännön tuomiin muutoksiin valmistautuminen oli käynnistänyt kehitystoimia esimerkiksi kyberturvallisuuden hallinnan systematisoimisessa, riskienhallinnan toimintamallin määrittelyssä tai toimitusketjujen kartoittamisessa. Asennoituminen sääntelyyn vaihteli yritysten keskuudessa. Parhaimmissa tapauksissa kehitykseen ei suhtauduta kertaluontoisena projektina, vaan yritysten kyberturvallisuusvastaavat olivat käyttäneet velvoitteita vipuvartena pidemmän aikavälin kehityssuunnitelmien läpiviennille.

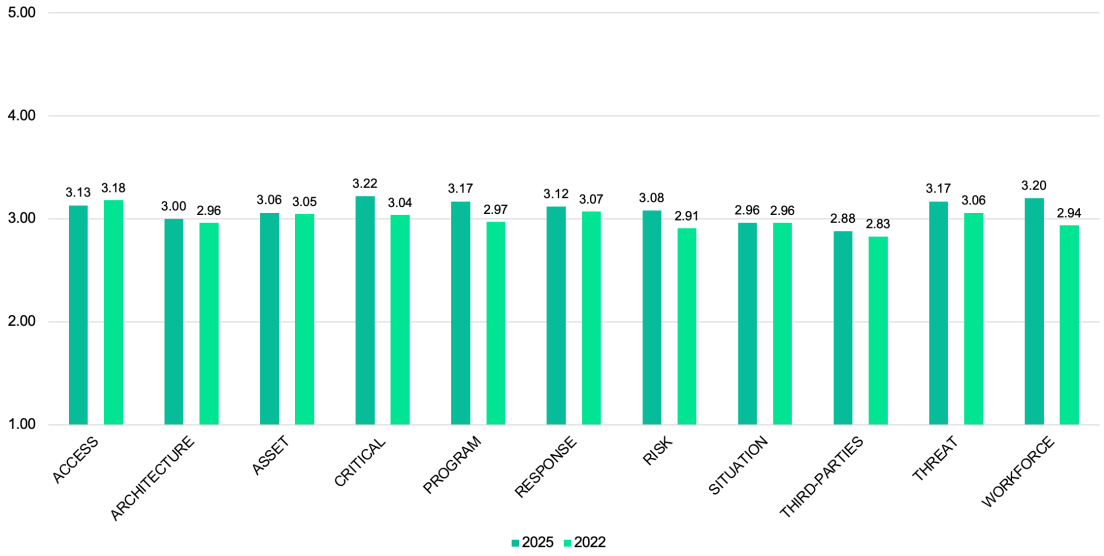
Erityisesti yritysten välillä tasoerot ovat huomattavia ja viidesosa jää matalalle tasolle. Parhaiten pärjänneisiin kuuluu erityyppisiä yrityksiä keskikokoisista suuryrityksiin. Osa on vahvasti säännellyiltä toimialoilta, kun taas osa on uudempia ja kasvavia teknologiayrityksiä. Parhaiten pärjänneitä yrityksiä tarkastellessa voidaan todeta, ettei organisaation pienempi koko ole korkeaa kyberkypsyyttä estävä tekijä, mutta määrällisesti matalammilta kypsyystasoilta löytyy enemmän pieniä ja keskisuuria yrityksiä.

[1]*Kaikkien toimialojen keskiarvo 3.09 on laskettu yrityskohtaisista tuloksista. Toimialojen keskiarvojen yhteenlaskettu keskiarvo antaa eri tuloksen. Toimialojen otoskoot vaihtelevat, jonka vuoksi yksittäisen yrityksen tulosten painoarvo vaihtelee toimialoittain.



Kuva 2: Kaikkien toimialojen tuloksissa on hajontaa[2]

Muutos vuoteen 2022 nähden



Kuva 3: Kybermittarin osa-aluekohtaiset tulokset vuosina 2022 ja 2025*[3]

Toimialojen kyberkypsyysselvitys toteutettiin edellisen kerran vuonna 2022, jolloin arvioitiin 121 yrityksen kyberkypsyys. Vuoden 2025 selvityksessä yrityksiä on 146 ja kokonaan uusia toimialoja ovat rakennusala ja yksityinen turva-ala, jonka lisäksi muiden toimialojen otannoissa on tapahtunut muutoksia, jotka on kuvattu tarkemmin menetelmäkuvauksessa*[4]

Aihealueittain tarkasteltuna yritysten kyberkypsyys ei ole merkittävästi muuttunut ja pienet numeraaliset muutokset voivat olla selitettävissä otannan muutoksilla (Kuva 3). Myöskään haastatteluiden perusteella kybertilannekuva ei ole merkittävästi muuttunut vuosien välillä. Yritykset kamppailevat edelleen samojen aiheiden, kuten resurssien ja kyberosaamisen niukkuuden kanssa. Vuoden 2022 tavoin vahvuudet ja kehityskohteet ovat edelleen lähinnä yrityskohtaisia, sillä saman toimialan sisällä voi olla täysin eritasoisia toteutuksia. Yleisimpinä heikkouksina on vuoden 2022 lailla häiriötilanteiden harjoittelun vähäisyys, riskienhallinta ja etenkin kolmansien osapuolten riskienhallinta. etenkin kolmansien osapuolten riskienhallinta. Lisäksi

[2]Kuva osoittaa yrityskohtaisten tulosten hajonnan toimialoittain. Kuvaan on merkitty mustilla viivoilla toimialakohtaisten tulosten vaihteluväli ja vihreällä palkilla, mihin 50 % vastauksista sijoittuu. Hajontaa tarkastellessa on huomioitava, että toimialojen otannat vaihtelevat 7 ja 15 yrityksen välillä. Toimialojen otantojen kappalemäärät on esitelty tarkemmin raportin liitteissä (Taulukko 1).
[3] Aihealueet pohjautuvat Liikenne- ja viestintävirasto Traficomin Kybermittariin ja niiden sisältö on tarkemmin avattu menetelmäkuvauksessa raportin lopussa
[4] Toimialojen otannat 2025 selvityksessä ja muutokset vuoteen 2022 verrattuna on kuvattu menetelmäosuudessa raportin lopussa (Taulukko 1)

teollisuus- ja tuotantoympäristöjen (OT) hallinnan eriytyneisyys jatkuu kyberkypsyyttä laskevana trendinä sellaisilla toimialoilla, joita se koskee.

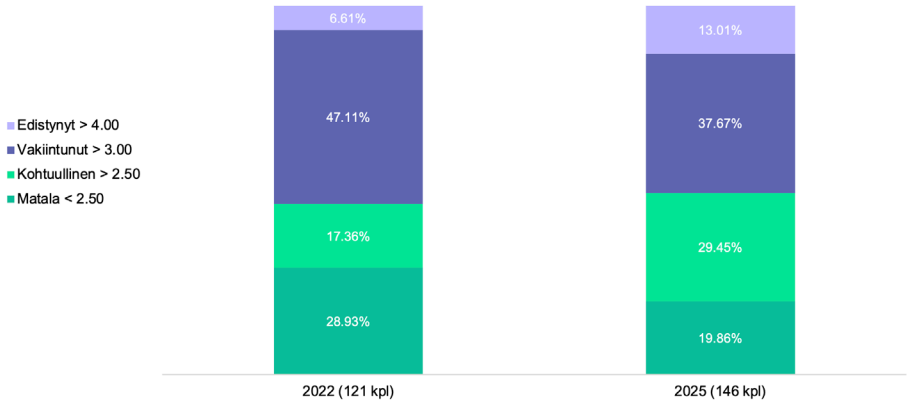
Vaikka kaikkien toimialojen keskiarvo on noussut vain kymmenyksellä (0.09) vuodesta 2022, kyberturvallisuuden hallinta on muuttumassa aiempaa järjestelmällisemmäksi ja johdon kiinnostus aihetta kohtaan on lisääntynyt. Haastatteluissa useat yritykset kuvasivat etenkin NIS2-direktiivin ja viestinnän kohonneesta kyberuhkatilanteesta johtaneen lisääntyneeseen kyberturva-aiheiden käsittelyyn johdon toimesta. Toisaalta johdon lisääntynyt kyberuhkatietoisuus havaittiin jo vuoden 2022 selvityksessä, mutta ainakaan vielä tietoisuuden lisääntyminen ei näy konkreettisesti kyberkypsyydessä.

Vuoden 2022 selvityksessä erityishuomiota kiinnitettiin kyberturvallisuustietoisuuden ja -osaamisen kehittämiseen ja korostettiin sitä, että osaamisen ja tietoisuuden ylläpito vaatii yrityksiltä jatkuvaa työtä. Osaamisen kehittämiseksi yrityksissä on tehty toimenpiteitä, sillä henkilöstön johtamisen ja kehittämisen osa-alueen (WORKFORCE) tulokset ovat nousseet eniten. NIS2-direktiivi ja kasvanut uhkatietoisuus ovat osaltaan tämänkin kehityssuunnan taustalla. Yleisesti yritykset pitävät kyberosaamiseen ja -tietoisuuteen panostamista tärkeänä sekä tukevat sitä erimuotoisilla, säännöllisillä koulutuksilla.

Kokonaisuutena toimialojen kyberkypsyystaso on pysynyt pitkälti ennallaan yksittäisistä positiivisista kehityssuunnista huolimatta. Merkittävää edistystä ei ole havaittavissa uhkatilanteen kiristymisestä huolimatta. Tulosten numeraalinen kasvu on hyvin vähäistä ja lähes jokaisella toimialalla on vastauksissa laajaa hajontaa. Vertailtaessa tuloksia vuoden 2022 raporttiin, huomionarvoista on myös se, että kehityskohteet ovat pysyneet lähestulkoon samoina. Haasteet siis tunnistetaan, mutta niihin ei löydetä kestäviä ratkaisuja.

Yritysten välisiä kypsyyseroja selittävät tekijät

Kuva 4 erottelee selvitykseen osallistuneiden yritysten jakauman vuosina 2022 ja 2025. Positiivisena kehityksenä voidaan pitää sitä, että alimmassa joukossa on vuonna 2025 pienempi määrä yrityksiä, mutta edelleen lähes viidennes otannasta jää matalalle tasolle.
Vertailussa on mukana yrityksiä kokoluokiltaan pienistä ja keskikokoista yrityksistä suuryrityksiin. Yritykset toimivat maantieteellisesti kaikkialla Suomessa, jonka lisäksi suurimmalla osalla on jonkinlaista kansainvälistä liiketoimintaa. Kaikki mukana olevat yritykset ovat kriittisiä huoltovarmuuden tai yhteiskunnan kriisinkestävyyden kannalta.

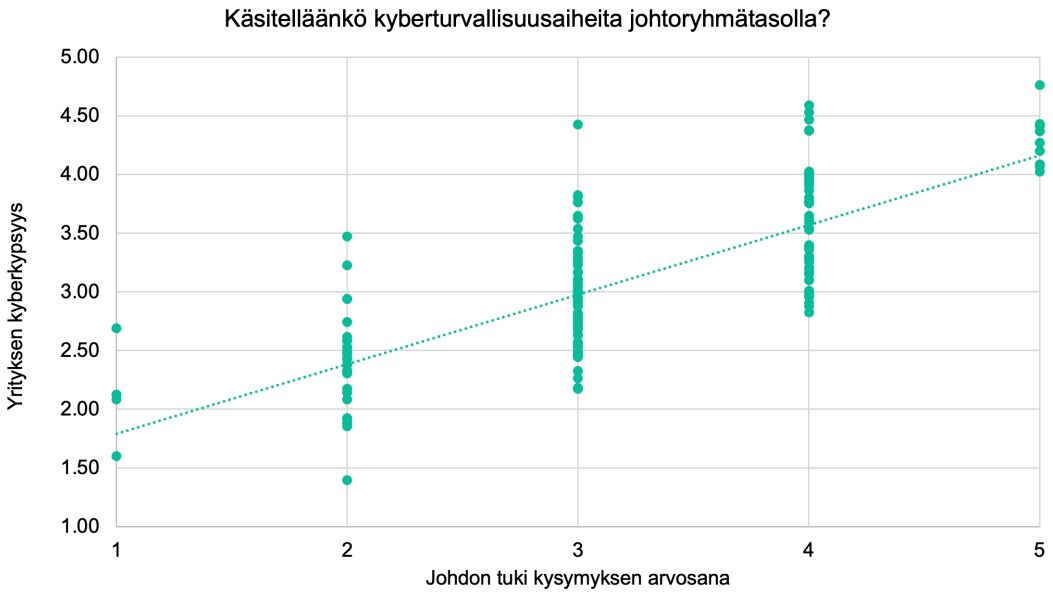


Kuva 4: Kummallakin selvityskerralla noin puolet yrityksistä ylittää tason 3.00 ja puolet jää sen alle

Kyberkypsyysvertailussa erittäin hyvin pärjänneet yritykset toteuttavat kyberturvallisuutta kerroksellisesti ja moniulotteisesti. Yrityksiä yhdistää ajattelu jatkuvasta ja aktiivisesta kehittämisestä sekä herkkyydestä kyberuhkatrendien ja toimintaympäristön muutoksiin.

Johdon tuki

Selkein yksittäinen tekijä korkean kypsyystason yritysten välillä on organisaation ylimmän johdon tuki. Kypsimmissä organisaatioissa johtoryhmä käsittelee strategisen tason kybertilannekuvaa sekä merkittävimpiä kyberriskejä ja niiden hallintatoimia. Haastatteluista käy ilmi, että näissä yrityksissä johtoryhmä on tehnyt tietoisen päätöksen nostaa kyberturvallisuuden prioriteettia, tehdä kyberturvallisuuteen liittyen strategisen tason ohjausta ja osoittaa sen toteuttamiseen tarvittavat resurssit. Johdon kykyä tehdä kyberturvallisuuteen liittyviä päätöksiä on osassa parhaiten sijoittuneista yrityksistä kehitetty johdolle suunnatulla kyberturvallisuuskoulutuksella.



Kuva 5: Johdon säännöllisellä käsittelyllä on vahva yhteys yrityksen kyberkypsyyteen

Kyberkypsyysvertailussa erittäin hyvin pärjänneet yritykset toteuttavat kyberturvallisuutta kerroksellisesti ja moniulotteisesti. Yrityksiä yhdistää ajattelu jatkuvasta ja aktiivisesta kehittämisestä sekä herkkyydestä kyberuhkatrendien ja toimintaympäristön muutoksiin.

Harjoittelu ja havainnointikyky

Parhaiten pärjänneet yritykset eivät tyydy hyvään suunnitteluun ja jatkuvaan kehittämiseen, vaan ylläpitävät jatkuvaa poikkeamien havainnointi- ja reagointikykyä. Häiriöiden tunnistamisen pohjana on monitasoinen ja ympärivuorokautinen valvontakyvykkyys. Huolimatta siitä, onko kyberturvavalvonta itse tuotettua tai ulkoistettua, valvomo (Security Operations Center, SOC) on saumaton osa kypsimpien yritysten varautumisorganisaatiota ja valvontakykyä. Myös häiriötilanteiden toimintatapoja kehitetään jatkuvasti läheisessä yhteistyössä.

Korkean kyberkypsyyden yritykset testaavat aktiivisesti kyberresilienssiään harjoittelemalla poikkeamatilanteiden hallintaa järjestelmien palauttamisesta laajempiin, koko organisaation jatkuvuusharjoituksiin. Lisäksi yritykset tekevät yhteisharjoittelua tärkeimpien kumppaneiden kanssa sekä osallistuvat toimialakohtaisiin ja kansallisiin jatkuvuusharjoituksiin.

Matalamman kyberkypsyyden tekijät

Matalammalle tasolle jäävillä yrityksillä on useammin käytännön tasolla muodostuneita toimintatapoja ja niihin liittyvä dokumentaatio on rajallisempaa. Kirjaamattomat prosessit vähentävät paitsi toiminnan säännöllisyyttä, määrämuotoisuutta ja mitattavuutta, ne luovat avainhenkilöriskejä, varsinkin kyberturvallisuushenkilöstön määrän ollessa usein vähäisempää näissä yrityksissä.

Matalalle ja kohtuulliselle tasolle jäävissä yrityksissä on selvitysaineiston perusteella useammin puutteita kyberturvallisuuteen liittyvässä henkilöresursoinnissa. Kyberturvallisuusvastaavat ovat yksin vastuussa kaikista kyberturvallisuuden osa-alueista tai tehtävät on voitu jopa liittää osaksi jotain muuta, jo itsessään kokopäiväistä työnkuvaa. Henkilömäärällisesti pienemmissä organisaatioissa isomman kyberturvatiimin palkkaaminen ei välttämättä ole tarkoituksenmukaista, mutta kokoluokaltaan pienemmätkään yritykset eivät voi ohittaa riittävän kyberosaamistason varmistamista esimerkiksi ulkoistamalla osan tehtävistä tai tukemalla henkilöstön kouluttautumista uusiin vastuualueisiin.

Käytännön tason varmistaminen jää usein puutteelliseksi matalamman kypsyystason yrityksissä. Nämä yritykset saattavat tehdä vuosikellon mukaisesti kyberturvallisuustehtäviä ja laatia erilaisia suunnitelmia, mutta kyberturvallisuuden teknisen toteutuksen taso jää epäselväksi ilman testaus- ja harjoittelukäytäntöjä. Varmistumisen puute näkyy myös siinä, ettei eri kyberturvallisuuden seurantaan ole mittareita eikä esimerkiksi ulkoistettuja palveluita tai kumppaneiden velvollisuuksien täyttymistä seurata.

Kyberuhkat

Viime vuosien aikana uhkataso on useiden viranomaisten[5] mukaan pysynyt jatkuvasti korkeana, mikä heijastuu myös selvityksen haastatteluissa. Valtiollinen kybertoiminta on aktiivista ja vakavat tapaukset ovat lisääntyneet. Haavoittuvuuksia hyödynnetään nopeammin ja kalastelu- sekä huijausyritykset ovat kasvussa. Keskeinen uhkatoimija kaikkien alla esitettyjen kyberuhkien taustalla voi olla valtiolliset toimijat, joita 43 % osallistuneista yrityksistä piti merkittävänä toiminnalleen. Niillä on laajat resurssit, osaaminen ja pidempikestoisia strategisia tavoitteita, joiden taustalla vaikuttavat sotilaalliset, poliittiset tai taloudelliset päämäärät. Kampanjat voivat olla osa hybridivaikuttamista tai teollisuusvakoilua, jonka 11,6 % yrityksistä nosti keskeiseksi kyberuhkaksi.

Toimitusketjuihin kohdistuvat hyökkäykset

- Hyökkääjä voi päästä kohdeorganisaation järjestelmiin, tietoihin tai ohjelmistoihin luotettujen kumppaneiden tai toimittajien kautta. Kriittiseen toimitusketjuun kuuluminen voi altistaa hyökkäyksille, vaikka organisaatio ei olisi hyökkäyksen ensisijainen kohde. Riippuvuus kriittisiä palveluita tarjoavista kumppaneista, kuten pilvestä, tietoliikenneyhteyksistä ja energiasta, korostui haastatteluissa. 80 % vastaajista koki toimitusketjuihin liittyvät kyberuhkat merkittäväksi.

Ohjelmistohaavoittuvuudet

- Tieto- ja tuotantojärjestelmien, sekä IoT-laitteiden haavoittuvuuksiin kohdistuvat tai niitä hyödyntävät kyberhyökkäykset, joiden tavoitteena on esimerkiksi tunkeutua järjestelmiin, häiritä tai keskeyttää toiminta tai vahingoittaa järjestelmiä.

Kiristyshaittaohjelmat

- Kiristyshaittaohjelma on haittaohjelman tyyppi, joka estää laitteen normaalin käytön, yleensä salaamalla tiedostot, joiden avaamiseksi hyökkääjä vaatii lunnaita. Kiristyshaittaohjelmia levitetään tavallisesti kohdennettujen tietomurtojen, roskapostin ja kalasteluviestien välityksellä.

Tietojenkalastelu

- Tietojenkalasteluhyökkäyksessä hyökkääjä pyrkii huijaamaan vastaanottajaa luovuttamaan luottamuksellisia tietoja, kuten käyttäjätunnuksia, salasanoja tai maksutietoja, esiintymällä luotettavana tahona sähköpostissa, tekstiviestissä tai puhelussa. Kalastelun tarkoituksenavoi olla myös haittaohjelman asentaminen tai järjestelmään tunkeutuminen. Noin kolmasosa vastaajista nosti kalastelun kriittiseksi kyberuhkaksi.

Sisäpiiriuhkat

- Henkilö, jolla on ollut tai on valtuutettu pääsy organisaation kriittisiin resursseihin, käyttää pääsyä, joko tahallisesti tai tahattomasti, tavalla, joka vaikuttaa organisaatioon haitallisesti.

Tekoälypohjaiset hyökkäykset

- Tekoälyn nopean kehittymisen myötä vakuuttavamman sosiaalisen manipuloinnin ja erilaisten huijausten uhka nousee, samoin hyökkäysten tai niiden osien automatisointi. Lisäksi uhkana on tietovuodot tekoälytyökalujen hallitsemattoman käytön kautta.

[5] Mm. Traficom ja Supo: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/traficom-ja-supo-kyberturvallisuuden-uhkataso-pysynyt-koholla-vakavien-tapausten

Johtopäätökset

Kyberuhkatietoisuus jatkaa kehittymistään, mutta konkreettiset toimet jäävät jälkeen

Jo edellisellä selvityskierroksella vuonna 2022 havaittiin, että turvallisuusympäristöön merkittävästi vaikuttavat tapahtumat nostavat ainakin hetkellisesti organisaatioiden kyberturvatietoisuutta. Tällaisia tapahtumia ovat esimerkiksi geopoliittiset muutokset tai julkisuuteen nousseet kyberhyökkäykset, erityisesti verrokkiorganisaatioissa. Kyberturvallisuuden asiantuntijoiden uhkatietoisuutta kehittävät haastatteluiden perusteella erityisesti kyberturvallisuusalan verkostot ja toimialakohtaiset tiedonvaihtofoorumit. Kasvanut tietoisuus kiristyneestä kyberuhkaympäristöstä ei kuitenkaan edelleenkään näy automaattisesti yritysten arjen toimintamalleissa. Haasteena useassa organisaatiossa on kyberturvatietoisuuden keskittyminen. Tällöin esimerkiksi johto ei välttämättä näe uhkatilanteen kehitystä liiketoiminnan viitekehyksessä, eikä heillä ole kannustinta resursoida kyberturvallisuuden kehitystä riittävästi.

Matalamman kypsyystason toimialoilla uhkakentän laajentuminen tiedostetaan, mutta useat organisaatiot arvioivat asemaansa houkuttelevana hyökkäyskohteena varsin kapeasti. Erityisesti osa pienemmistä yrityksistä ei hahmota omaa paikkaansa kokonaisketjussa, mikä näkyy kybervarautumisen matalampana tasona. Erityisesti toimialoilla, joilla digitalisaation taso on matala, haastattelut osoittivat, että yritykset ovat saattaneet tehdä tietoisen päätöksen rajoittaa kyberturvallisuusinvestointeja. Taustalla on käsitys, että jopa kaikkia digitaalisia järjestelmiä lamaannuttavaa kyberhyökkäystä ei pidetä liiketoiminnan jatkuvuuden kannalta kriittisenä uhkana. PK-yritysten matala kyberkypsyyden taso muodostaa riskin myös korkeamman kypsyystason organisaatioille niin toimitusketjujen teknisten ja toiminnallisten rajapintojen kuin tiedon luottamuksellisuuden näkökulmasta. Valtiolliset kyberuhkatoimijat ja vakoilu korostuivat haastatteluissa käydyissä uhkakeskusteluissa. Siitä huolimatta kybervarautumisen yhteydessä ei laajasti käsitelty toimenpiteitä, joilla varmistettaisiin, ettei organisaatio menetä omaa tai asiakkaidensa luottamuksellista tietoa huomaamatta.

Yksi kehitystä hidastava tekijä on se, että kyberturvallisuus nähdään edelleen vuoden 2022 tavoin usein liiketoiminnasta erillisenä tukitoimintona, joka näkyy resursointihaasteina ja kehityksen kankeutena. Riskilähtöisiä päätöksiä ei voida tehdä, jos kyberriskit eivät välity liiketoiminnallisiin päätöksiin. Tietoisuus ei myöskään voi muuttua suorituskyvyksi ilman mittareita eivätkä monet matalamman tason yrityksistä ole asettaneet tavoitteita, joita vasten kehitystä voitaisiin mitata. Usein syy konkreettisen tason kehityksen hitaudessa ei ole välinpitämättömyys vaan rakenteiden ja resurssien puute. Kun johdon ja kyberturvallisuustoimintojen välinen vuoropuhelu ei ole säännöllistä ja toimivaa, tieto ei kulje kybervastaavilta liiketoimintaan ja riskit eivät muutu prioriteeteiksi tai toimenpiteiksi.

Kyberriskienhallinnan kehitys on epätasaista, eikä sen tuottamaa tietoa kyetä hyödyntämään päätöksenteossa

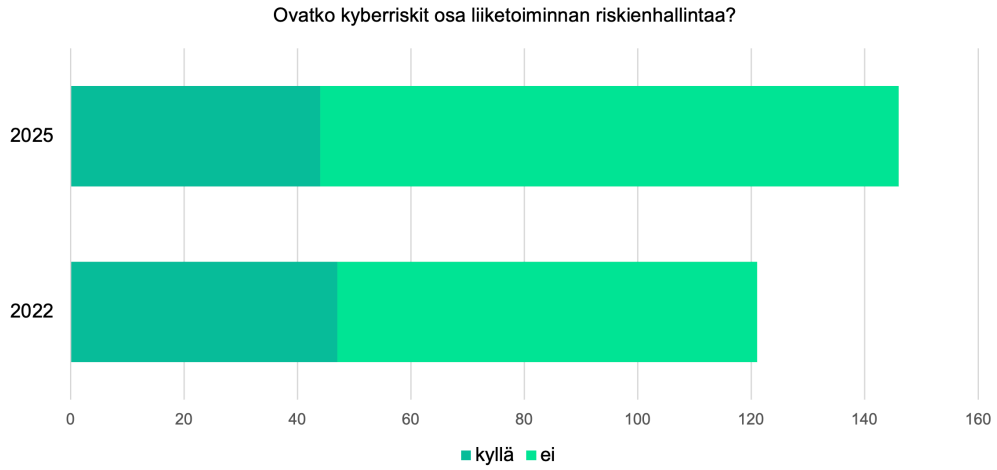
Organisaatioiden kyberriskien hallinta vaihtelee merkittävästi. Haastatteluissa havaittiin, että NIS2-direktiivin asettamat riskienhallinnan velvoitteet ovat johtaneet siihen, että monissa organisaatioissa oli haastatteluhetkellä juuri valmistuneita kyberriskienhallinnan toimintamalleja, joiden käytännön soveltaminen on vielä edessä. Edelleen voidaan kuitenkin todeta, että varsinkin PK-sektorilla kyberriskien hallintaa tehdään vähemmän, erityisesti osana jokapäiväistä toimintaa.

Kyberriskienhallinta on tyypillisesti vakiintuneella tasolla korkeamman kyberkypsyysarvion saaneilla toimialoilla, kuten finanssi-, teleliikenne-, ICT ja ohjelmisto- sekä energia-aloilla. Näillä toimialoilla erityisesti suuret yritykset tekevät systemaattista ja kattavaa kyberriskienhallintaa sekä operatiivisella että strategisella tasolla. Strategisen tason kyberriskejä seurataan organisaation ylimmällä tasolla, jolloin myös yritysten johto on ottanut kyberriskien seurannan luonnolliseksi osaksi liiketoiminnan riskienhallintaa.

Vuoden 2022 kyberkypsyysselvityksessä kyberriskienhallinta oli vielä tyypillisesti erillinen oma toimintonsa ja tulosten valossa tilanne näyttää jopa heikentyneen hieman selvityskierrosten välillä (Kuva 6).

Selvitysaineiston perusteella matalan tason toimijoilta kyberriskienhallinta puuttuu kokonaan tai sitä tehdään tapauskohtaisesti, reaktiona jo toteutuneisiin uhkakuviin. Reaktiivinen toiminta jättää organisaation haavoittuvaksi, koska kyberturvallisuuteen liittyviä päätöksiä ja kehitystöitä ei voida priorisoida riskipohjaiseen tietoon perustuen. Jo vuonna 2022 havaittiin, että riskienhallintaa saatetaan tehdä vain rajatussa osassa organisaatiota tai kyberriskejä käsitellään ainoastaan kyberturva-asiantuntijoiden kesken. Haastatteluissa havaittiin, että kyberriskin, kyberuhkan ja haavoittuvuuden käsitteet menevät usein matalamman kyberkypsyystason yrityksissä sekaisin. Sama havainto tehtiin myös edellisellä selvityskierroksella, sillä silloin kyberturvallisuuden asiantuntijat mielsivät riskienhallinnan usein tekniseksi uhkien ja haavoittuvuuksien hallinnaksi. Vaikka vuonna 2025 yhä useampi organi-

saatio ymmärtää asioiden eron, tämän kaltainen toiminta voi johtaa väärään priorisointiin ja tekee aidosti riskipohjaisesta päätöksenteosta mahdotonta. Erityisesti pienissä ja keskisuurissa yrityksissä on haasteita tunnistettujen kyberuhkien konkretisoitumisen vaikutusten ja niiden kriittisyyden arvioinnissa, eli arvioinnista jää puuttumaan keskeinen näkökulma riskilähtöisen toiminnan mahdollistamiseksi. Lisäksi näille yrityksille on usein myös haastavaa tunnistaa juuri omaan ydinliiketoimintaan vaikuttavat kyberriskit, sillä selvityksen haastatteluissa usein nousi esiin ilmiöitä, joita on ollut laajemmin esillä esimerkiksi mediassa.



Kuva 6: Kuvassa yritysten vastaukset ovat esitetty kappalemäärittäin vuosien 2022 ja 2025 välillä

Selvitysaineiston perusteella matalan tason toimijoilta kyberriskienhallinta puuttuu kokonaan tai sitä tehdään tapauskohtaisesti, reaktiona jo toteutuneisiin uhkakuviin. Reaktiivinen toiminta jättää organisaation haavoittuvaksi, koska kyberturvallisuuteen liittyviä päätöksiä ja kehitystöitä ei voida priorisoida riskipohjaiseen tietoon perustuen. Jo vuonna 2022 havaittiin, että riskienhallintaa saatetaan tehdä vain rajatussa osassa organisaatiota tai kyberriskejä käsitellään ainoastaan kyberturva-asiantuntijoiden kesken. Haastatteluissa havaittiin, että kyberriskin, kyberuhkan ja haavoittuvuuden käsitteet menevät usein matalamman kyberkypsyystason yrityksissä sekaisin. Sama havainto tehtiin myös edellisellä selvityskierroksella, sillä silloin kyberturvallisuuden asiantuntijat mielsivät riskienhallinnan usein tekniseksi uhkien ja haavoittuvuuksien hallinnaksi. Vaikka vuonna 2025 yhä useampi organisaatio ymmärtää asioiden eron, tämän kaltainen toiminta voi johtaa väärään priorisointiin ja tekee aidosti riskipohjaisesta päätöksenteosta mahdotonta. Erityisesti pienissä ja keskisuurissa yrityksissä on haasteita tunnistettujen kyberuhkien konkretisoitumisen vaikutusten ja niiden kriittisyyden arvioinnissa, eli arvioinnista jää puuttumaan keskeinen näkökulma riskilähtöisen toiminnan mahdollistamiseksi. Lisäksi näille yrityksille on usein myös haastavaa tunnistaa juuri omaan ydinliiketoimintaan vaikuttavat kyberriskit, sillä selvityksen haastatteluissa usein nousi esiin ilmiöitä, joita on ollut laajemmin esillä esimerkiksi mediassa.
Yrityksissä, joissa kyberriskien hallinta perustuu vaatimustenmukaisuuteen, käytännön toteutus on usein kesken tai kokonaan aloittamatta. Erityisesti riskien säännönmukaisessa tunnistamisessa on haasteita ja uusia tai päivitettyjä riskejä nostetaan prosessiin mukaan harvoin. Lisäksi kyberriskienhallinta on siiloutunutta ja esimerkiksi tuotantoympäristöihin liittyvät riskit puuttuvat prosesseista, vaikka ne olisivat liiketoiminnalle hyvin merkityksellisiä. Riskienhallinta sekoittuu osassa vastauksista kyberuhkien ja haavoittuvuuksien lisäksi myös eritasoisiin varautumis- ja jatkuvuussuunnitelmiin, mikä kertoo siitä, etteivät riskienhallinnan toimenpiteet toteudu suunnitellusti.

Kumppaniriskienhallinta:

Kolmansien osapuolten riskienhallinta on selvityksessä kartoitetuista osa-alueista heikoin, vaikka 80 % selvitykseen osallistuneista yrityksistä on tunnistanut toimitusketjut yhtenä keskeisenä kyberuhkana. Toimitusketjujen kokonaisvaltainen hallinta arvioitiin matalalle kypsyystasolle ja nostettiin esiin selkeänä kehityskohteena jo vuonna 2022. Riippuvuuksien tunnistamisessa on kuitenkin yleisesti kehitytty edellisen selvityksen useampi yritys on kartoittanut toimitusketjuaan ensimmäistä linkkiä pidemmälle.

Kumppaneiden vastuulla on moni liiketoiminnalle kriittinen toiminto, mutta tästä huolimatta kumppaniriskienhallinnan käytännöt eivät ole vielä kaikilla yrityksillä vakiintuneella tasolla.

Kumppaniriskienhallinnan haasteet liittyvät erityisesti riippuvuuksien tunnistamiseen, johtamiseen ja vastuu jakoon sekä kyberturvallisuusvaatimusten asettamiseen ja niiden toteutumisen seurantaan. Selvityksessä on mukana useita yrityksiä, joissa ei ole selkeää tietoa

siitä, mitä ja miten kumppani tuottaa heille palveluita tai miten palveluntarjoaja huolehtii omasta kyberturvallisuudestaan. Kumppaneihin luotetaan usein oletusarvoisesti ilman turvallisuuskäytäntöjen arviointia tai tuntemista, etenkin jos taustalla on pidempi sopimussuhde. Vesi- ja jätehuollon, liikenteen ja logistiikan sekä kaupan ja jakelun toimialoilla tämä on tunnistettu koko toimialaa koskevaksi haasteeksi. Samoja haasteita esiintyi myös vuoden 2022 selvityksessä, mutta tällä kertaa joukosta löytyy myös enemmän yrityksiä, joilla on kattavia kumppaniriskienhallinnan ohjelmia, joihin kuuluu säännöllisiä auditointeja tai tarkastuksia. Koska toimitusketjujen kautta realisoituvat uhkat ovat tavallisesti arvioitu kriittisiksi, toimitusketjuja on pyritty kartoittamaan pitkälle ja osa yrityksistä seuraa tilannetta ohjelmistokirjastojen tasolle asti.

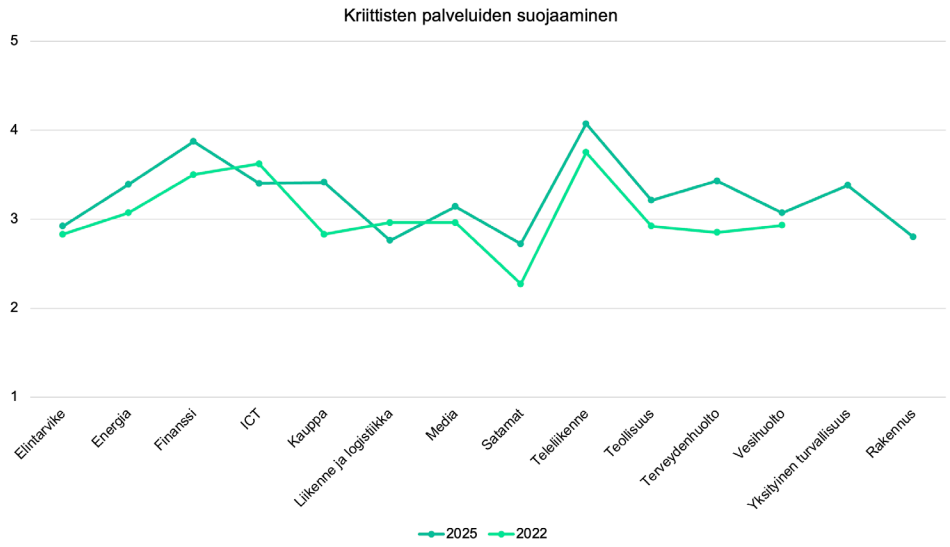
Häiriötilanteisiin varautuminen on ottanut harppauksen eteenpäin

Vaikka yleisessä kyberkypsyyden tasossa ei ole nähtävissä merkittävää nousua, selvitysaineiston mukaan yritysten varautuminen häiriötilanteisiin on lisääntynyt. Valtaosa yrityksistä on laatinut varautumissuunnitelman ainakin kriittisiksi tunnistamilleen palveluille ja monissa yrityksissä suunnitelmien laatiminen on myös johtanut konkreettisiin varautumistoimenpiteisiin. Kokonaistilanteen parantumisen taustalla ovat haastatteluiden mukaan ainakin NIS2-direktiivin varautumisvaatimukset ja yleinen uhkatilanteen kehitys.

Vaikka varautuminen on kokonaisuutena kehittynyt, yritystasolla tarkasteltuna erot ovat suuria. Osa eroista selittyy sillä, etteivät kaikki yritykset ole ottaneet juuri kyberhäiriöitä riittävästi huomioon varautumissuunnitelmissaan. Haastatteluiden perusteella tämä johtuu ainakin siitä, etteivät kyberhäiriöiden vaikutukset ole yhtä suuria kaikkialla, koska yritysten häiriösietoisuudessa ja liiketoiminnan teknologiariippuvuudessa on vaihtelua. Toisaalta kaikissa matalamman kyberkypsyystason yrityksissä varautumiseen liittyvät päätökset eivät välttämättä perustu harkintaan uhkamallinnuksen, riskianalyysin tai tilannekuvan pohjalta. Usein varautumistoimenpiteet kohdistuvat vasta jo toteutuneisiin uhkiin. Esimerkiksi tietoliikenneyhteyksiä on kahdennettu vasta kaapelivaurioista aiheutuneen teleoperaattoreihin kohdistuvan luottamuksen heikentymisen jälkeen sen sijaan, että kriittisiä riippuvuuksia olisi arvioitu ja niihin olisi varauduttu ennakolta.

Useimmin matalampi kybervarautumisen taso johtuu kuitenkin resurssien tai osaamisen puutteesta. Erityisesti harjoittelua tehdään vielä verrattain vähän eli varautumissuunnitelmien toimivuutta käytännössä ei kyetä todentamaan ja suunnitelmien säännöllinen kehitys ja päivittäminen jää tekemättä. Jatkuvuusharjoituksilla joko toimialan sisäisesti tai laajemmin yhteiskunnan tasolla on kybervarautumista edistävä vaikutus erityisesti pienissä ja keskisuurissa yrityksissä, joissa yhteisharjoittelu on ainoita keinoja harjoitella häiriötilanteiden hallintaa käytännössä. Yhteisharjoittelu voi muodostaa perustavanlaatuisen osan jopa kokonaisen toimialan varautumisesta.

Tietyillä toimialoilla varautuminen on vakiintunut osa kulttuuria ja kyberhäiriöt on huomioitu laajasti osana suunnitelmia ja niitä päivitetään jatkuvasti osana prosessia ja harjoituksista saaduilla käytännön opeilla. Korkeammalla tasolla olevilla yrityksillä harjoittelu on monitasoista yksittäisten järjestelmien palauttamisesta laajoihin kriisiharjoituksiin yhdessä ylimmän johdon ja sidosryhmien kanssa. Korkean kypsyystason yrityksillä on myös konkreettisella tasolla monipuolisia varautumistoimenpiteitä, kuten varajärjestelmiä, eriytettyjä ympäristöjä ja kahdennuksia.



Kuva 7: Kahta lukuun ottamatta kaikkien toimialojen keskiarvo on noussut osa-alueessa, joka mittaa kriittisten palveluiden tunnistamista, suojaamista ja niihin kohdistuviin häiriöihin varautumista

Liitteet

Menetelmä

Toimialojen kyberkypsyyden selvitys

Kyberkypsyys toimialoilla 2025 on Huoltovarmuuskeskuksen rahoittama ja Huoltovarmuusorganisaation Digipoolin tilaama selvitys, jonka toteuttajana toimii Accenture. Selvitys on osa Huoltovarmuuskeskuksen Digitaalinen Turvallisuus 2030 -ohjelmaa1 (DT2030) ja jatkaa vuosina 2019–2020 ja 2022 toteutettujen selvitysten kokonaisuutta. Vuonna 2025 toteutetussa selvityksessä arvioitiin 146:n suomalaisen yrityksen kyberturvallisuustoimintaa neljällätoista huoltovarmuuskriittisellä toimialalla. Osallistuneiden toimijoiden valinnan tavoitteena oli tuottaa laaja otos eri toimialoista sekä erilaisista organisaatioista toimialojen sisällä. Toimialoja selvitykseen kertyi 14. Osallistujat valittiin ja kutsuttiin mukaan Huoltovarmuusorganisaation toimialapoolien avustuksella ja otokseen kerättiin huoltovarmuusketjun toimijoita monipuolisesti eri profiileilla, organisaation koon, toimialueen ja liiketoi mintamallin perusteella. Mukana oli vaihtelevasti 7–15 kappaletta yritystä per toimiala. Toimialaraporteissa on pyritty painottamaan laadullista analyysiä suoran numeraalisen vertailun sijaan, koska toimialat eivät ole keskenään suoraan vertailukelpoisia. Myöskään osallistuvat yritykset eivät ole täysin samoja kuin vuonna 2022, mikä täytyy huomioida selvityskierrosten välistä vertailua tehdessä.

Toimiala- ja yritysvalinnat

Selvityksen toimialat päätettiin projektin ohjausryhmässä ja niiden pohjana käytettiin NIS2-direktiivissä määriteltyjä kriittisiä toimialoja. Taulukko 1 kuvaa toimialojen otannat ja muutokset vuodesta 2022.

Toimiala	2022	2025
Energia	Paikallisia ja valtakunnallisia energiayhtiöitä, jotka toimivat sähkön ja lämmön tuotannossa ja jakelussa sekä polttoainekaupassa, verkkopalveluiden ja siirtoinfrastruktuurin ylläpitäjinä sekä muita energia-alan teknologia- ja palveluyrityksiä.	Ei muutoksia
Finanssi	Pankit ja vakuutusyhtiöt	Lisätty taloushallinto
Teleliikenne	Teleoperaattorit	Ei muutoksia
ICT ja ohjelmisto	ICT- ja ohjelmistoalan yritykset	Ei muutoksia
Terveydenhuolto	Yksityiset ja julkiset terveydenhuollon toimijat	Poistettu julkiset terveydenhuollon toimijat
Teollisuus	Metsä-, kemia-, konepaja-, sekä puolustusteollisuus	Rakennusala eriytetty omaksi toimialaksi
Kauppa ja jakelu	Vähittäis- ja tukkukaupat, päivittäistavarakaupat, jakelu sekä ruokapalveluiden toimijat	Ei muutoksia
Media	Media-alan yritykset	Ei muutoksia
Vesihuolto	Vesihuollon yritykset	Lisätty jätehuolto
Elintarvike	Alkutuotanto ja elintarviketeollisuus	Ei muutoksia
Satamat, operaattorit ja telakat	Satamat, operaattorit, telakat ja merenkulku	Merilogistiikka eriytetty osaksi liikennettä ja logistiikkaa
Liikenne ja logistiikka	Ilma-, maa- ja raidekuljetukset	Lisätty meriliikenne

Rakennus		Infra- ja talorakennusalan yritykset
Yksityinen turvallisuus		Alan yritykset, jotka tarjoavat kulunhallinnan-, valvonta- ja hälytysjärjestelmien, lukitusratkaisujen sekä kameravalvonnan, turvateknologian, vartioinnin ja turvallisuuspalveluiden suunnittelun, asennuksen ja ylläpidon ratkaisuja

Taulukko 1: Selvityksen toimialat

Arviointityökalu

Kyberturvallisuuden maturiteettitason arvioimisessa hyödynnettiin Liikenne- ja viestintävirasto Traficomin Kybermittarista aihealueittain johdettua versiota. Selvityksessä käytetyssä versiossa osa-alueet säilytettiin samoina kuin alkuperäisessä Kybermittarissa, mutta osa-aluekohtaisia kysymyksiä tiivistettiin tai poistettiin työpajoissa käytössä olevan ajan vuoksi. Kybermittari oli päivitetty vuonna 2025 ja selvitystä varten käytettyä uutta versiota tiivistäessä varmistettiin, ettei se poikennut merkittävästi vuoden 2022 selvityksessä käytetystä versiosta.

Traficom on luonut materiaalin, joka vertailee Kybermittaria tässä selvityksessä käytettyyn tiivistettyyn vertailutyökaluun:
https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybermittari_vs_HVK_Digipoolin_toimialaselvitys-2025_vertailu.pdf

Osa-alue	Otsikko	Kuvaus
PROGRAM	Kyberturvallisuuden hallinta	Osa-alueessa arvioidaan organisaation kykyä hallita ja ylläpitää organisaation laajuista kyberturvallisuusohjelmaa.
ARCHITECTURE	Kyberturvallisuuden hallinta	Osa-alueessa arvioidaan organisaation kykyä hallita ja ylläpitää organisaation laajuista kyberturvallisuusohjelmaa.
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
THIRD-PARTIES	Kumppaniverkoston 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 poikkeamien hallinta	Osa-alueessa arvioidaan organisaatioiden kykyjä hallinnoida, reagoida sekä palautua kyberhäiriötilanteista.
ACCESS	Identiteetin- ja pääsynhallinta	Identiteetin- ja pääsynhallinta osa-alueessa arvioidaan organisaation kykyä hallinnoida ja rajoittaa loogisia ja fyysisiä pääsyoikeuksia yrityksen suojattavaan omaisuuteen.

Taulukko 2: Osa-alueiden kuvaukset

Mittaristo ja arviointikriteeristö

Kypsyysarvioiden mittaristo pohjasi yleiseen 5-tasoiseen kypsyysmalliin, kuten esimerkiksi CMM-mallissa (Capability Maturity Model, malli organisaatioiden prosessien kypsyystasoille). Taulukko 3 kuvaa eri kypsyystasojen yleisvaatimukset.

Kypsyystaso	Kuvaus
1	Ei määritelty. Organisaatio ei toteuta osa-alueeseen liittyviä käytäntöjä. Käytäntöjen mahdollinen toteuttaminen reaktiivista ja suunnittelematonta.
2	Organisaatio toteuttaa käytäntöjä tapauskohtaisesti ja tekeminen ei ole säännöllistä. Esimerkiksi joitain prosesseja on olemassa, mutta niitä ei ole dokumentoitu. Kehittämisen ja ylläpidon ei tarvitse olla systemaattista.
3	Toiminta systemaattista, esim. regulaatiolähtöistä. Toimintatavat ja prosessit dokumentoitu, mutta koskevat vain osaa toiminnoista, vaativat päivitystä tai niitä ei ole jalkautettu kauttaaltaan. Ei jatkuvaa arviointia / auditointia.
4	Organisaatiolla on dokumentoidut säännöllisesti toistettavat ja ylläpidettävät kyberturvallisuuden hallinnan mallit, vastuut ja valtuudet käytäntöjen toteuttamiseksi. Selkeät prosessit ja toimintatavat, joita noudatetaan ja niiden toteutumista valvotaan. Priorisointia tehty kriittisyyden ja riskiarvion perusteella.
5	Organisaatio toteuttaa käytäntöjä riskilähtöisesti, koko organisaation kattavia toimintamalleja ylläpidetään jatkuvasti ja kyberturvallisuudelle on määritetty tavoitteet, joita mitataan säännöllisesti. Toimintaa johdetaan strategisesti, organisaation johto on sitoutunut toimintaan. Käytössä toimintaa tukevat modernit teknologiset kyvykkyydet.

Taulukko 3: Kypsyysarvioiden mittaristo

Uhkakartoitus

Toimialauhkakartoitus toteutettiin osana työpajoja kaikkien osallistujien kanssa. Toimialauhkalistat perustuivat Accenturen globaaleista uhkatietoraporteista kerättyihin toimialauhkiin sekä Traficomin ja Digipoolin syötteistä tulleisiin näkemyksiin. Alkuperäisten uhkien lisäksi kartoituksessa huomioitiin ja listattiin työpajoissa ilmenneet yritysten näkemykset toistuvista toimialaa koskettavista uhkista. Uhkakartoituksessa heräteltiin keskustelua ennalta kerättyjen uhkien ja niiden määritelmien avulla ja haastateltavat arvioivat suullisesti niiden todennäköisyyttä ja vaikuttavuutta. Uhkat pisteytettiin lämpökarttaan frekvenssin ja merkittävyyden perusteella ja lisäksi niitä verrattiin eri osa-alueiden kypsyystasoon, jolloin esimerkiksi heikompi kypsyystaso osa-alueella nosti uhkan merkittävyyttä. Pisteytetyt uhkat huomioitiin yrityskohtaisissa suosituksissa. Tähän kansallisen tason raporttiin kerättiin kaikilla toimialoilla useimmin esiintyneet aihepiirit.

Työpajat

Työpajat toteutettiin edellä esiteltyjen työkalun ja uhkakartoituksen mukaan strukturoituna haastatteluina. Kohdeyritysten osallistujat vaihtelivat yrityksen mukaan, osalla osallistujina oli yksi tai kaksi kyberturvallisuuden asiantuntijaa (usein CISO), mutta monella osallistujia oli laajempi joukko mm. riskienhallinnan, tuotannollisen teknologian sekä yleis-IT:n edustajia. Kunkin osa-alueen kysymykset käytiin läpi kypsyysarvioiden muodostamiseksi, tarvittaessa pyydettiin tarkennuksia sekä esimerkkejä havainnollistamaan asioita, erityisesti erilaisten dokumenttien tai prosessikuvausten osalta.

Toimialakohtaiset yhteenvedot

Finanssi: Vakiintunut taso: 3.71

- Toimijajoukko sisälsi pankkeja ja vakuutusyhtiöitä. Lisäksi vuodesta 2022 poiketen mukana oli taloushallinnon yrityksiä, joiden osallistumisella ei arvioida olleen merkittävää vaikutusta toimialan kokonaiskeskiarvoon.

Vahvuudet

- Kyberturvallisuuden kehitystä on tehty jo pitkään, mikä tarkoittaa, että toimijoilla on ollut mahdollisuus määritellä kyberturvallisuuden johtamisen ja hallinnan malleja sekä mitata ja arvioida niiden vaikuttavuutta pitkällä aikavälillä.
- Finanssialan yritykset investoivat vahvasti henkilöstön kyberturvallisuusosaamiseen. Parhaisiin käytäntöihin kuuluvat mm. kyberturvallisuuteen keskittyvälle henkilöstölle varattu viikoittainen kouluttautumisaika ja roolikohtaiset kyberturvallisuuskoulutukset keskittyen kriittisiin rooleihin. Suurin osa toimijoista mittaa ja arvioi säännöllisesti kyberturvallisuusosaamisen tasoa suhteessa uhkatilanteeseen.
- Riskienhallinnan korkean kypsyystason taustalla ovat lainsäädäntö ja standardit, mutta useammalla alan yrityksellä kehitystä tehdään minimivaatimuksia pidemmälle. Parhaisiin käytäntöihin kuuluu mm. automatisoitua Due Diligence- skannausta.

Kehityskohteet:

- Kriittisin haaste liittyy riippuvuuteen legacy-infrastruktuurista. Muuten kypsällä tasolla olevia prosesseja ja teknisiä kyvykkyyksiä ei voida ylettää koko IT-infrastruktuuriin, jonka vuoksi kyberturvallisuuden kokonaistilannetta ei voida pitää riittävänä.
- Kehitettävää löytyy lisäksi tietoturvavalvonnasta, jonka taso vaihtelee yrityksissä. Kaikilla yrityksillä SOC-yhteistyö ei toimi saumattomasti niin, että palvelua kyettäisiin hyödyntämään hälytysten generointia pidemmälle. Kun monitorointipalvelua ei voida hyödyntää laajasti oman varautumisorganisaation jatkeena, yritykset menettävät kustannustehokkuutta ja kykyä vastata komplekseihin kyberuhkiin.
- Tietovarantojen hallinta on usein muuta omaisuudenhallintaa heikommalla tasolla. Yritykset kertovat haasteista ylläpitää rekisteriä tietovarannoista sekä kyvystä valvoa tiedon hyväksyttävää käyttöä, jakamista ja säilytystä.

Vertailu 2022–2025

- Finanssialan kyberkypsyys on noussut vuoden 2022 tasosta 3,34 vuoden 2025 keskiarvoon 3,71, mikä kertoo tasaisesta ja myönteisestä kehityksestä. Suurimmat parannukset on nähty kyberturvallisuuden hallinnassa, uhkien ja haavoittuvuuksien hallinnassa sekä kolmansien osapuolten riskienhallinnassa. Kehitystä ovat vauhdittaneet geopoliittiset jännitteet, kyberuhkien lisääntyminen ja tarkentuva sääntely, joka hallinnollisesta kuormasta huolimatta on ohjannut organisaatioita vahvistamaan häiriönsietokykyä ja strategista ohjausta. Henkilöstön osaamisen kehittäminen on edistynyt merkittävästi, mutta haasteita aiheuttavat edelleen omaisuudenhallinta, legacy-järjestelmät ja hajautetut ympäristöt. Valvontakäytännöt ja SOC-yhteistyö vaativat kehittämistä, vaikka parannusta on tapahtunut. Kokonaisuutena kehityssuunta on oikea, mutta korkean kypsyystason ylläpito edellyttää jatkuvia investointeja ja panostusta nopeasti muuttuvassa uhkaympäristössä.

Teleliikenne: Vakiintunut taso: 3.68

- Otanta koostuu suurista ja keskisuurista teleliikennealan toimijoista.

Vahvuudet

- Alan yrityksissä kyberturvallisuus on kiinteä osa organisaation johtamista ja kokonaisriskienhallintaa, ei erillinen tukitoiminto. Tietoturvan hallintamallit ja prosessit ovat vakiintunut osa jokapäiväistä toimintaa ja käytäntöjen vaikuttavuutta seurataan ja kehitetään jatkuvasti.
- Kypsimmissä organisaatioissa kriittisten palveluiden suojaus, varautuminen ja jatkuvuusharjoittelu ovat korkealla tasolla. Kypsyyttä tukevat lainsäädännön varautumisvaikutukset sekä johtoryhmien aktiivinen rooli kriittisten toimintojen ja palveluiden saatavuuden seurannassa, mikä näkyy myös riittävinä resursseina tietoturvatoiminnalle.
- Organisaatioilla on käytössä jatkuvat, automatisoidut haavoittuvuusskannaukset, joita tuetaan ajantasaisilla omaisuusrekistereillä. Säännölliset penetraatio- ja red teaming- harjoitukset täydentävät teknistä varautumista. Uhkatiedustelu on olennainen osa toimintaa ja yritykset hyödyntävät monilähteistä uhkatietoa teknisellä, taktisella ja strategisella tasolla. Kypsimmissä organisaatioissa tiedustelu on automatisoitu ja integroitu tietoturvavalvontaan.

Kehityskohteet:

- Toimialan tasapainoisempi kehitys vähentäisi alihankintaketjujen ja verkottuneiden toimintamallien kautta realisoituvia kyberuhkia ja -riskejä.
- Identiteetin- ja pääsynhallinnan alueella esiintyy joissain organisaatioissa käyttöoikeuksien kasaantumista ja manuaalisia käytäntöjä, jotka lisäävät riippuvuutta yksittäisistä henkilöistä ja heikentävät näkyvyyttä kokonaistilanteeseen. Myös omaisuudenhallinnan osalta manuaaliset käytännöt ovat osassa organisaatioista yleisiä, mikä rajoittaa näkyvyyttä ja hidastaa reagointia poikkeamiin.
- Kumppanien hallinnan osalta käytännöt ja vaatimusten kattavuus vaihtelevat huomattavasti. Kumppanien auditointikäytännöt ja sopimusvelvoitteet eivät ole kaikilta osin yhdenmukaisia, mikä vaikeuttaa toimitusketjun riskien arviointia ja valvonnan kokonaiskuvan muodostamista.

Vertailu 2022–2025

- Vuoden 2025 teleliikennealan kyberkypsyys on keskiarvoltaan 3,68, lähes sama kuin vuoden 2022 taso 3,71. Toimialan keskiarvo on korkea, mutta hajonta on suurta. Kyberturvallisuuskulttuuri on vahvistunut, mutta vastuiden määrittelyssä on edelleen haasteita matalamman kypsyystason toimijoilla. Strateginen kehittäminen jatkuu riskiperusteisesti, ja valtaosa organisaatioista ylittää sääntelyn vähimmäisvaatimukset. Haavoittuvuuksien hallinta on kehittynyt automaation ja omaisuusrekisterien avulla, ja uhkatiedustelu on monipuolista. Heikoin osa-alue on kumppaniverkoston riskienhallinta, jossa tarvitaan lisää resursseja ja systemaattisia menetelmiä. Identiteetin- ja pääsynhallinnan sekä omaisuudenhallinnan tulokset ovat laskeneet, mikä liittyy osin keskeneräisiin kehitysprojekteihin. Teleliikenteen vahva varautumiskulttuuri ja kriittisten palveluiden suojaustoimet säilyvät toimialan keskeisinä vahvuuksina.

ICT: Vakiintunut taso: 3.51

- Toimialan otanta koostui keskisuurista ja suurista ICT-alan organisaatioista.

Vahvuudet

- ICT-alan kyberturvallisuuden parhaat käytännöt perustuvat pitkäjänteiseen kehitystyöhön, selkeisiin johtamisrakenteisiin ja liiketoimintalähtöisyyteen. Asiakkaiden vaatimukset edellyttävät usein kyvykkyyksien todentamista, minkä vuoksi johtamisjärjestelmät ja sertifioinnit, kuten ISO 27001, ovat yleisiä.
- Korkean kypsyystason yritykset rakentavat vaatimustenmukaisuuden ympärille riskilähtöisen toimintamallin, jossa tekniset, operatiiviset ja strategiset kyvykkyydet tukevat toisiaan. Tämä näkyy esimerkiksi kumppaniriskien hallinnassa, jossa edistyneimmät toimijat seuraavat riskejä ja riippuvuuksia aina ohjelmistokomponenttitasolle asti.
- Organisaatioille on tyypillistä selkeästi eriytetyt resurssit, kuten oma tietoturvavalvomo, joka toimii riippumatta asiakasresurssien saatavuudesta. Henkilöstön osaamisen kehittämiseen panostetaan suunnitelmallisesti, ja koulutukset kytketään usein palkitsemiseen ja urakehitykseen. Monipuoliset ja roolikohtaiset koulutussisällöt tukevat vahvan kyberturvallisuuskulttuurin muodostumista.

Kehityskohteet:

- Tilannekuvan muodostamisessa kehittämistarpeet liittyvät etenkin valvonnan kattavuuteen, ajantasaisen tiedon kokoamiseen ja sen hyödyntämiseen päätöksenteon tukena.
- Osalla toimijoista uhkatiedon hyödyntäminen on vielä satunnaista tai rajoittuu yksittäisiin lähteisiin. Sovellusturvallisuuteen tulisi kiinnittää lisää huomiota, sillä se on toimialan ydintoimintaa ja vain osalla yrityksistä turvallinen sovelluskehitys on huomioitu kattavasti.
- Riskinäkökulmasta myös kumppaniverkoston hallinnasta löytyi organisaatioilta kehitettävää esimerkiksi sopimusvaatimusten lisäämisen ja niiden säännöllisen päivittämisen osalta. Lisäksi tietoturvan toteutumisen seuranta ja auditointikäytäntöjen laajentaminen tukevat ketjun hallittavuutta ja läpinäkyvyyttä. Kehittämistarpeita havaittiin myös kyberhäiriön- ja jatkuvuudenhallinnan sekä testaamisen alueella. Prosesseja ja palautumissuunnitelmia on usein laadittu, mutta niiden testaaminen kaipaa osassa yrityksistä systemaattisuutta.

Vertailu 2022–2025

- Vuoden 2025 ICT-toimialan kyberkypsyys on keskiarvoltaan 3,51, mikä on hieman laskenut vuoden 2022 tasosta 3,67. Keskeiset käytännöt ovat vakiintuneita, mutta hajonta on kasvanut ja otannan pienentyminen voi vaikuttaa vertailtavuuteen. Riskienhallinta on kehittynyt, kun kyberriskit liitetään yhä useammin osaksi liiketoiminnan muuta riskienhallintaa, vaikka osa toimijoista painottaa edelleen asiakas- ja regulaatiovaatimuksia.
- Kolmansien osapuolten riskienhallinta on edistynyt NIS2-vaatimusten myötä, mutta seurantatoimenpiteet ja elinkaarenhallinta ovat edelleen haasteita. Henkilöstön kehittäminen on ainoa osa-alue, jonka keskiarvo on noussut. Heikoin osa-alue on tilannekuva, jossa valvonta ja tiedon hyödyntäminen johdon päätöksenteossa ovat edelleen puutteellisia. Kokonaisuutena kehitystä ohjaavat asiakas- ja regulaatiovaatimukset, mutta resurssien rajallisuus voi hidastaa pienempien toimijoiden kyvykkyyksien kehittämistä.

Yksityinen turvallisuusala: Vakiintunut taso: 3.45

- Toimialan otanta koostuu yksityisen turvallisuusalan yrityksistä, jotka tarjoavat kulunhallinnan, valvonta- ja hälytysjärjestelmien, lukitusratkaisujen sekä kameravalvonnan, turvateknologian, vartioinnin ja turvallisuuspalveluiden suunnittelun, asennuksen ja ylläpidon ratkaisuja teollisuuden, kiinteistöjen ja yhteisöjen tarpeisiin. Toimiala on osa selvitystä ensimmäistä kertaa.

Vahvuudet

- Toimialan turvallisuuskriittisen asiakaskunnan sekä lainsäädännön vaatimusten vuoksi organisaatiot kehittävät aktiivisesti kyberturvallisuuskäytäntöjään. Kilpailuedun ja luotettavuuden kasvattamiseksi yritykset tukeutuvat kansainvälisiin tietoturvastandardeihin ja usealla onkin tavoitteenaan esimerkiksi ISO27001-sertifioitu tietoturvan hallintamalli.
- Samasta syystä myös erilaisia varautumis- ja jatkuvuussuunnitelmia myös kyberhäiriöiden varalle on toimialalla tehty kattavasti. Suunnitelmia katselmoidaan säännöllisesti ja toimialalla järjestetään aktiivisesti omia harjoituksia tai osallistutaan asiakkaiden ja kumppaneiden kyberharjoituksiin.
- Fyysinen pääsynhallinta on yksi alan keskeisistä ydinosaamisalueista ja siihen liittyvät teknologiat ja käytännöt on tasokkaasti toteutettu ja niiden toteutumista valvotaan. Asianmukaisesti hoidettu fyysinen suojaus täydentää teknisiä tietoturvatoimia ja muodostaa niiden kanssa kokonaisvaltaisen suojausratkaisun.

Kehityskohteet:

- Alan merkittävimmät kehityskohteet liittyvät etenkin henkilöstöresurssien riittävyyteen. Rajalliset resurssit vaikeuttavat yhdenmukaisten prosessien ja dokumentaation kehittämistä ja ylläpitoa, mikä voi heikentää kokonaisvaltaista kyberturvallisuuden hallintaa

.

- Toimialakohtaisen kyberosaamisen saatavuus on haastavaa osin johtuen toimialan pienestä koosta, ja osa toimijoista on ulkoistanut toimintojaan kumppaneille ilman täyttä näkyvyyttä tai varmuutta toteutettavista käytännöistä.
- Kolmansien osapuolten riskienhallinnan kehittäminen alkaa kriittisten palveluiden ja kumppaneiden sekä niiden välisten riippuvuuksien tunnistamisesta ja rekisteröinnistä. Selkeiden ja seurattavien tietoturvavaatimusten asettaminen kumppaneille ja yhteisten jatkuvan seurannan käytäntöjen muodostaminen tukevat riskienhallintaa ja pienentävät toimitusketjun kautta tulevan uhkan todennäköisyyttä.

Analyysi kyberturvallisuuden nykytilasta

- Kyberturvallisuuden kehitystä ohjaavat asiakasvaatimukset, NIS2-direktiivi ja kasvava tarve strukturoidulle raportoinnille. Useat yritykset tavoittelevat ISO 27001 -sertifiointia kilpailuetuna ja vastauksena vaatimuksiin. Vaikka toimiala ei ole suoraan kyberlainsäädännön velvoittama, asiakkuudet ja uhkaskenaariot lisäävät motivaatiota kehittämiseen.
- Kyberturvallisuuden johtaminen on monilla yrityksillä vielä kehittyvää, ja vastuut kuuluvat usein turvallisuuspäällikölle tai IT:lle ilman erillistä tiimiä. ISMS-järjestelmien käyttöönotto on monin paikoin kesken, ja haasteena on varmistaa, ettei kehitys jää politiikkatasolle, vaan tekninen toteutus vastaa uhkia. Rajalliset resurssit johtavat usein ulkoistettujen palveluiden käyttöön, mikä voi aiheuttaa riskejä, jos prioriteetteja ja tavoitteita ei määritellä selkeästi kumppaneille.

Energia: Vakiintunut taso: 3.38

- Paikallisia ja valtakunnallisia energiayhtiöitä, jotka toimivat sähkön ja lämmön tuotannossa ja jakelussa sekä polttoainekaupassa, verkkopalveluiden ja siirtoinfrastruktuurin ylläpitäjiä sekä muita energia-alan teknologia- ja palveluyrityksiä.

Vahvuudet

- Kaikki toimialan yritykset kouluttavat kyberturvallisuutta, joka varmistaa henkilöstön kyvyn tunnistaa ja torjua kyberuhkia eri rooleissa, sekä tukee turvallisuuskulttuurin vahvistumista ja sääntelyvaatimusten täyttymistä.
- Uhkien ja haavoittuvuuksien hallinnan alueella toiminta on kehittynyttä. Haavoittuvuustietoa kerätään monipuolisista lähteistä ja organisaatiot ovat aktiivisesti mukana alan sidosryhmissä. Systemaattisen haavoittuvuusskannauksen lisäksi kypsimmät toimijat hyödyntävät tietoturvatestausta ja skenaariopohjaisia harjoituksia osana laajempaa uhkien ja haavoittuvuuksien hallintaa.
- Toimialalla on useita yrityksiä, jotka kykenevät ylläpitämään kattavaa kyberturvallisuuden tilannekuvaa, havainnoimaan poikkeamia ja reagoimaan niihin ennalta määritettyjen prosessien mukaisesti tehokkaasti ja viiveettä.

Kehityskohteet:

- Yrityksissä, joissa IT ja OT ovat organisatorisesti erillään, on haasteita ylläpitää kokonaisvaltaista käsitystä kybertilannekuvasta. Erilliset vastuualueet ilman yhteistoimintamalleja vaikeuttavat riskilähtöistä päätöksentekoa ja resurssien priorisointia.
- Pienemmissä organisaatioissa kybertehtävien henkilöriippuvaisuus korostuu keskeisenä riskinä. Pienet IT- tai kyberturvatiimit voivat lisätä toiminnan ketteryyttä, mutta usein henkilöstön ja resurssien vähäisyys kuormittavat työntekijöitä tai pakottavat ne priorisoimaan jopa kriittisten kehityskohteiden välillä.
- Toimialan varautumisvelvoitteiden myötä lähes jokainen organisaatio on luonut perustason varautumissuunnitelmat kriittisille palveluille, mutta joissain yrityksissä varautuminen saattaa olla toteutettu lähinnä vaatimustenmukaisuuden täyttämisen näkökulmasta.

Vertailu 2022–2025

- Vuonna 2025 energia-alan kyberkypsyys on noussut keskiarvoon 3,38 (2022: 3,12), ja mukana on nyt 12 yritystä aiemman 9 sijaan. Yritysten välillä on suuria eroja: osa yhtiöistä on erittäin kypsiä, kun taas pienemmät paikalliset toimijat jäävät matalammalle tasolle resurssipulan vuoksi. Johdon sitoutuminen ja pitkän aikavälin suunnitelmat ovat lisääntyneet myös matalamman tason yrityksissä, mutta joillakin varautuminen jää lainsäädännön velvoitteiden tasolle. Henkilöstön kyberosaaminen ja uhkien hallinta ovat parantuneet, mutta OT-ympäristöjen hallinnassa on edelleen puutteita. Energia-ala on edelleen korkean kyberkypsyyden toimiala, mutta suuri hajonta ja matalan kypsyystason toimijoiden joukko voivat uhata koko energiajärjestelmän kyberresilienssiä. NIS2-direktiivi voi vauhdittaa kehitystä, mutta riskinä on, että vaatimusten täyttäminen jää kertaluontoiseksi projektiksi eikä johda jatkuvaan kehitykseen.

Terveydenhuolto: Vakiintunut taso: 3.18

- Vuoden 2025 selvityksessä on mukana terveyspalveluiden tuottajien lisäksi mukana yrityksiä terveydenhuollon tuotanto- ja jakelusegmenteistä.

Vahvuudet

- Tietoturvatietoisuuden ja -koulutuksen osalta käytännöt ovat pääosin vahvoja ja varsin yhtenäisiä. Kaikki otannan organisaatiot ovat tunnistaneet koulutuksen tärkeäksi ja järjestävät henkilöstölleen monipuolisia koulutuksia sekä säännöllisiä tietoiskuja. Jossain organisaatioissa on otettu käyttöön myös roolipohjaiset koulutusohjelmat, jotka tukevat riskiperusteista osaamisen kehittämistä ja varmistavat työtehtävien mukaiset kyberturvallisuusvalmiudet.
- Osa-alueista vahvimman, kriittisten palveluiden suojaamisen parhaimpiin käytäntöihin kuuluu palautumiskyvyn säännöllinen testaus, jota kypsimmät organisaatiot toteuttavat osana jatkuvuudenhallintaa. Säännöllinen palautumistestaus auttaa tunnistamaan kehityskohteita ja lyhentämään mahdollisia käyttökatkoja.
- Lisäksi suurin osa toimijoista järjestää säännöllisesti erilaisia kyberharjoituksia organisaation eri tasoilla, jotka tukevat valmiuden ylläpitämistä ja parantavat reaktiokykyä todellisissa poikkeamatilanteissa.

Kehityskohteet:

- Toimialalla esiintyvät kehityskohteet liittyvät usein organisaatiokohtaisiin eroihin hallintamalleissa, teknologisissa ratkaisuissa ja resursoinnissa. Monissa tapauksissa haasteet johtuvat siitä, ettei suunniteltuja toimintamalleja kyetä tehokkaasti viemään käytännön tasolle. Kyberosaamisen riittävyys ja resurssien saatavuus muodostavat haasteen erityisesti kehitystyön jatkuvuuden näkökulmasta.
- Kolmansien osapuolten riskienhallinta on toimialan heikoin osa-alue. Riskienhallinta nojaa organisaatioissa pääosin sopimuksiin ja auditointikäytännöt ovat usein puutteellisia tai satunnaisia. Hankintaprosesseissa esiintyy haasteita, kun tietoturvavaatimuksia ei ole systemaattisesti määritelty tai ymmärretty, joka vaikeuttaa kumppanien yhdenmukaista hallintaa ja jatkuvaa seurantaa.
- Identiteetin- ja pääsynhallinnan prosessien automatisointi ja tehokkuus ovat keskeisiä kehityskohteita, sillä manuaaliset toimintatavat hidastavat reagointikykyä ja lisäävät inhimillisten virheiden riskiä.

Vertailu 2022–2025

- Vuoden 2025 selvitys kattaa seitsemän yritystä, joten koko toimialaa koskevia laajoja johtopäätöksiä ei voida tehdä. Keskiarvo osoittaa pientä kypsyystason nousua, mutta osa-alueiden muutokset vaihtelevat, ja hajonta on vähentynyt edelliseen selvitykseen verrattuna. Suurin edistys on kriittisten palveluiden suojaamisessa, joka on nyt vahvin osa-alue yhdessä tapahtumien ja poikkeamien hallinnan kanssa. Kehitystä on vauhdittanut kiristynyt sääntely ja kasvava uhkakenttä, mutta jatkuvuussuunnitelmien ajantasaisuus ja testaaminen vaativat edelleen huomiota. Kyberturvallisuuden hallinta on parantunut ja kaikilla toimijoilla on käytössä tai kehitteillä tietoturvan hallintamalli. Henkilöstön kehittämisessä näkyy positiivisia merkkejä, vaikka keskiarvo on säilynyt ennallFaan. Heikoimpia osa-alueita ovat identiteetin- ja pääsynhallinta, jossa manuaaliset prosessit aiheuttavat riskejä, sekä kolmansien osapuolten riskienhallinta, jossa valvontatoimenpiteet ja resurssit ovat puutteellisia. Toimitusketjut tunnistetaan kriittisimmäksi kybersidonnaiseksi uhkaksi, mikä korostaa tarvetta systematisoida valvonta ja priorisoida kehitystoimet riskiperusteisesti.

Teollisuus: Vakiintunut taso: 3.14

- Toimialan otanta kattaa yrityksiä metsä-, kemia-, konepaja-, ja puolustusteollisuudesta.

Vahvuudet

- Korkean kypsyystason organisaatioissa kyberturvallisuus on johdon prioriteetti, ja tilannekuvasta raportoidaan säännöllisesti. Tätä tukee riskipohjainen kyberstrategia, joka on sidottu liiketoiminnan strategiaan, sekä selkeät hallintajärjestelmät, usein ISO 27001 -sertifioituina.
- Uhkien ja haavoittuvuuksien hallinta on vahvin osa-alue: kypsimmät organisaatiot hyödyntävät SOC-tiimejä, uhkametsästystä, penetraatiotestausta ja kyberharjoituksia sekä jakavat aktiivisesti uhkatietoa verkostoissa.
- Identiteetin- ja pääsynhallinta on tasaisella tasolla, ja useilla toimijoilla on keskitetyt IAM-ratkaisut, jotka tukevat automatisoituja prosesseja ja perustuvat vähimpien oikeuksien periaatteeseen sekä roolipohjaiseen malliin.

Kehityskohteet:

- Kybertilannekuvan seuranta on monilla yrityksillä puutteellista, ja valvonta ei kata kaikkia kriittisiä tuotantojärjestelmiä. OT-omaisuuden hallinnan heikkoudet lisäävät altistumista kyberuhille ja vaikeuttavat poikkeamiin reagointia, mikä voi hidastaa tai estää oikea-aikaiset toimenpiteet.
- Joissakin organisaatioissa johdon vähäinen kiinnostus kyberturvallisuuteen näkyy resurssien ja budjetin riittämättömyytenä sekä hajanaisina riskienhallintakäytäntöinä.
- Tuotantojärjestelmät ovat teollisuustoimialalla kriittisiä, mutta niiden suojauskäytännöt ovat usein puutteellisia. Haasteita esiintyy suojauskontrolleissa, järjestelmien segmentoinnissa sekä kriittisten resurssien ja omaisuuden kartoituksessa. Näiden järjestelmien asianmukainen suojaaminen ja hallinta on keskeistä tuotantoprosessien häiriöttömän toiminnan turvaamiseksi ja kyberriskien hallitsemiseksi.

Vertailu 2022–2025

- Teollisuusalan kyberkypsyys on noussut, mutta yritysten väliset erot ovat edelleen suuria, matalimman ja korkeimman kypsyystason eron ylittäessä kaksi yksikköä. Yritykset jakautuvat karkeasti kolmeen ryhmään: strategisesti johdetut ja kokonaisvaltaiset kyberturvallisuustoimijat, keskitason yritykset, joissa perusprosessit ovat olemassa mutta johdon sitoutuminen hakee paikkaansa, sekä toimijat, joissa kyberturvallisuus nähdään erillisenä teknisenä osa-alueena. Vahvimpia osa-alueita ovat uhkien ja haavoittuvuuksien hallinta, identiteetin- ja pääsynhallinta sekä kriittisten palveluiden suojaaminen. Merkittävin edistysaskel liittyy henkilöstön kehittämiseen, jota NIS2-direktiivi on vauhdittanut, vaikka kaikki yritykset eivät vielä täytä sen vaatimuksia.
- Heikoimpia osa-alueita ovat tilannekuva, riskienhallinta, kyberarkkitehtuuri ja omaisuudenhallinta, joissa näkyvyyden puutteet ja OT-omaisuuden hajautunut hallinta vaikeuttavat riskien priorisointia. Kolmansien osapuolten riskienhallinta on edelleen heikko, vaikka kypsyystaso on noussut puuttuvat jatkuva seuranta ja sopimusvaatimukset vielä monilta. Johdon rooli on ratkaiseva: strategisesti sitoutuneissa organisaatioissa riskienhallinta on integroitu liiketoimintaan, kun taas muissa se jää hajanaiseksi ja resurssit riittämättömiksi. Kokonaisuutena kehitys on myönteistä, mutta toimialan resilienssin vahvistaminen edellyttää perusrakenteiden tasaisempaa kehittymistä.

Kauppa ja jakelu: Vakiintunut taso: 3.11

- Otanta koostuu vähittäis- ja tukkukaupoista, päivittäistavarakaupoista, jakelun sekä ruokapalveluiden toimijoista.

Vahvuudet

- Parhaisiin käytäntöihin kuuluvat tunnettuihin viitekehyksiin, kuten ISO/IEC 27001-standardiin, perustuvat johtamisjärjestelmät, jotka tukevat systemaattista ja riskilähtöistä kehittämistä. Kyberturvallisuudelle on lisäksi yhä useammin asetettu strategia tai suunnitelma, joka ohjaa kehitystyötä ja on sidoksissa liiketoiminnan tavoitteisiin.
- Toimialalla kriittiset palvelut on tunnistettu ja huomioitu kattavasti. Niiden jatkuvuutta ja toimintavarmuutta tarkastellaan useista eri näkökulmista, joka näkyy esimerkiksi valmiussuunnittelussa ja palveluiden toipumiskyvyn varmistamisessa. Kypsimmissä organisaatioissa johto osallistuu aktiivisesti häiriötilanteiden hallintaan, mikä heijastaa vahvaa sitoutumista.
- Uhkien ja haavoittuvuuksien hallinnassa hyödynnetään laajasti automaattisia ja säännöllisiä haavoittuvuusskannauksia ja kypsimmät toimijat hyödyntävät bug bounty- ohjelmia jatkuvan haavoittuvuustilanteen monitoroinnin tukena.

Kehityskohteet:

- Kumppaneihin tukeudutaan useissa kriittisissä toiminnoissa, mutta kumppaniverkoston riskienhallinnasta puuttuvat usein johdonmukaiset käytännöt. Kumppanuus perustuu tavallisesti pitkäkestoiseen luottamussuhteeseen, eikä toimittajiin liittyviä riskejä tai vaatimuksenmukaisuutta seurata systemaattisesti.
- Vaikka kriittisten palveluiden rooli on tunnistettu, niihin liittyvät jatkuvuussuunnitelmat ovat matalamman kypsyystason yrityksissä keskeneräisiä tai tekemättä, palveluiden priorisointia ei ole viety loppuun asti ja toimintatapojen harjoittelua ei tehdä kyberhäiriötilanteisiin varautumisen tukena.
- Kyberarkkitehtuurin alueella tarvitaan kehittämistoimia, vaikka tekniset perusteet ovat kunnossa. Kokonaiskuvan laatiminen toisi järjestelmällisyyttä ja strategista näkökulmaa tekniseen kehittämiseen. Erityisesti tietojen luokittelu ja datan hallinta ovat puutteellisia, vaikka yrityksillä on käytössään paljon arkaluontoista dataa. Lisäksi identiteetinhallinnassa esiintyy manuaalisia, virheille alttiita prosesseja.

Vertailu 2022–2025

- Kaupan ja jakelun toimialan yritysten välinen hajonta on hieman tasaantunut, ja suurin osa yrityksistä sijoittuu hyvälle perustasolle. Kehitystä on vauhdittanut erityisesti NIS2-direktiivi ja kansallinen lainsäädäntö, jotka ovat lisänneet johdon kiinnostusta kyberturvallisuuteen ja tukeneet hallintamallien, kuten ISO 27001:n käyttöönottoa. Vaikka strateginen sitoutuminen on vahvistunut, riittävä resurssointi on edelleen haaste. Yritykset ovat parantaneet kriittisten palveluiden suojaamista ja jatkuvuussuunnittelua, joissa huomioidaan nyt kyberhäiriöiden vaikutukset ja hyödynnetään monitorointia. Digitalisaatio ja pilvipalvelujen käyttöönoton kasvu ovat lisänneet painetta kehittää kyberresilienssiä. Kyberriskienhallinta on kuitenkin edelleen hajanaista, mikä heikentää ennakoivaa varautumista. Henkilöstön osaaminen on kehittynyt: pakolliset koulutukset, kalastelusimulaatiot ja tietoisuustoimet ovat yleistyneet, ja henkilöstön rooli nähdään keskeisenä osana kokonaisvaltaista kyberturvallisuutta.

Media: Vakiintunut taso: 3.01

- Otanta koostuu suurista ja keskisuurista suomalaisista media-alan yrityksiä ja joukosta löytyy monipuolisesti erilaista media-alan toimintaa.

Vahvuudet

- Media-alan kyberkypsimmät organisaatiot ovat ottaneet käyttöön strategisesti johdetun ja dokumentoidun kyberturvallisuuden hallintamallin, joka tukee liiketoiminnan tavoitteita. Hallintamalli perustuu usein ISO/IEC 27001–viitekehykseen ja on sertifioitu tai se on tulevaisuuden tavoitteena.
- Uhkatietoisuuden kasvu näkyy erityisesti teknisten suojaustoimien vahvistumisena: SOC-palvelut, tekniset skannaukset ja uhkien havainnointikyvykkyydet ovat yleistyneet. Loogisen pääsynhallinnan osalta parhaat käytännöt sisältävät roolipohjaisen ja automatisoidun hallinnan sekä monivaiheisen tunnistautumisen (MFA).
- Kaikki toimijat ovat tunnistaneet kriittiset palvelunsa, ja korkeamman kypsyystason organisaatioissa näille on laadittu jatkuvuussuunnitelmat. Näitä suunnitelmia myös testataan säännöllisesti, mikä osoittaa kypsää otetta resilienssin kehittämiseen.

Kehityskohteet:

- Vaikka edistystä on tapahtunut, monilla organisaatioilla on edelleen haasteita resurssien riittävyydessä. Tämä näkyy erityisesti dokumentaation puutteina ja kyberturvallisuuteen liittyvien käytäntöjen hajanaisuutena.
- Riskienhallinnan prosessit ovat monin paikoin vielä kehittymättömiä tai epäyhtenäisiä, eikä niitä ole yleensä integroitu liiketoiminnan kokonaisriskienhallintaan.
- Kumppaniriskienhallinta on toinen keskeinen kehityskohde. Tietoturvavaatimusten määrittely ja niiden täyttymisen seuranta yhteistyökumppaneiden kanssa on usein puutteellista.
- Vaikka kriittiset palvelut on tunnistettu, jatkuvuussuunnitelmat ovat monessa organisaatiossa vielä keskeneräisiä tai dokumentoimatta, mikä heikentää valmiutta reagoida ja toipua häiriötilanteista.

Vertailu 2022–2025

- Vuoden 2022 keskeiset kehityskohteet liittyivät turvallisuuskulttuuriin ja henkilöstön tietoturvatietoisuuden vahvistamiseen, ja näillä alueilla on tapahtunut edistystä. Yritykset ovat panostaneet koulutuksiin ja tietoisuustyöhön, mikä on parantanut valmiuksia tunnistaa ja hallita uhkia. Kehitystä ovat vauhdittaneet geopoliittinen epävarmuus, monimutkaistuvat toimitusketjut ja sääntelyuudistukset, kuten NIS2-direktiivi, jotka ovat lisänneet painetta vahvistaa kyberturvallisuuden hallintaa. Puolella otannan yrityksistä on nyt käytössä tietoturvan johtamisjärjestelmä, ja kaikki kehittävät hallintamallejaan.
- Riskienhallinta on kehittynyt, mutta säilyy heikoimpien osa-alueiden joukossa, sillä yhtenäiset ja liiketoimintaan integroidut käytännöt puuttuvat monilta. Kumppaniriskien hallinta on edelleen haavoittuva alue, vaikka tietoisuus on lisääntynyt. Uhkienhallinnassa kehitys on ollut poikkeuksellisen myönteistä: organisaatiot siirtyvät reaktiivisista toimintatavoista kohti säännöllistä ja osin automatisoitua haavoittuvuuksien arviointia. Vaikka toimialan keskiarvo ei ole muuttunut, taustalla näkyy positiivisia kehityskulkuja, joiden jatkuminen edellyttää johdon aktiivista roolia ja kyberriskien tiivistä kytkemistä liiketoiminnan päätöksentekoon.

Rakennus: Vakiintunut taso: 3.0

- Toimialaotanta koostui suurista ja keskisuurista kotimaisista ja kansainvälisiin konserneihin kuuluvista rakennusalan yrityksistä. Otanta on muuttunut vuoden 2022 ja nykyselvityksen välillä siten, että edellisellä selvityskierroksella rakennusalan yritykset kuuluivat teollisuusalan toimialaotantaan. Tästä syystä suoraa vertailua edelliseen selvitykseen ei voida tehdä ja analyysissa keskitytään rakennusalan nykytulosten käsittelyyn.

Vahvuudet

- Rakennusalan kyberturvallisuuden parhaat käytännöt perustuvat selkeisiin tavoitteisiin ja jatkuvaan kehittämiseen. Kehittyneemmät organisaatiot näkevät kyberturvallisuuden liiketoiminnan mahdollistajana, mutta samalla kehitystä ohjaavat myös ulkoiset vaatimukset kuten asiakasodotukset ja sääntely, esimerkiksi NIS2-direktiivi ja sen kansallinen toimeenpano.
- Erityisesti tunnettuihin viitekehyksiin kuten ISO/IEC 27001 -standardiin perustuvat johtamisjärjestelmät nähdään kilpailuetuna ja useimmilla organisaatioilla hallintamalli on jo olemassa tai sen käyttöönotto ja sertifiointi tavoitteena.
- Vahvuutena erottuu haavoittuvuuksien hallinta, jossa kypsimmillä se on pitkälti automatisoitua ja testausta tehdään monipuolisesti. Haavoittuvuuksien korjaustoimenpiteet priorisoidaan kriittisyyden mukaan, ja joissain organisaatioissa on käytössä kannustinmalleja ennakoivaan haavoittuvuuksien tunnistamiseen.
- Talouteen ja maksuliikenteeseen liittyvät järjestelmät on tunnistettu toiminnan kannalta kriittisiksi ja erityisesti niiden suojaukseen on panostettu toimialalla.

Kehityskohteet:

- Selvitysaineistosta havaittiin yhteneväisiä haasteita, jotka hidastavat kyberturvallisuuden kehitystä. Useilla toimijoilla kyberturvallisuuden resurssit ovat rajalliset, mihin vaikuttaa sekä toimialan yleinen tilanne, että johdon vaihteleva sitoutuminen. Johdon tuki on monin paikoin reaktiivista ja kehityspanostuksia saatetaan tehdä vasta poikkeamatilanteiden jälkeen.
- Useissa tapauksissa kyberturvallisuutta kehitetään ensisijaisesti ulkoisten vaatimusten, kuten asiakasodotusten ohjaamana. Tällöin esimerkiksi johtamisjärjestelmien todellinen hyöty voi jäädä käyttämättä, jos niiden käytännön soveltaminen ei juurru organisaation toimintaan.
- Lähes kaikkia organisaatioita yhdistävä haaste on kolmansien osapuolten riskienhallinta, joka on ristiriidassa sen kanssa, että useat toimialan yritykset kertovat merkittävän osan kyberturvapoikkeamista olevan lähtöisin juuri toimitusketjuista. Erityisesti resurssivajeet, selkeiden prosessien puuttuminen sekä monitoimittajaympäristön hallinnan haasteet vaikuttavat heikkoon näkyvyyteen.

Analyysi kyberturvallisuuden nykytilasta

- Rakennusalan kyberturvallisuuden osa-alueet ovat tasaisia, mutta yritysten välillä on merkittävää hajontaa. Vahvin osa-alue on uhkien ja haavoittuvuuksien hallinta, jossa kehittyneimmät toimijat hyödyntävät automatisoituja prosesseja ja SOC-yhteistyötä, kun taas matalammalla tasolla toimintamallit ovat reaktiivisia ja resurssit rajallisia. Suurimmat kehitystarpeet liittyvät kyberriskienhallintaan, jotka käsitellään usein irrallaan liiketoiminnan riskienhallinnasta. Kolmansien osapuolten riskienhallinta on heikoin osa-alue. Kehitystä ohjaavat asiakasvaatimukset ja sertifioinnit, kuten ISO 27001, joita nähdään kilpailuetuna, mutta riskilähtöinen toimintamalli on monilla vielä kehittymässä. Jotta rajalliset resurssit kohdistuvat oikein ja kyberturvallisuustoimet tuottavat todellista lisäarvoa, riskilähtöisyyden vahvistaminen on välttämätöntä.

Vesi- ja jätehuolto: Kehittyvä taso: 2.83

- Otanta koostuu yhteensä yhdeksästä vesi- tai jätehuollon yrityksestä ja se kattaa alan suurimpia toimijoita, pieniä paikallisia toimijoita ei ole selvityksessä mukana.

Vahvuudet

- Tunnettuihin viitekehyksiin, kuten ISO/IEC 27001 perustuvat johtamisjärjestelmät ovat toimialalla yleistymässä. Johtamisjärjestelmien avulla organisaatiot saavat selkeän rakenteen kyberturvallisuuden hallintaan, mikä vahvistaa turvallisuuskulttuuria ja varmistaa jatkuvuutta. Yksinkertaisimmillaan käytössä on tietoturvallisuuden vuosikello, joka lisää suunnitelmallisuutta ja hallittavuutta.
- Kriittiset palvelut on toimialalla tunnistettu ja niiden suojaamiseen sekä jatkuvuuteen liittyviä toimenpiteitä seurataan ja kehitetään säännöllisesti. Organisaatiot osallistuvat toimialakohtaiseen ISAC-ryhmän työhön aktiivisesti, jonka kautta jaetaan uhkatietoa ja kehitetään yhteistä tilannekuvaa. Yhteistyö sidosryhmien kanssa on tärkeä osa toimintavarmuutta.
- Lisäksi poikkeamatilanteisiin varautuminen on monessa organisaatiossa edistynyttä. Suunnitelmat, ohjeistukset ja vastuut on määritelty selkeästi ja toimintamalleja on harjoiteltu käytännössä. Valmius näkyy erityisesti yrityksissä, joissa johto on aktiivisesti mukana häiriötilanteiden hallinnassa ja varautumisen johtamisessa.

Kehityskohteet:

- Toimialalla kyberturvallisuustyötä haastavat rajalliset resurssit. Budjetointi, osaamisen saatavuus ja johdon sitoutuminen eivät aina ole tasolla, joka mahdollistaisi pitkäjänteisen ja suunnitelmallisen kehittämisen. Tämä näkyy erityisesti kyberturvallisuusarkkitehtuurin hallinnan, prosessien jalkauttamisen ja käytännön toteutuksen hajanaisuutena. Vaikka dokumentaatiota ja ohjeistuksia on usein olemassa, niiden ylläpito ja käytännön hyödyntäminen jäävät usein puutteellisiksi.
- Käyttöoikeuksienhallinta on useilla toimijoilla pitkälti manuaalista ja siihen liittyy monia käytännön haasteita. Käyttöoikeuksia kasaantuu ja niiden ajantasaisuuden tarkastelukäytännöt vaihtelevat. Monivaiheinen tunnistautuminen ei ole vielä kaikilla tasoilla käytössä, mikä voi jättää kriittisiä järjestelmiä haavoittuviksi.
- Lisäksi useissa organisaatioissa luotetaan vahvasti kumppaneihin ja toimittajiin, mutta yhteistyöhön liittyvät riskit eivät aina ole järjestelmällisesti tunnistettuja tai hallittuja. Toimittajille asetettavat tietoturvavaatimukset saattavat jäädä yleisluontoisiksi, eikä niiden toteutumista valvota aktiivisesti.

Vertailu 2022-2025

- Viime selvityskierroksella mukana oli vain vesihuollon yrityksiä, kun taas tällä kierroksella otanta kattaa yhdeksän vesi- ja jätehuollon toimijaa, painottuen alan suurimpiin yrityksiin. Erot yritysten välillä ovat suuria, mutta osa-alueiden sisäinen vaihtelu on pientä, ja kehitys on tasaista lukuun ottamatta kyberarkkitehtuuria ja riskienhallintaa, joissa muutosta ei ole nähtävissä. Kehityksen hidasteena ovat edelleen henkilöstö- ja budjettivajeet, kun taas NIS2-direktiivi ja yhteiset kehityshankkeet ovat keskeisiä ajureita. Heikoin osa-alue on kyberturvallisuuden hallinta, vaikka keskiarvo on noussut 0,41 yksikköä ja kaikki toimijat ylittävät tason 2; laajat hallintamallit ja johdon sitoutuminen kuitenkin puuttuvat. Vahvin osa-alue on kriittisten palveluiden suojaaminen (keskiarvo 3,07), mutta varautuminen ei aina kata ICT- ja automaatiojärjestelmiä, mikä korostaa kyberturvallisuuden kehittämisen merkitystä toimialan jatkuvuuden turvaamisessa.

Elintarvike: Kehittyvä taso: 2.71

- Toimialan otanta koostuu elintarvikealan alkutuotannon ja elintarviketeollisuuden organisaatioista.

Vahvuudet

- Parhaat käytännöt kypsimmissä organisaatioissa rakentuvat vahvasti johdon tuen, strategisen ohjauksen ja pitkäjänteisen kehittämisen ympärille.
- Kypsimmissä organisaatioissa on jo pitkään tehty toimia kyberkypsyyden edistämiseksi ja panostettu riskilähtöisesti mm. verkkojen segmentointiin sekä IT- ja OT-ympäristöjen eriyttämiseen. OT-ympäristöjen suojausta ja siihen liittyvää valvontaa ja dokumentointia kehitetään aktiivisesti, koska se on perinteisesti ollut tuotantoyritysten heikoin kohta.
- Parhaimmillaan kyberturvallisuuden kehittäminen on riskilähtöistä ja päätöksentekoa ohjaa kattava käsitys kybertoimintaympäristön uhkatilanteesta ja riskitasoista. Kypsimmissä organisaatioissa tilannekuvaa tukevat mm. SOC-palvelut, jotka kattavat IT-ympäristön lisäksi myös OT-puolen.
- Korkeamman kypsyystason yrityksissä kyberturvallisuuteen liittyvät tavoitteet ovat määritelty esim. kyberstrategiassa ja kyberasiantuntijoiden palkitseminen on sidoksissa strategisten tavoitteiden saavuttamiseen.

Kehityskohteet:

- Toimialan matalimman kypsyystason organisaatoissa tehdään kyberturvallisuustyötä, mutta se on usein vielä reaktiivista ja monin paikoin lähtöisin tarpeesta vastata NIS2-direktiivin vaatimuksiin. Johdon sitoutuminen on vaihtelevaa ja kyberturvallisuus nähdään usein teknisenä tukitoimintona strategisen kokonaisuuden sijaan.
- Strategisen tason kehityskohteisen lisäksi osassa organisaatioista on kehitettävää peruselementeissä. Roolipohjaiset pääsyoikeusmallit sekä keskitetyt identiteetin- ja pääsynhallinnan ratkaisut puuttuvat ja pääsyoikeuksien hallinta on manuaalista ja henkilöriippuvaista, joka nostaa riskiä oikeuksien kasaantumisesta sekä vaikeuttaa elinkaarenhallintaa. MFA:n käyttö ei ole kattavaa ja erityisesti OT-ympäristöjen suojauskäytännöt ovat puutteellisia.
- Toimitusketjujen riskienhallinta on rakenteellisesti heikkoa. Kumppaneiden tietoturvavaatimuksia ei ole systemaattisesti määritelty tai sisällytetty sopimuksiin. Heikomman kypsyystason organisaatioilta puuttuu näkyvyys alihankintaketjuihin eikä teknisiä riippuvuuksia ymmärretä laajasti yleisluontoisiksi, eikä niiden toteutumista valvota aktiivisesti.

Vertailu 2022-2025

- Vuonna 2022 kehityskohteina olivat strategisten tavoitteiden linjaaminen ja suunnitelman laatiminen johdon sitouttamiseksi ja riskilähtöisen päätöksenteon tukemiseksi. Kolmen vuoden aikana kyberturvallisuuden hallinta on vahvistunut, ISMS-malleja otettu käyttöön ja riskienhallinta kehittynyt laajemman tunnistamisen ja arvioinnin myötä. Johdon sitoutuminen, säännöllinen arviointi ja kyberriskien liiketoimintavaikutusten ymmärrys ovat nousseet trendeiksi, osin geopoliittisen epävarmuuden ja lainsäädännön paineiden vuoksi. Tilannekuva on heikoin osa-alue, erityisesti sen viestiminen johdolle, ja hajautetut ympäristöt ja SOC-tiedon vähäinen hyödyntäminen korostavat haastetta. Tapahtumien hallinnan taso on laskenut, mutta harjoitusten yleistyminen ja dokumentaation kehitys osoittavat edistystä, vaikka jatkuvuussuunnitelmat ovat puutteellisia. NIS2 vauhdittaa kehitystä, mutta monessa organisaatiossa ollaan vasta suunnitteluvaiheessa, ja kasvava uhkakenttä lisää varautumisen vaatimuksia.

Satamat, telakat ja operaattorit: Kehittyvä taso: 2.61

- Tällä selvityskierroksella toimialan analyysissä ovat mukana varsinaiset satamatoimijat, eli satamien lisäksi telakat ja operaattorit.

Vahvuudet

- Organisaatioiden kyberturvallisuuden hallintakäytännöissä korkeamman kypsyysarvon organisaatioilla on dokumentoitu tietoturvastrategia, joka on linjassa liiketoiminnan strategian kanssa. Tietoturvaa kehitetään esimerkiksi ISO27001-viitekehykseen pohjautuvan johtamisjärjestelmän avulla ja kuudessa organisaatiossa johdon tuki näkyy tuloksista.
- Kehittyneimmät suojaustoimet ovat monitasoisia, sisältäen SOC palveluita, IDS/IPS-järjestelmiä ja tietoverkkojen segmentointia. Kyberriskienhallinta on integroitu liiketoiminnan riskienhallinnan käytänteiden avulla. Kumppaniverkoston hallinnassa parhaat käytännöt huomioivat riskit osana kokonaisriskienhallintaa ja sopimuksia päivitetään säännöllisesti.
- Korkean kypsyystason yrityksillä on olemassa toiminnan jatkuvuus- ja palautumissuunnitelmat sekä henkilöstön varajärjestelyt. Henkilöstön tietoturvakoulutus on monipuolista ja sen vaikuttavuutta seurataan. Identiteetin- ja pääsynhallinta on toimialan vahvin osa-alue ja korkean kypsyystason organisaatioissa käytössä on keskitetyt IAM-järjestelmät.

Kehityskohteet:

- Matalamman kypsyystason organisaatioissa kyberturvallisuuden hallinta on reaktiivista, eikä se perustu strategiaan tai dokumentoituihin käytäntöihin. Arkkitehtuurin suunnittelu ja dokumentointi puuttuvat, mikä heikentää suojausten kokonaisuuden hallintaa.
- Riskienhallinnan käytännöt ovat vaihtelevia, ja jatkuvuus- ja palaututumissuunnitelmat ovat usein keskeneräisiä, päivittämättä ja testaamattomia. Toimijoita yhdistää usein uhkien ja haavoittuvuuksien hallinnan prosessien ja dokumentaation puutteet. Lisäksi OT-ympäristöjen suojauksessa on puutteita, esimerkiksi segmentointi, päivitykset ja valvonta ovat monin paikoin rajallisia. Tietovarantojen hallinnan hajanaisuus ja elinkaarenhallinnan työkalut on vaihtelevasti manuaalista tai osittain automatisoitua.
- Kumppanihallinnassa on puutteita tietotuvan järjestelmällisessä huomioinnissa esimerkiksi sopimuksessa esitettyjen vaatimusten osalta. Valvontakyvykkyyksien osalta toimijoiden kesken on merkittäviä eroja, ja osalla reaaliaikainen operatiivinen tilannekuva puuttuu kokonaan.

Vertailu 2022-2025

- Vuoden 2025 selvityksessä mukana ovat satamat, telakat ja operaattorit, kun merenkulun organisaatiot on siirretty liikenteen ja logistiikan toimialalle. Toimialan keskiarvo on noussut 2,61:stä vuoden 2022 tasosta 2,16, mikä kertoo sekä otannan muutoksista että aidosta kehityksestä kohti johdonmukaisempia käytäntöjä. Merkittävimmät parannukset näkyvät henkilöstön johtamisessa ja kyberturvallisuuden hallinnassa, joka oli aiemmin heikoin osa-alue. Haasteet, kuten resurssivaje ja epäselvä vastuunjako, eivät ole poistuneet, mutta kehitys on siirtynyt reaktiivisista toimista kohti suunnitelmallisuutta, osin NIS2-direktiivin ja geopoliittisen epävarmuuden vauhdittamana. Direktiivi on lisännyt johdon sitoutumista, selkeyttänyt vastuita ja vahvistanut riskienhallintaa, vaikka vaatimukset koetaan osin kuormittavina. Lisäksi IT-palveluiden ulkoistaminen markkinaehtoisille kumppaneille on parantanut näkyvyyttä ja hallintaa.

Liikenne ja logistiikka: Kehittyvä taso: 2.54

- 2025 otanta koostui yrityksistä maa-, meri- ja ilmakuljetusaloilta. Toimijoiden koot vaihtelevat pienistä yrityksistä kansainvälisiin konserneihin, mutta suurin osa on n. 100-500 henkilöä työllistäviä yrityksiä.

Vahvuudet

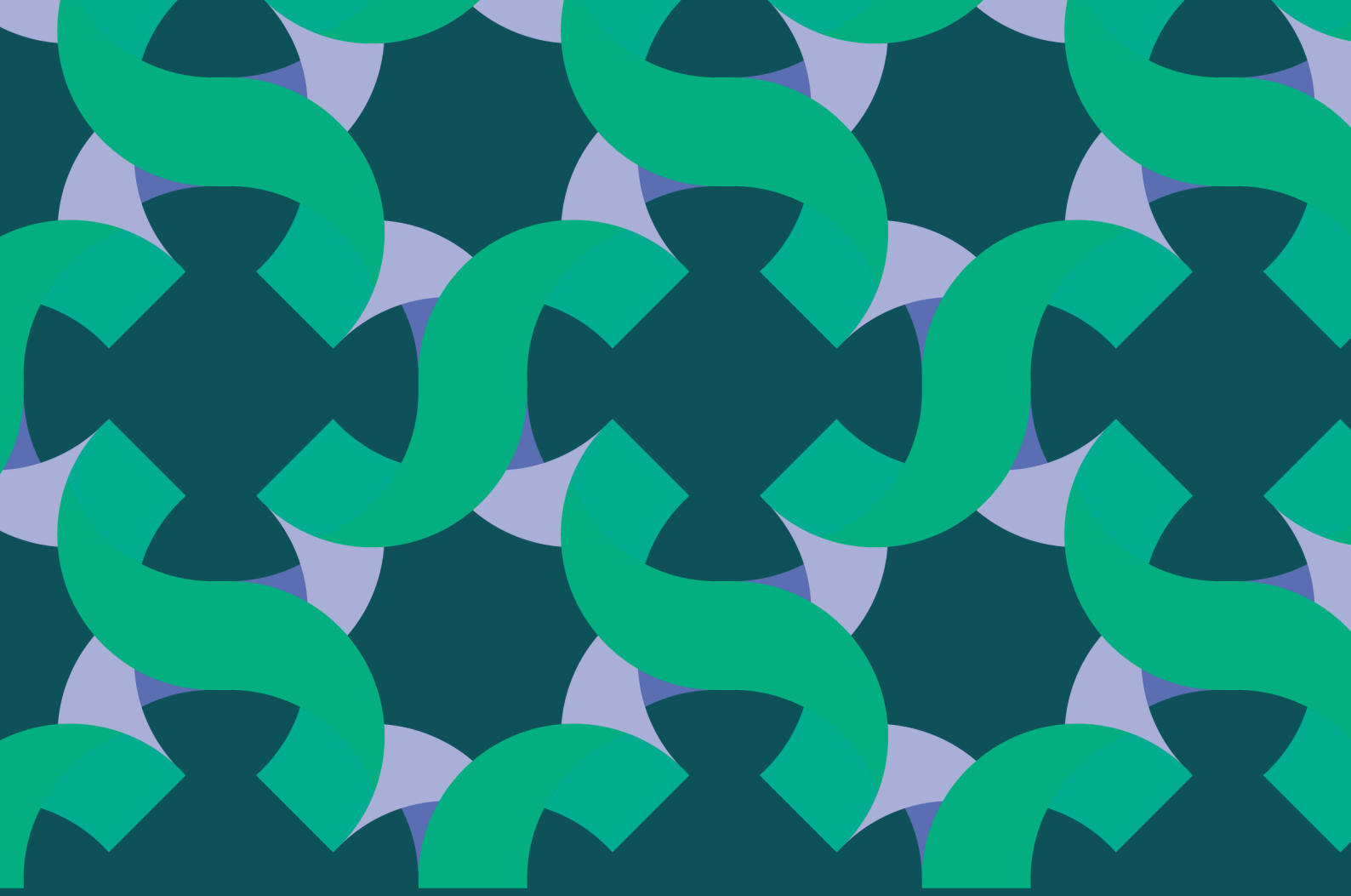
- Toimialan kypsimmät toimijat ovat monikansallisia konserneja, joissa kyberturvallisuusjohtaminen on keskitetty, mutta erilliset tiimit ovat vastuussa kyberturvallisuuden eri osa-alueista. Näillä toimijoilla kyberturvallisuuden suunnittelu ja hallinta on riskilähtöistä ja sille on määritetty strateginen suunta. Kypsimmät toimijat kuvaavat vuoropuhelua johdon kanssa aktiiviseksi ja tärkeäksi osaksi kehitystä.
- Kypsimmät toimijat keskittyvät siihen, että käsitys kybertoimintaympäristön tilasta (mm. haavoittuvuudet, monitorointi ja omaisuudenhallinta) kehittyy jatkuvasti ja kehitystoimenpiteitä voidaan kohdentaa riskilähtöisesti. Prosessit ja dokumentaatio tukevat näitä tavoitteita, mutta niitä ei tehdä vaatimustenmukaisuuden lähtökohdasta.
- Toimialan otannasta keskivaiheille sijoittuneita yrityksiä yhdistää melko hiljattain käynnistetyt kyberturvallisuuden kehitysprojektit, jotka parhaimmillaan perustuvat kyberturvallisuuden nykytilaselvitykseen ja riskien arviointiin.

Kehityskohteet:

- Osalla yrityksistä on merkittäviä haasteita organisoida kyberturvallisuuden osa-alueita. Nämä ovat usein pieniä tai keskisuuria yrityksiä, joilla ei välttämättä ole yhtäkään kyberturvallisuuteen keskittyvää työntekijää. Omien henkilöstöresurssien ollessa rajallisia, yritykset ovat ulkoistaneet merkittävän osan IT- ja kyberturvapalveluistaan.
- Ulkoistaminen voi olla kustannustehokasta ja tarkoituksenmukaista, mutta selvityksestä oli havaittavissa, ettei matalammalle kypsyystasolle sijoittuneet yritykset olleet varmoja siitä, mitä kumppanin vastuulle kyberturvallisuuden osalta kuuluu tai miten aihealueita, kuten omaisuuden- tai haavoittuvuuksienhallintaa toteutetaan. Tämä ymmärryksen puute kyberturvallisuuden nykytilasta näkyy siinä, että osalla yrityksistä kokonaisia osa-alueita on arvioitu tasolle 1, joka viittaa suunnittelemattomaan tai täysin reaktiiviseen tasoon.
- Isoin ero kypsimmän ja matalimmalle arvioidun yrityksen välillä on riskienhallinnassa. Matalammalla kypsyystasolla kyberriskejä arvioidaan satunnaisesti tai ei ollenkaan.

Vertailu 2022-2025

- Vuoden 2025 liikenne- ja logistiikka-alan kyberkypsyyden keskiarvo on 2,54, kun se vuonna 2022 oli 2,95, mutta otannan muutokset vaikeuttavat suoraa vertailua. Yritysten kypsyystasoissa on suurta hajontaa, kun jopa puolet jää alle tason 2,5. Erot ovat toimijakohtaisia, ei osa-aluekohtaisia. Hajontaa selittää ohjaavien vaatimusten puute ja digitalisaation epätasainen eteneminen. Vahvimmat osa-alueet ovat edelleen kyberturvallisuuden hallinta ja identiteetin- ja pääsynhallinta, heikoin tilannekuva. Identiteetin hallinnan vahvuutena on fyysinen kulunvalvonta ja prosessien kehitys, kun taas tilannekuvan haasteet liittyvät ulkoistettuun valvontaan ja OT-järjestelmien näkymättömyyteen. Yhteisiä kehityskohteita ei ole, mutta osa yrityksistä on edennyt merkittävästi, esimerkiksi luomalla kyberturvallisuuden vuosikellon tai harjoittelemalla automaatiojärjestelmien häiriötilanteita.



Huoltovarmuuskeskus