DIGI- JA VÄESTÖTIETO-VIRASTO

Digiturvan kokonaisku-vapalvelu

Raportti ja keskeiset havainnot

21.5.2025

Puh. **0295 536 000** (vaihde) | Yhteystiedot, katso **www.dvv.fi**

Sisällysluettelo

1 Johdon tiivistelmä 4

2 Yhteenveto tuloksista 7

2.1 Osa-alueiden keskiarvot 7

2.2 Kysymyskohtaiset keskiarvot 10

2.2.1 Johtaminen 11

2.2.2 Riskienhallinta 14

2.2.3 Toiminnan jatkuvuus ja varautuminen 16

2.2.4 Tietoturvallisuus 19

2.2.5 Tietosuoja 23

2.2.6 Kyberturvallisuus 26

2.2.7 Rahalliset ja ajalliset panostukset 29

2.2.8 Henkilöresurssit 31

2.2.9 Osaamisen kehittäminen 34

2.2.10 Poikkeamat ja kustannukset 35

3 Organisaatiotyyppien vertailu 38

Digiturvan kokonaiskuvapalvelu

Digi- ja väestötietoviraston (jäljempänä DVV) tehtävänä on edistää julkisen hallinnon organisaatioiden tietoturvallisuuden, sekä laajemmin digitaalisen turvallisuuden, kehittämistä. Osana tätä tehtävää se vastaa Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI), kolmen VAHTI-asiantuntijaryhmän sekä valtionhallinnon tietoturvavastaavien verkoston toiminnasta. Tässä toiminnassa on mukana yli 500 johdon edustajaa ja alan asiantuntijaa.

VAHTI-johtoryhmä on koonnut tietoa valtionhallinnon tietoturvallisuudesta jo 2000-luvun alusta alkaen, ja vuodesta 2017 tietoa on kerätty laajemmin koko julkisen hallinnon tietoturvallisuudesta. Vuodesta 2019 lähtien on koottu ja tarkasteltu hallinnollisen digitaalisen turvallisuuden tilannetietoa. Kyselyiden avulla on voitu selvittää muun muassa, miten lainsäädäntö – kuten tietoturvallisuusasetus vuonna 2010, EU:n yleinen tietosuoja-asetus vuonna 2018 sekä tiedonhallintalaki vuonna 2020 – on vaikuttanut organisaatioiden digitaalisen turvallisuuden osa-alueiden kehittymiseen. Kyselytuloksia on hyödynnetty Julkisen hallinnon digitaalisen turvallisuuden kehittämistoimenpiteiden, VAHTI-työryhmien toiminnan ja tehtävien suunnittelussa. Jatkossa digiturvan kokonaiskuvapalvelulla voidaan seurata myös 2025 voimaan tulleen kyberturvallisuuslain vaikutuksia julkisenhallinnon digi- ja kyberturvallisuuden kehittymiseen.

Digiturvan kokonaiskuvapalvelun tuloksia hyödynnetään myös kansallisen kyberturvallisuusstrategian ja sen toimeenpanosuunnitelman seurantaan julkisen hallinnon osalta.

Digiturvan kokonaiskuvapalvelu on toteutettu saman sisältöisenä vuosina 2021–2024. Vuonna 2022 otettiin käyttöön DVV:n kehittämä verkkopalvelu, jonka avulla julkisen hallinnon organisaatioille voidaan tarjota niiden omasta digiturvatilanteesta ajantasainen tilannekuva jatkuvaan käyttöön tarkoitetulla kokonaiskuvapalvelulla sekä vertailutietoa muuhun julkiseen hallintoon. Vuonna 2024 digiturvan kokonaiskuvapalvelua kehitettiin Loisto-hankkeessa. Loisto-hankkeessa kysymyksen asettelua ja kysymyksiä päivitettiin hieman sekä päivitettiin vastausvaihtoehtoja. Muutokset toteutettiin niin, että vuonna 2025 kerätty data on vertailukelpoista aiempien vuosien kanssa.

Digiturvan kokonaiskuvapalvelun ohella DVV on toteuttanut Henkilöstön ja kansalaisten Digiturvabarometria syyskuusta 2020 alkaen. Digiturvan kokonaiskuvapalvelun avulla seurataan, miten organisaatioiden hallinnollinen digiturvallisuus kehittyy. Digiturvabarometrin avulla kartoitetaan digitaaliseen toimintaympäristöön liittyvää henkilöstön osaamista, koulutustarpeita, toteutuneita uhkia sekä luottamusta digimaailman toimijoihin ja palveluihin. Digi- ja väestötietoviraston kyselyyn vastasi 1500 täysi-ikäistä suomalaista elokuussa 2024.

26.9.2024 julkaistun Digi- ja väestötietoviraston Digiturvabarometrin mukaan suomalaisten luottamus digipalveluiden ja -laitteiden turvallisuuteen on heikentynyt edelleen. 36 % vastaajista toteaa luottamuksen heikentyneen, laskua viime vuoteen 8 prosenttiyksikköä. Vastaavasti vastaajien luottamus on parantunut 10 prosenttiyksiköllä vastaajista, jossa nousua on 1 prosenttiyksikkö. Heikentymisen syinä mainitaan mm. tietomurrot, huijaukset, maailmanpoliittinen tilanne ja tekoäly. Vaikka verkkorikollisuus ja muut uhat koetaan merkittävänä uhkana, 91 % vastaajista kokee edelleen

osaavansa käyttää digilaitteita ja palveluita turvallisesti, tämä taso on säilynyt vuosina 2023-2024.

Vastaajia huolestuttaa eniten eli erittäin tai melko paljon ”Palveluihin syöttämiäni tietojani käsitellään väärin tai minulle epäedullisella tavalla”, 60 %, toiseksi eniten ”Tekoälypalveluiden nopea kehittyminen”, 59 % ja kolmanneksi eniten ”Joudun identiteettivarkauden uhriksi”, 56 %. Tekoälykysymys esitettiin ensimmäistä kertaa, kahden muun kysymyksen tulokset eivät ole muuttuneet merkittävästi.

Millaisia digiturvallisuuteen liittyviä tekoja vastaajat ovat tehneet viimeisen vuoden aikana? 85 % on ”Tunnistanut minulle lähetetyn viestin huijaukseksi tai tietojen kalasteluksi”. 81 % on ”Vaihtanut salasanan turvallisemmaksi yhdessä tai useammassa digipalvelussa tai -laitteessa”. 80 % on ”Tarkistanut tai päivittänyt tietoturvapäivitykset ajan tasalle tietokoneessa tai muussa älylaitteessa.” Myöskään tässä ei ole tapahtunut merkittäviä muutoksia.

Luottamus on säilynyt päivittäiseen toimintaan digitaalisessa toimintaympäristössä, vastaajista 85 % kokee sen melko tai erittäin turvallisena arjessa sekä 86 % työpaikalla. Myös luottamus viranomaisten (2024: 89 % vs 2023: 87 %), oman työantajaan (2024: 85 % vs 2023: 82 %) kykyyn käsitellä turvallisesti henkilötietojasi ja muita tärkeitä tietojasi on jopa noussut ja vaikka luottamus finanssialan palveluihin on laskenut 4 prosenttiyksikköä eli on nyt 88 %, tätäkin voidaan pitää erittäin hyvänä tuloksena.

Lisätietoja vuoden 2024 digiturvabarometristä löydät täältä: Digiturvabarometri- raportti

Lisätietoja kokonaiskuvapalvelusta antaa:

Erityisasiantuntija Tapani Rinne, puh. 0295 537 266, tapani.rinne@dvv.fi

1 Johdon tiivistelmä

Digi- ja väestötietovirasto toteutti helmi-maaliskuussa 2025 Digiturvan kokonaiskuvapalvelun kampanjan, johon saatiin 203 vastausta julkisen hallinnon organisaatioilta. Saman sisältöinen kysely on tehty myös vuosina 2021, 2022, 2023 ja 2024; vastanneet organisaatiot tosin vaihtelevat vuosittain.

- Vuonna 2021 kampanjaan vastasi 121 organisaatiota
- Vuonna 2022 kampanjaan vastasi 118 organisaatiota
- Vuonna 2023 kampanjaan vastasi 203 organisaatiota
- Vuonna 2024 kampanjaan vastasi 185 organisaatiota
- Vuonna 2025 kampanjaan vastasi 203 organisaatiota

Yhteensä palveluun on vastannut 374 organisaatiota. Vuoden 2023 hyvinvointialueiden uudistus ja eri vuosina tapahtuneet kuntayhdistymiset ovat jonkin verran vaikuttaneet organisaatioiden määrään, jotka voivat vastata palveluun.

Vastanneiden määrää on viime vuosina vakiintunut n. 200 organisaatioon. Vastaajaorganisaatioissa tapahtuu kuitenkin jonkin verran vaihtelua. Esim. vuoden 2025 kampanjaan vastasi 40 uutta organisaatiota. Mahdollisia vastaajaorganisaatioita julkishallinnossa on n. 700.

Kerätyn tiedon luotettavuutta ja vertailtavuutta saadaan parannettua sitä mukaa kun uusien vastaajien määrä lisääntyy. Toivomme, että yhä useampi julkisen hallinnon organisaatio ottaisi nämä kokonaiskuvan raportointipalvelut omaan käyttöönsä ja kytkisi ne osaksi organisaation digiturvan hallintaa ja säännöllistä johdon raportointia.

Digitaalisen turvallisuuden osa-alueissa tapahtunut kehittyminen

Digiturvan kokonaiskuvapalvelu kattaa kaikki digitaalisen turvallisuuden osa-alueet eli digiturvan johtamisen, riskienhallinnan, toiminnan jatkuvuuden ja varautumisen, tietoturvan, tietosuojan ja kyberturvallisuuden, joiden kaikkien tasapainoista kehittämistä tarvitaan digitaalisen ja fyysisen toimintaympäristön suojaamiseksi.

Tulosten perusteella voidaan todeta, että organisaatioiden hallinnollinen turvallisuus on kokonaisuudessaan kehittynyt parempaan vuosina 2021–2025. Sen sijaan yksittäisissä osa-alueissa ja tehtävissä on tapahtunut merkittävää vaihtelua. Erityisesti kyberturvallisuuden osa-alue on kehittynyt positiivisesti 2023 – 2025 kyselyiden perusteella.

Koska digitaalisen turvallisuuden kehittämiseen on rajallinen määrä henkilöresursseja ja rahaa, organisaatiot joutuvat priorisoimaan kehittämistoimiaan. Keskimäärin resurssien määrää pidettiin liian pienenä. Reaalimaailman ilmiöt kuten koronaviruspandemia, Venäjän hyökkäyssota ja globaalin maailmantilanteen kiristyminen näkyvät kehittämistoimien priorisoinnissa. Vuonna 2022 oli nähtävissä, että organisaatiot panostivat jonkin verran enemmän riskienhallintaan ja jatkuvuuden hallintaan, kun taas vuonna 2025 parantumista on nähtävissä kaikilla muilla osa-alueilla paitsi riskienhallinnassa. Resurssien puutteen vuoksi valitettavasti kaikkiin osa-alueisiin ei aina

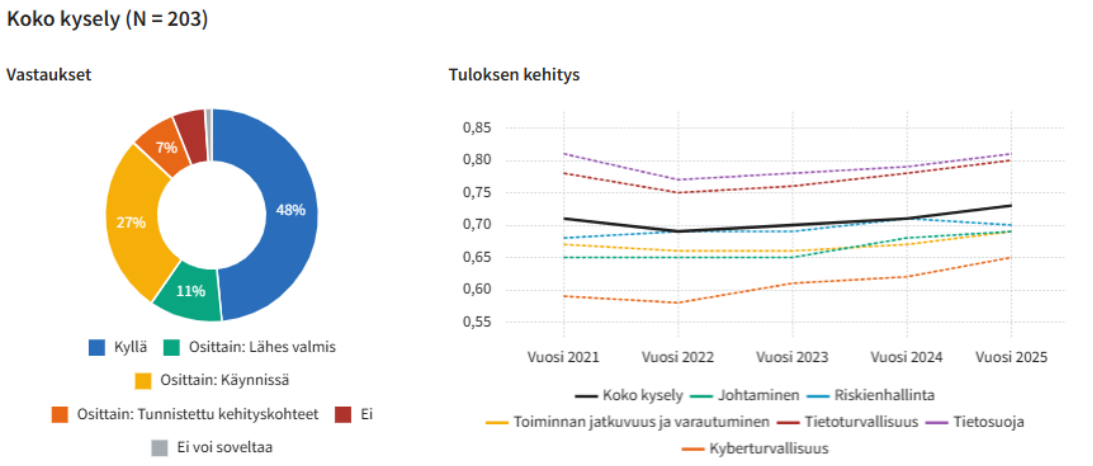
pystytä panostamaan. Resurssien puutteellisuuden vuoksi kehitys digiturvassa on maltillista. On kuitenkin syytä huomioida, että 0,01 parannus osa-alueen tulokseen on merkityksellinen. Tuloksen paraneminen muodostuu koko osa-alueen kysymyksistä ja yli 200 organisaation vastausten keskiarvosta. Yksittäisten lukuarvojen sijaan lukuarvojen trendi on siksi merkityksellisempi, kun arvioidaan kansallisesti julkisen hallinnon digi- ja kyberturvan kehittymistä

Alla olevassa taulukossa ovat vuosien 2021–2025 vastausten keskiarvot osa-alueittain. Mitä lähempänä arvoa 1, sitä paremmin organisaatiot ovat arvioineet suoriutuneensa kyselyssä esitetyissä väittämissä.

	2025	2024	2023	2022	2021
Koko kysely	**0,73**	**0,71**	**0,70**	**0,69**	**0,71**
Johtaminen	**0,69**	**0,68**	**0,65**	**0,65**	**0,65**
Riskienhallinta	**0,70**	**0,71**	**0,68**	**0,70**	**0,68**
Toiminnan jatkuvuus ja varautuminen	**0,69**	**0,67**	**0,66**	**0,67**	**0,67**
Tietoturvallisuus	**0,80**	**0,78**	**0,75**	**0,75**	**0,78**
Tietosuoja	**0,81**	**0,79**	**0,78**	**0,77**	**0,81**
Kyberturvallisuus	**0,65**	**0,62**	**0,61**	**0,59**	**0,59**

Taulukko 1. Digiturvakyselyn eri osioiden keskiarvot

Alla olevassa kuvassa sama tulos kuvattuna kaaviona sekä vastausten jakautuminen prosentteina. Lähes puolet kaikista annetuista vastauksista on Kyllä; Olemme toteuttaneet tarvittavat toimenpiteet riittävälle tasolle. Seuraavaksi eniten on vastauksia luokassa osittain: käynnissä. Lisätietoa vastausvaihtoehdoista löytyy luvusta 2.1. Osa-alueiden keskiarvot.



Kuva 1 kokonaiskuvapalvelun vastausten jakautuminen prosentteina sekä digitaalisen turvallisuuden kokonaiskuvapalvelun tuloksen kehitys, koko kysely ja digiturvan osa-alueet

Toimintaympäristön muutokset ja niiden vaikutus

Edellinen vastaavanlainen raportti Digiturvan kokonaiskuvapalvelusta tuotettiin keväällä 2023. Silloin tuloksista oli nähtävissä kyber- ja digiturvan kehityksen kääntyminen loivaan nousuun vuoden 2022 laskun jälkeen.

Kyselykierros tehtiin myös kesällä 2024. Tuloksista ei kuitenkaan tuotettu laajaa raporttia, vaan tuloksia esiteltiin DVV:n tilaisuuksissa. Silloin tuloksissa oli nähtävissä muuttuneen maailmantilanteen vaikutus. Venäjän hyökkäyssodan seurauksena organisaatioissa alettiin kiinnittää enemmän huomiota riskitilanteen seurantaan, riskien arviointiin ja niiden raportointiin johdolle. Lisäksi varautuminen ja harjoittelu oli lisääntynyt ja tietoturvallisuuteen budjetoitu raha lisääntynyt jonkin verran.

Vuonna 2025 Venäjän hyökkäyssota jatkuu edelleen ja Suomessakin on havaittu lisääntyneitä verkkohyökkäyksiä ja kielteistä verkkovaikuttamista. Kyselyn tuloksista on havaittavissa, että kyberturvallisuuden osa-alueella on tapahtunut selvää parantumista. Sen tulokset ovat edelleen osa-alueista heikoimmalla tasolla, mutta globaalin tilanteen kehittyminen pakottanee kiinnittämään siihen lisää huomiota myös jatkossa.

Kansainvälisesti verkkorikollisuus jatkaa kasvuaan, mutta se ei tämän kyselyn perusteella ainakaan merkittävästi näy organisaatioiden kokemien verkkohyökkäysten määrässä.

Kyberturvallisuuslain ja tiedonhallintalain 4a luvun vaikutukset

NIS2 -direktiivin mukaiset velvoitteet tulivat voimaan 8.4.2025. Kyberturvallisuusdirektiivin tavoitteena on vahvistaa sekä EU:n yhteistä että jäsenvaltioiden kansallista kyberturvallisuuden tasoa useiden yhteiskunnan toiminnan kannalta kriittisten toimialojen osalta. NIS 2 -direktiivi korvaa aiemman EU:n verkko- ja tietoturvadirektiivin (NIS-direktiivi), jolla on säädetty tiettyihin toimialoihin kohdistuvista kyberturvallisuusvelvoitteista. NIS 2 direktiivin pohjalta säädettiin kansallinen kyberturvallisuuslaki (124/2025) sekä tehtiin muutoksia lakiin julkisen hallinnon tiedonhallinnasta (906/2019)

Kyberturvallisuuslaki ja tiedonhallintalain luku 4a asettavat tietyille organisaatioille uusia velvoitteita muun muassa kyberturvallisuutta koskevien riskien hallintaan ja poikkeamista raportointiin.

Koska digiturvan kokonaiskuvapalvelu tarkastelee myös riskienhallinnan, poikkeamien havainnoinnin ja kyberturvallisuuden osa-alueita, voidaan tulevien vuosien tarkastelussa seurata myös uuden lainsäädännön vaikutuksia lain soveltamisalan ja yleisemminkin vastaajaorganisaatioiden arvioihin vuosittaisten muutosten ja kehittymistrendien avulla.

Keskeiset kehittämiskohteet

Tämä kyselyn tulokset painottuvat julkisen hallinnon organisaatioiden hallinnollisen digiturvan kokonaiskuvaan. Hallinnollisen turvallisuuden yhteinen kehittäminen on merkittävästi helpompaa kuin teknisen tietoturvallisuuden tai jatkuvuuden hallinnan kehittäminen. Hallinnollista digitaalista turvallisuutta voidaan kehittää esimerkiksi hankkeiden, työpajojen, tukimateriaalien sekä osaamisen kehittämisen tukivälineiden avulla. Sen sijaan teknisen tietoturvallisuuden ja jatkuvuuden hallinnan parantaminen vaativat organisaatiokohtaisia keinoja, johtuen käytössä olevista teknisistä järjestelmistä ja palveluista. Tästä huolimatta olemme nostaneet esille myös sellaisia

tekniseen tietoturvallisuuteen ja jatkuvuuden hallintaan liittyviä toimenpiteitä, joita suosittelemme organisaatioiden tarkastavan ja ottavan käyttöön omassa ympäristössään.

Kaikki suositellut kehittämiskohteet on lueteltu kappaleissa 2.2.1–2.2.7.

2 Yhteenveto tuloksista

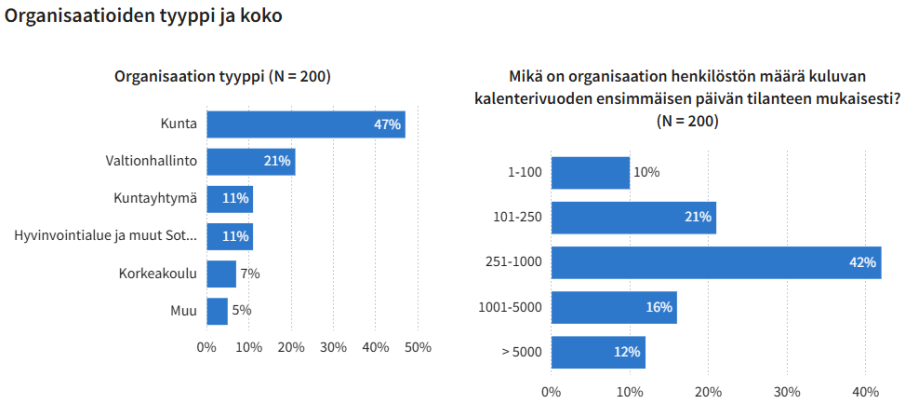
Tämä yhteenveto sisältää Digiturvan kokonaiskuvakyselyn eri osa-alueiden keskiarvotulokset, keskeiset toimiala- ja osa-aluekohtaiset havainnot sekä tulosten perusteella esille nostetut kehittämiskohteet.

Digiturvakyselyssä 2025 oli 21 taustakysymystä sekä 99 väittämää, joiden avulla kartoitettiin vastaajaorganisaatioiden digitaalisen turvallisuuden tilannekuvaa. Rakenteeltaan Digiturvakysely jakautui seuraaviin osa-alueisiin: taustatiedot, johtaminen, riskienhallinta, toiminnan jatkuvuus ja varautuminen, tietoturvallisuus, tietosuoja, kyberturvallisuus ja havainnointi. Alla oleviin kaavioihin ja taulukoihin on koottu osa-alue- ja väittämäkohtaiset keskiarvot.

Digiturvan kokonaiskuvapalvelusta ja sen tuloksista on hyvä huomioida, että kyseessä on organisaation itsearviotyökalu. Jokaisen organisaation vastaukset ovat organisaation itsensä tuottaa arvio omasta tilanteesta ko. väittämän osalta. Organisaatioiden tulkinnat väittämistä ja arviot vastauksissa voivat vaihdella organisaatioiden välillä. Digiturvan kokonaiskuvapalvelua ei siis voida pitää absoluuttisena totuutena, auditointityökaluna eikä organisaation kypsyystason mittarina.

Alla olevassa kuvassa on nähtävissä vastaajaorganisaatioiden tyyppi ja koko. Noin puolet vastaajista on kuntia. Seuraavaksi eniten vastaajia on valtiohallinnosta. 100 – 1000 henkilön organisaatiot kattavat kaksi kolmasosaa vastaajista.

Kuva 2 vastaajaorganisaatioiden tyyppi ja koko

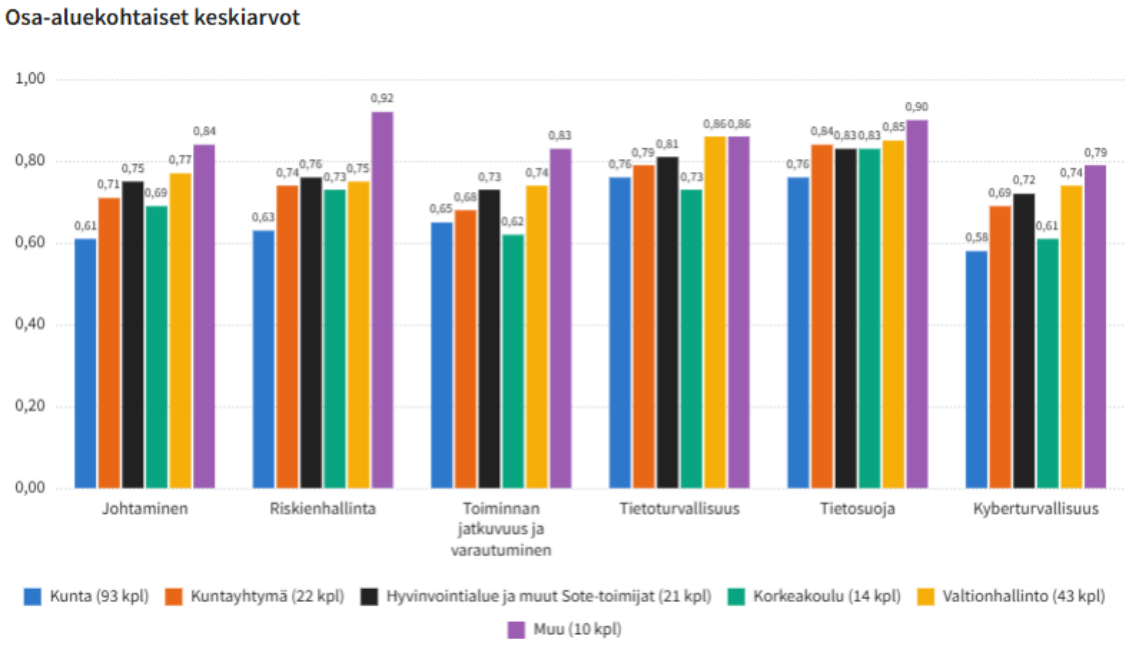


2.1 Osa-alueiden keskiarvot

Kuvassa 1 esitetään Digiturvakyselyn eri osioiden (johtaminen, riskienhallinta, toiminnan jatkuvuus ja varautuminen, tietoturvallisuus, tietosuoja ja kyberturvallisuus)

vastausten keskiarvot asteikolla 0–1. Organisaatiot vastasivat annettuihin väittämiin kuusiportaisella asteikolla ja vastaukset on pisteytetty seuraavasti:

- **Kyllä**; Olemme toteuttaneet tarvittavat toimenpiteet riittävälle tasolle. (**1,00**)
- **Osittain** – Lähes valmis; Olemme tehneet lähes kaikki tarvittavat toimenpiteet asian kehittämiseksi riittävälle tasolle. (**0,75**)
- **Osittain** – Käynnissä; Olemme määritelleet tavoitetason ja suunnitelleet tarvittavat toimenpiteet. (**0,50**)
- **Osittain** – Tunnistettu kehityskohteet; Olemme tunnistaneet, että asia on merkityksellinen organisaatiomme digiturvalle, mutta emme ole vielä aloittaneet toimenpiteitä. (**0,25**)
- **Ei**; Emme ole tunnistaneet toimenpiteitä, tai emme aio kehittää asiaa. (**0,00**)
- **Ei koske meitä**; Voimme osoittaa, että kysyttävä asia tai vaatimus ei koske meitä. (**ei huomioida keskiarvossa**)



Kuvio 1. Digiturvakyselyn eri osioiden keskiarvot vastaajaryhmittäin

Kuvion 1 tiedot on esitetty alla taulukkomuodossa (taulukko 1). Lisäksi taulukkoon on sisällytetty koko kyselyn toimialakohtaiset keskiarvot.

Taulukko 1. Digiturvakyselyn eri osioiden keskiarvot vastaajaryhmittäin

	Kaikki organisaatiot 203 kpl	**Kunta 93 kpl**	**Kuntayhtymä 22 kpl**	**Hyvinvointialue ja muut sote-toimijat 21 kpl**	**Korkeakoulu 14 kpl**	**Valtionhallinto 43 kpl**	**Muu 10 kpl**
Johtaminen	**0,69**	0,61	0,71	0,75	0,69	0,77	0,84
Riskienhallinta	**0,70**	0,63	0,74	0,76	0,73	0,75	0,92

Toiminnan jatkuvuus ja varautuminen	**0,69**	0,65	0,68	0,73	0,62	0,74	0,83
Tietoturvallisuus	**0,80**	0,76	0,79	0,81	0,73	0,86	0,86
Tietosuoja	**0,81**	0,76	0,84	0,83	0,83	0,85	0,90
Kyberturvallisuus	**0,65**	0,58	0,69	0,72	0,61	0,74	0,79
Keskiarvo	**0,73**	**0,68**	**0,75**	**0,77**	**0,70**	**0,79**	**0,86**

Korkeimmat vastauskeskiarvot saavutettiin tietosuojan (kaikkien vastausten keskiarvo 0,81) ja matalimmat kyberturvallisuuden (0,65) alueilla. Näiden ero on kuitenkin hiukan pienentynyt viime vuosina, vuonna 2023 vastaavat luvut olivat 0,78 ja 0,61. Välimaastoon asettuvat tietoturvallisuus (0,76), riskienhallinta (0,69), toiminnan jatkuvuus ja varautuminen (0,66) sekä johtaminen (0,65).

Huomionarvoista on, että kaikki osa-alueet ovat kehittyneet parempaan 2021–2025, pienistä laskuista huolimatta. Organisaatiotyyppien sisällä kehitys on ollut vielä voimakkaampaa.

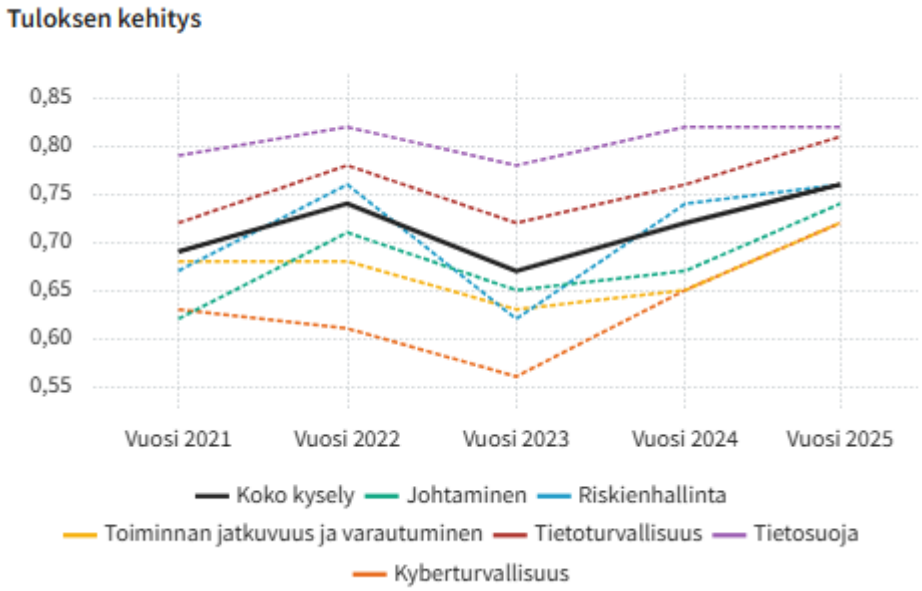
Vastaajaryhmät on muodostettu kyselyyn osallistuneiden organisaatioiden (yht. 203 organisaatiota) toimialajaottelun perusteella, ja ne ovat seuraavat:

- kunta (93 vastaajaa),
- kuntayhtymä (22 vastaajaa),
- hyvinvointialue tai muu sote-toimija (21 vastaajaa),
- korkeakoulu (14 vastaajaa),
- valtionhallinto (43 vastaajaa),
- joku muu (10 vastaajaa).

Vastaajamäärissä eri organisaatiotyyppiluokissa tapahtuu vuosittain vaihtelua. Kaikki organisaatiot eivät vastaa säännöllisesti vuosittain. Siitä syystä eri vuosien keskiarvoja ei voida suoraan verrata toisiinsa. Julkisen hallinnon vastaajien määrää vähentää tekninen rajoite, joka toistaiseksi estää palvelun käytön Y-tunnuksettomilta organisaatioilta.

Kaikkien vastaajien osalta kyselyn keskiarvotulos on 0,73. Korkein toimialakohtainen keskiarvo on ryhmässä ”muut”, johon kuuluu mm. välillistä valtionhallintoa, kuten rahastoja, säätöitä ja laitoksia (0,86), jota seuraa valtionhallinto (0,79), hyvinvointialueet (0,77), kuntayhtymät (0,75), korkeakoulut (0,70), sekä kunnat (0,68).

Eri vuosien vastauksia vertailtaessa on huomattava, että hyvinvointialueiden toiminta käynnistyi vasta vuoden 2023 alussa. Digiturvakyselyssä kartoitetaan organisaation toimintaprosesseja ja menettelyitä, jotka ovat aloittavissa organisaatioissa väistämättä vasta kehitysvaiheessa. Tästä syystä sote-toimijoiden tulokset ovat putosivat huomattavasti vuodesta 2022, jolloin ne menestyivät hyvin erityisesti riskienhallinnassa ja jatkuvuuden hallinnassa. Vuosina 2024 ja 2025 kampanjoissa hyvinvointialueiden tulokset ovat kuitenkin kehittyneet erittäin voimakkaasti. Poikkeuksen tekee tietosuoja, joka sote-toimijoilla on ollut lähtökohtaisesti korkealla tasolla.



Kuvio 2. Hyvinvointialueiden digiturvan osa-alueiden kehitys vuosina 2021 - 2025

Verrattaessa sote-toimijoiden vastauksia edellisiin vuosiin voidaan havaita, että kehitys on ollut voimakasta erityisesti kyberturvallisuudessa. Tietosuojan ja riskienhallinnan kehitys on taittunut maltillisempaan kehitykseen 2025 tulosten perusteella. Erityisesti puutteita on mittaristojen asettamisessa, toimittajayhteistyössä riskienhallinnassa, digiturvan kehittämisessä osana kokonaisarkkitehtuuria ja rakenteettoman tiedon tunnistamisessa. Myös auditointien toteuttamisessa on kehitettävää ja digiturvan vastuuhenkilöiden määrä arvioidaan liian pieneksi.

Koska Digiturvakyselyn viimeinen osio ”Havainnointi” poikkeaa vastausrakenteeltaan muista, sen tuloksia ei ole mukana vertailutaulukossa. Sen sijaan vastaajaorganisaatioiden havainnoimia ja raportoimia digiturvauhkia analysoidaan erikseen kappaleessa 2.2.7.

2.2 Kysymyskohtaiset keskiarvot

Taulukoissa 2–8 eritellään Digiturvakyselyn osa-alueiden – johtaminen, riskienhallinta, jatkuvuus ja varautuminen, tietoturvallisuus, tietosuoja, kyberturvallisuus ja havainnointi – väittämäkohtaiset vastauskeskiarvot sekä kaikkien vastaajien osalta että toimialakohtaisesti. Taulukon keskiarvot ovat värikoodattu. Samaa värikoodausta käytetään kaikkien osa-alueiden väittämien keskiarvoissa. Mitä lähempänä arvoa 1,00 keskiarvo on, sitä parempi tilanne ko. väittämän osalta on. Värikoodit ja niiden arvot:

- Punainen: arvot 0,00–0,29 (Suurin osa vastauksista ei ja osittain – tunnistettu kehityskohteet, vain vähän kyllä vastauksia)
- Oranssi: arvot 0,30–0,59
- Keltainen: arvot 0,60–0,79

- Vihreä: arvot 0,80–1,00 (Suurin osa vastauksista kyllä ja osittain – lähes valmis)

2.2.1 Johtaminen

Taulukossa 2 esitetään johtamisosion 13 väittämän vastauskeskiarvot.

Taulukko 2. Johtaminen – kysymyskohtaiset keskiarvot

Johtaminen / Väittämä	Kaikki organisaatiot 203	Kunta 93 kpl	Kuntayhtymä 22 kpl	Hyvinvointialue ja muut Sote-toimijat 21 kpl	Korkeakoulu 14 kpl	Valtionhallinto 43 kpl	Muu 10 kpl
1. Organisaation digitaalisen turvallisuuden tehtävät ja vastuut on tunnistettu ja kuvattu selkeästi.	0,76	0,67	0,81	0,84	0,77	0,84	0,95
2. Organisaatio on kartoittanut sen digitaalista turvallisuutta ohjaavan lainsäädännön ja tunnistanut siitä aiheutuvat velvoitteet.	0,76	0,64	0,75	0,95	0,8	0,89	0,8
3. Organisaatio on kartoittanut keskeiset sidos- ja asiakasryhmät sekä niiltä tulevat digiturvavaatimukset.	0,7	0,58	0,71	0,76	0,73	0,81	0,95
4. Organisaatiossa on riittävästi osaavaa henkilöstöä digiturvallisuuden eri osa-alueilla.	0,53	0,45	0,64	0,58	0,52	0,6	0,65
5. Organisaatiolla on riittävä budjetti digiturvallisuuden ylläpitoon sekä kehittämiseen.	0,61	0,53	0,76	0,59	0,54	0,65	0,75
6. Organisaation johto on sitoutunut digitaalisen turvallisuuden kehittämiseen.	0,77	0,69	0,78	0,8	0,75	0,87	0,88
7.Organisaation digitaalisen turvallisuuden osa-	0,63	0,52	0,75	0,67	0,7	0,7	0,88

alueita kehitetään järjestelmällisesti.							
8. Henkilöstölle on olemassa riittävä ohjeistus digitaalisesta turvallisuudesta.	0,72	0,69	0,74	0,65	0,73	0,75	0,83
9. Henkilöstölle annetaan säännöllisesti koulutusta digitaalisesta turvallisuudesta.	0,7	0,65	0,64	0,78	0,55	0,8	0,85
10. Organisaatiolla on olemassa prosessi väärinkäytöksiin reagoimiseksi.	0,84	0,79	0,84	0,87	0,84	0,9	0,98
11. Digitaaliseen turvallisuuteen liittyvät mittarit on määritelty.	0,4	0,32	0,35	0,48	0,48	0,48	0,68
12. Digitaalisen turvallisuuden tilaa seurataan jatkuvasti.	0,79	0,73	0,86	0,78	0,86	0,82	0,88
13. Digitaalisen turvallisuuden kokonaistilanteesta raportoidaan säännöllisesti organisaation johdolle.	0,74	0,67	0,64	0,79	0,64	0,88	0,9

Paras kysymyskohtainen keskiarvo (0,98) oli väittämässä 10, joka koskee prosessia väärinkäytöksiin reagoimisessa. Tämän väittämän keskiarvot ovat korkealla kaikissa vastaajaorganisaatioiden tyyppiluokissa. Seuraavaksi parhaat keskiarvot ovat keskeisten sidosryhmien kartoittamisen tilanne ja vastuiden ja tehtävien tunnistaminen ja kuvaaminen (0,95). Heikointa suoriutuminen on digitaalisen turvallisuuden mittaristoa koskevassa väittämässä (0,32). Mittarien määrittely oli heikolla tasolla kaikissa vastaajaorganisaatioluokissa paitsi ryhmässä muut (0,68). Lisäksi väittämät ”Organisaatiolla on riittävä budjetti digiturvallisuuden ylläpitoon ja kehittämiseen” ja ”Organisaatiossa on riittävästi osaavaa henkilöstä kehittämässä digiturvallisuuden eri osa-alueita” osoittavat, että resurssien kanssa tuskaillaan hyvin monissa organisaatiossa.

Yksi keino kehittää organisaation digiturvaan liittyvä mittaristoa on ottaa kokonaiskuvapalvelu ja siellä olevat kyselyt osaksi organisaation digiturvan mittaamista ja raportointia.

Osa-alueen kokonaiskeskiarvo (0,69) on digiturvallisuuden viidestä osa-alueesta toiseksi matalin yhdessä toiminnan varautumisen ja jatkuvuuden kanssa. Eroja toimialojen kesken on; korkein keskiarvo on ryhmässä muut (0,84) ja alin kunnilla (0,61). Kunnat ja korkeakoulut ovat ainoat ryhmät, joissa keskiarvo on alle 0,70.

Kaikilla muilla organisaatiotyypeillä osa-alueen keskiarvo on nousussa paitsi kunnissa ja kuntayhtymissä. Keskiarvon kasvu on voimakkainta hyvinvointialueilla (2023: 0,67 → 2025: 0,76)

Kehitys vuoteen 2023 verrattuna

Vuoden 2023 kyselyyn verrattuna kokonaiskeskiarvo on kasvanut 0,65 → 0,69. Myös yksittäisten väittämien tuloksissa on pientä vaihtelua. Väittämien keskinäinen järjestys on pysynyt kutakuinkin samana. Digiturvallisuuden tilanteen seuranta on hiukan parantunut, kenties kyberhyökkäysten määrästä ja maailmantilanteen muutoksista johtuen. Lisäksi osaavan henkilöstön ja riittävän budjetin tilanne on kehittynyt hieman parempaan, vaikka suuressa osassa organisaatioita osaavan henkilöstön määrä ja riittävä budjetti digiturvan ylläpitoon ja kehittämiseen koetaan edelleen riittämättömäksi.

Eri toimialojen keskiarvoissa on tapahtunut pieniä muutoksia; valtionhallinnossa taso on hiukan noussut ja sote-toimijoiden osalta kasvu on ollut merkittävämpää. Kunnissa osa-alue on pysynyt käytännössä samana, vaikka vuoden 2024 tuloksissa näkyikin pientä kehitystä parempaan.

Johtamisen kehittämiskohteet

Kehittämiskohde – Osaamisen kehittäminen

Henkilöstön osaamisen ja koulutustarpeiden edelleen kehittäminen. Jokaisella organisaatiolla tulisi olla selkeä suunnitelma siitä, mistä aiheista koulutetaan ja mistä muistutetaan esimerkiksi sisäisellä viestinnällä. Asioiden omaksumista ja muistamista edistää se, että niitä käsitellään pitkin vuotta. Asiantuntijoiden osaamistarpeet voivat poiketa muun henkilökunnan tarpeista.
Suosittelemme osallistumaan hyödyntämään digiturvan tietopankkia (linkki) ja palveluhakemistoa(linkki), hyödyntämään Digiturvallinen elämä -materiaaleja (linkki) sekä seuraamaan Digi- ja väestötietoviraston tuottamia verkkotilaisuuksia (linkki). Kuukausittaisen digiturvatunnin avulla organisaation henkilöstö saa säännöllistä digiturvakoulutusta läpi vuoden. Jo tämän koulutuksen avulla organisaatioiden digiturvakoulutuksen määrää saisi nostettua seuraavalle tasolle.

Kehittämiskohde – Harjoittelu

Harjoitustoiminnan kehittäminen. Organisaation johdolla on kriittinen rooli erilaisten kriittisten häiriötilanteiden, hyökkäysten ja loukkausten hallinnan johtamisessa, ja siksi johdon ja asiantuntijoiden tulisi harjoitella yhdessä. Mikäli organisaatio ei ole aiemmin toteuttanut digitaalisen turvallisuuden harjoituksia, se voi osallistua siihen joko marraskuussa 2025.
https://dvv.fi/taisto

Kehittämiskohde – Prosessit kuntoon

Prosessit kuntoon. Digitaaliseen turvallisuuteen liittyvät tärkeimmät prosessit tulee kuvata ja jalkauttaa, jotta niistä saadaan luontainen osa organisaation toimintaa. Prosessien toimivuutta tulee seurata ja kehittää niitä edelleen systemaattisesti. Digiturvallisuuden hallintamallien kehittämiseen löytyy materiaalia digiturvan tietopankista (linkki)

Kehittämiskohde – Resurssointi

Digiturvan resurssointi koetaan edelleen julkisessa hallinnossa riittämättömäksi. Erityisesti kunnissa, korkeakouluissa ja hyvinvointialueilla koetaan, että digiturvaan ei ole riittävää budjettia ja organisaatioilla ei ole riittävästi osaavaa henkilöstöä digiturvan eri osa-alueille. Tilanne on hieman parempi valtiohallinnossa ja kuntayhtymissä sekä ryhmässä muut, mutta erot ovat pieniä. 2/3 organisaatioista vastasi, että heillä on käytettävissä alle 1 htv jokaisella digiturvan

eri osa-alueella. 78% organisaatioista käyttää alle 100 000€ digiturvan kehittämiseen. Neljännes vastaajista käyttää alle 10 000€ vuodessa digiturvan kehittämiseen. Digitaalisen turvallisuuden ylläpitokustannuksiksi 38% vastaajista arvioi alle 100 000€ ja 29% alle 1 000 000€. Nämä kehittämis- ja ylläpitokustannukset eivät ole organisaatioiden vastausten perusteella riittäviä. Suosittelemme että organisaatiot seuraavat

Kehittämiskohde – Mittarointi
Digiturvakyselyn ja kokonaiskuvapalvelun olemassa oloajan, digitaaliseen turvallisuuteen liittyvien mittareiden määrittely on ollut yksi heikoimman keskiarvon saaneista väittämistä vuosittain. Mittarointiin liittyvän väittämän keskiarvot ovat heikolla tasolla koko julkishallinnossa. Kuntien osalta keskiarvo on alhaisin (0,32). Kuntayhtymissä tilanne on toiseksi huonoin (0,35). Hyvinvointialueilla, korkeakouluissa ja valtiohallinnossa tilanne on hieman parempi (0,48). Ryhmässä muut keskiarvo on parhaimmalla tasolla (0,68). Suosittelemme hyödyntämään digiturvan kokonaiskuvapalvelua ja Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen Kybermittaria (linkki) organisaation digiturvan mittaroinnissa ja kyber- sekä digitaalisen turvallisuuden kehittämisessä. Mittareita hyödyntämällä myös edellisen kehittämiskohteen eli resurssoinnin tilannetta voidaan kehittää, koska mittareita hyödyntämällä voidaan olemassa olevat resurssit kohdentaa paremmin ja tehokkaammin.

Kehittämiskohde – johdolle raportointi
Mittareiden tehokkaamman hyödyntämisen ohella suosittelemme johdolle raportoinnin kehittämisestä. Lisäksi suosittelemme, että organisaation johto edellyttää raportointia heille organisaation kyber- ja digitaalisen turvallisuuden tilanteesta ja kehittämisestä. Johdolle raportointi tukee johdon toimia resurssien kohdentamiseksi oikein sekä keskeisimpien kehityskohteiden tunnistamista ja kehittämistä, mitä mm. kyberturvallisuuslaki ja tiedonhallintalaki edellyttää.

2.2.2 Riskienhallinta

Taulukossa 3 esitetään riskienhallinnan yhdeksän väittämän vastauskeskiarvot.

Taulukko 3. Riskienhallinta – kysymyskohtaiset keskiarvot

Riskienhallinta / Väittämä	**Kaikki organisaatiot 202 kpl**	**Kunta** 93 kpl	**Kuntayhtymä** 22 kpl	**Hyvinvointialue ja muut Sote-toimijat** 21 kpl	**Korkeakoulu** 14 kpl	**Valtionhallinto** 43 kpl	**Muu** 10 kpl
14. Organisaatiolla on johdon hyväksymät, toimintaan sovitetut riskienhallinnan linjaukset, vastuut ja prosessi.	0,78	0,68	0,8	0,81	0,84	0,88	0,9
15. Organisaatio tekee digiturvallisuuteen liittyvää säännöllistä riskienarviointia, jossa huomioidaan uudet ilmiöt, toimintaympäristön muutokset ja oman toiminnan vaikutukset sidosryhmien ja asiakkaiden tilanteeseen.	0,61	0,52	0,57	0,75	0,7	0,67	0,93
16. Organisaatiossa viestitään digiturvallisuuden riskitilanteesta	0,79	0,79	0,82	0,8	0,75	0,76	0,95

ja uusista riskeistä koko organisaation laajuisesti.							
17. Organisaatiossa raportoidaan riskitilanteesta johdolle säännöllisesti.	0,78	0,69	0,82	0,85	0,8	0,84	1
18. Organisaation tunnistamat kriittiset riskit raportoidaan johdolle välittömästi.	0,88	0,84	0,98	0,9	0,82	0,91	1
19. Organisaatio seuraa riskien ja niiden hallintatoimenpiteiden tilannetta säännöllisesti.	0,7	0,64	0,74	0,75	0,71	0,72	0,93
20. Organisaation ylin johto sekä organisaation hallitus (tai vastaava) seuraa merkittävien riskien ja niiden hallintatoimenpiteiden tilannetta säännöllisesti.	0,55	0,46	0,64	0,59	0,63	0,62	0,85
21. Organisaatiossa arvioidaan jäännösriskejä riskienhallintatoimenpiteiden toteuttamisen jälkeen ja jäännösriskit käsitellään asianmukaisella tasolla.	0,55	0,48	0,58	0,66	0,5	0,62	0,78
22. Organisaatiossa kehitetään riskienhallintaprosessia saatujen riskienhallinnan tavoitteiden tai saatujen kokemusten perusteella.	0,68	0,59	0,7	0,74	0,79	0,72	0,9

Korkein kysymyskohtainen keskiarvo saavutettiin väittämässä, joka koski kriittisten riskien raportoimista johdolle välittömästi (0,88). Kysymyksen keskiarvo laski vähän viime vuodesta (0,89) Heikoimmiksi tuloksiksi jää organisaation ylimmän johdon merkittävien riskien ja niiden hallintatoimenpiteiden seuraaminen sekä jäännösriskien arvioinnissa ja käsittelyssä (0,55) sekä säännöllisessä digiturvallisuuteen liittyvässä riskienarvioinnissa, jossa huomioidaan uudet ilmiöt, toimintaympäristön muutokset ja oman toiminnan vaikutukset sidosryhmien ja asiakkaiden tilanteeseen (0,61).

Osa-alueen keskiarvo on 0,70. Osa-alueen keskiarvo laski vuodesta 2024 vähän (0,69). Suhteessa vuoden 2023 tilanteeseen osa-alueen keskiarvo on kuitenkin parantunut vähän (0,69)

Kehitys vuoteen 2023 verrattuna

Osa-alueen keskiarvo on hieman parempi kuin vuoden 2023 keskiarvo (0,69 → 0,70). Väittämien keskinäisessä järjestyksessä ei ole käytännössä muutoksia, mutta riskienhallinnan säännöllisyydessä ja johdolle raportoinnissa on tapahtunut pientä parannusta. Osa-alueessa on myös yksi uusi kysymys:

Organisaation ylin johto sekä organisaation hallitus (tai vastaava) seuraa merkittävien riskien ja niiden hallintatoimenpiteiden tilannetta säännöllisesti

Vastausten perusteella organisaatioiden ylimmällä johdolla on kehitettävää merkittävien riskien ja niiden hallintakeinojen seuraamisessa.

Vastaajaryhmistä suurin muutos on sote-toimijoilla, joiden tulos on parantunut merkittävästi (0,60 → 0,73). Käytännössä kaikissa vastaajaryhmissä riskienhallinnan osa-alue on kehittynyt parempaan vuodesta 2023 paitsi valtiohallinnossa, jossa keskiarvo on pysynyt samana (0,75).

Riskienhallinnan kehittämiskohteet

Kehittämiskohde – Kokonaisvaltainen riskienhallinta
Digitaalisen toimintaympäristön riskienhallinnan kokonaisvaltainen kehittäminen. Riskien arviointia tulee toteuttaa järjestelmällisesti kaikissa keskeisissä muutoksissa, häiriöissä ja poikkeamissa – niin sisäisissä kuin ulkoisissa. Organisaatiolla tulee olla kuvattuna riskienhallinnan toteuttamista ohjaavat linjaukset, joissa kuvataan siihen liittyvät menettelytavat ja vastuut. Vain kerran vuodessa tehtävästä toiminnasta on syytä päästä useammin toteutettavaan muutosarviointiin ja uusien riskien tunnistamiseen. Toistuvuuteen tulee yhdistää seurantatoimet ja jäännösriskien tarkastelu. Muutosten ja riskitasojen seurannan raportointia johdolle pitää kehittää. Myös johdon tulee vaatia riskienhallinnan raportointia, toimenpiteiden toteutumisen raportointia ja jäännösriskien hallintakeinoista tietoa johdolle sopivassa muodossa.

2.2.3 Toiminnan jatkuvuus ja varautuminen

Toiminnan jatkuvuus ja varautuminen -osion 16 väittämän vastauskeskiarvot ovat taulukossa 4.

Taulukko 4. Toiminnan jatkuvuus ja varautuminen – kysymyskohtaiset keskiarvot

Toiminnan jatkuvuus ja varautuminen / Väittämä	**Kaikki organisaatiot 202kpl**	Kunta 93 kpl	Kuntayhtymä 22 kpl	Hyvinvointialue ja muut Sote-toimijat 21 kpl	Korkeakoulu 14 kpl	Valtionhallinto 43 kpl	Muu 10 kpl
23. Organisaation tehtävät ja vastuut ovat selkeät myös poikkeustilanteissa ja poikkeusoloissa.	0,84	0,84	0,85	0,83	0,87	0,81	0,93
24. Organisaatiolla on prosessi ja valmiudet nopeaan	0,77	0,69	0,85	0,81	0,75	0,84	0,9

ja tehokkaaseen digiturvallisuuden häiriöiden, uhkien ja poikkeamien käsittelyyn.							
25. Organisaatio on kuvannut jatkuvuuden hallinnan periaatteet, tavoitteet, organisoinnin ja vastuut.	0,63	0,56	0,64	0,63	0,64	0,76	0,7
26. Organisaatio on tunnistanut ja dokumentoinut suojattavat kohteet.	0,69	0,66	0,74	0,69	0,68	0,73	0,85
27. Suojattavien kohteiden tunnistamiseen ja kriittisyyden määrittelyyn on dokumentoitu ja hyväksytty menetelmä.	0,67	0,6	0,72	0,75	0,71	0,76	0,81
28. Organisaatio on määritellyt kuinka pitkiä toimintakatkoksia kriittiset toiminnot sietävät organisaation toiminnan häiriintymättä.	0,56	0,53	0,6	0,6	0,34	0,63	0,58
29. Toiminnan jatkuvuuden edellyttämät palvelutasovaatimukset ovat osa hankintavaatimuksia ja sopimuksia.	0,69	0,66	0,69	0,75	0,7	0,71	0,85
30. Jatkuvuuteen liittyviä riskejä ja riskitilanteen muutosta arvioidaan säännöllisesti.	0,58	0,49	0,57	0,71	0,43	0,66	0,88
31. Organisaatiolle ja sen kriittisille toiminnoille/palveluille on laadittu jatkuvuussuunnitelmat, jotka perustuvat tunnistettuihin riskeihin.	0,54	0,49	0,43	0,55	0,39	0,66	0,8
32. Kriittisille tietojärjestelmille on laadittu toipumissuunnitelmat.	0,59	0,49	0,63	0,71	0,45	0,67	0,88
33. Organisaatiolla on häiriö- ja kriisitilanteiden viestintäsuunnitelma.	0,87	0,86	0,81	0,88	0,73	0,91	0,98
34. Suunnitelmien sisältö on koulutettu häiriötilanteiden hallintaan osallistuville henkilöille.	0,6	0,6	0,57	0,57	0,59	0,62	0,7
35. Organisaatiossa on luotu yhteydet ja verkostot tarvittavien sidosryhmien väliseen viestintään poikkeamatilanteissa.	0,72	0,71	0,65	0,75	0,57	0,77	0,8
36. Organisaatiolla on olemassa menettely sen toimintaa kohdistuvien häiriöiden, hyökkäysten ja loukkausten ilmoittamiseksi keskeisille viranomaisille.	0,92	0,9	0,93	0,98	0,88	0,96	0,95

37. Organisaatio harjoittelee säännöllisesti sen toimintaan kohdistuvien häiriöiden, poikkeamien ja hyökkäysten havainnointia, reagointia ja johtamista.	0,72	0,68	0,57	0,8	0,71	0,76	0,83
38. Jatkuvuus-, toipumis- ja viestintäsuunnitelmia päivitetään harjoitusten tai toteutuneiden häiriötilanteiden perusteella.	0,65	0,64	0,63	0,71	0,5	0,66	0,85

Osion kaikkien vastausten keskiarvo on 0,69. Korkein kysymyskohtainen keskiarvo (0,92) oli väittämässä ”Organisaatiolla on olemassa menettely sen toimintaan kohdistuvien häiriöiden, hyökkäysten ja loukkausten ilmoittamiseksi keskeisille viranomaisille”. Heikoimmat keskiarvot koskivat riskienhallinnan huomioimista jatkuvuussuunnittelussa. Siihen liittyvät väittämät ”Jatkuvuuteen liittyviä riskejä ja riskitilanteen muutosta arvioidaan säännöllisesti” (0,58) ja ”Organisaatiolle ja sen kriittisille toiminnoille/palveluille on laadittu jatkuvuussuunnitelmat, jotka perustuvat tunnistettuihin riskeihin” (0,54).

Toimialoista korkeimpaan keskiarvoon yltää ryhmä muut (0,80) ja matalin keskiarvo on korkeakouluilla (0,62).

Kehitys vuoteen 2023 verrattuna

Osa-alueen keskiarvo on hiukan parantunut kahden vuoden takaisesta 0,67 →0,69. Organisaatiotyypeittäin kehitys on ollut:

Kunnat 0,65 → 0,65

Kuntayhtymä 0,77 → 0,74

Hyvinvointialueet ja muut sotetoimijat 0,63 → 0,72

Korkeakoulut 0,62 → 0,62

Valtiohallinto 0,74 → 0,76

Muut 0,66 → 0,80

Hyvinvointialueilla on tapahtunut kahdessa vuodessa merkittävää kasvua. Tämä on mahdollisesti seurausta toimintatapojen vakiintumisesta yhtenäistymisestä. Lisäksi Sosiaali- ja terveysministeriö on tukenut hyvinvointialueiden digiturvan kehittämistä kohdennetusti digiturvan kokonaiskuvan tulosten pohjalta.

Myös ryhmässä muut, on tapahtunut merkittävää kehitystä. Tässä ryhmässä kuitenkin vastaajien määrä on pieni, joten vaihtelu vastanneissa organisaatioissa voi vaikuttaa tuloksiin merkittävästi. Valtionhallinnossa on tapahtunut pientä parannusta. kunnissa ja korkeakouluissa keskiarvot ovat pysyneet samana ja kuntayhtymissä laskenut hieman.

Erityisen positiivista on, että vastaajaorganisaatiot ovat kattavasti tunnistanut ja kuvannut tehtävät ja vastuut poikkeustilanteissa ja poikkeusoloissa (0,84). Lähes kaikilla vastaajaorganisaatioilla on häiriö- ja kriisitilanteiden varalta viestintäsuunnitelma. Häiriö ja kriisitilanteissa viestinnän merkitys korostuu. Lisäksi lähes kaikilla vastaajilla on menettely viranomaisilmoitusten tekoon häiriö-, hyökkäys- ja loukkaustilanteissa. Taisto-harjoitusten vaikutus todennäköisesti näkyy varautumisen ja jatkuvuudenhallinnan positiivisessa kehityksessä. Taistossa viranomaisilmoitusten laatiminen on olennainen tehtävä ja harjoitus on helppo tapa aloittaa kyberharjoittelu, jos organisaatio ei ole aiemmin harjoitellut.

Toiminnan jatkuvuuden ja varautumisen kehittämiskohteet

Kehittämiskohde – Kokonaisvaltainen jatkuvuuden hallinta riskilähtöisesti
Jatkuvuuden hallinnan kehittäminen. Jokaisen organisaation tulisi varautua toimintaa merkittävästi haittaaviin häiriöihin. Organisaatiolla tulisi olla kuvattuna jatkuvuuden hallintaa ohjaavat linjaukset, joissa kuvataan mm. häiriötilanteiden johtaminen, vastuut ja viestintä. Kriittiset toiminnot ja palvelut tulee tunnistaa ja laatia jatkuvuussuunnitelmat ainakin niille. Olennainen osa jatkuvuuden hallintaa on häiriötilanteiden harjoittelu ja suunnitelmien päivittäminen niistä saatujen oppien perusteella. Edelle kuvattu tulee tehdä tunnistettujen riskien pohjalta ja riskiympäristön muutoksia tulee seurata säännöllisesti.

2.2.4 Tietoturvallisuus

Taulukossa 5 esitetään Tietoturvallisuus-osion 16 väittämän vastauskeskiarvot.

Taulukko 5. Tietoturvallisuus – kysymyskohtaiset keskiarvot

Tietoturva / Väittämä	Kaikki organisaatiot 203 kpl	Kunta 93 kpl	Kuntayhtymä 22 kpl	Hyvinvointialue ja muut Sote-toimijat 21 kpl	Korkeakoulu 14 kpl	Valtionhallinto 43 kpl	Muu 10 kpl
39. Organisaatiolla on johdon hyväksymä tietoturvapolitiikka tai vastaava tietoturvallisuuden toteuttamista ohjaava asiakirja.	0,95	0,94	0,94	0,98	0,95	0,93	1

40. Organisaatiolla on olemassa henkilöiden taustatarkistuksiin liittyvä menettely, joka kattaa oman ja palvelutoimittajien henkilöstön.	0,59	0,39	0,37	0,89	0,25	0,97	0,5
41. Organisaatiolla on olemassa käyttövaltuuspolitiikka ja prosessi käyttövaltuuksien hallintaan.	0,8	0,78	0,76	0,78	0,79	0,83	0,9
42. Käyttövaltuuksien ajantasaisuus varmistetaan säännöllisesti.	0,68	0,67	0,74	0,66	0,63	0,71	0,65
43. Organisaatio on määrittänyt fyysisesti suojatut turvallisuusalueet asiakirjojen käsittelyn ja tietojärjestelmien suojaamiseksi.	0,72	0,64	0,65	0,66	0,71	0,9	0,86
44. Organisaation tietojärjestelmät ja laitteet ovat kattavasti järjestelmänhallinnan piirissä.	0,89	0,88	0,93	0,88	0,89	0,88	0,95
45.Organisaatiolla on käytössä monivaiheinen tunnistus etäkäytössä.	0,87	0,82	0,91	0,93	0,8	0,97	0,78
46. Toimitilojen ulkopuolella työskenneltäessä yhteydet organisaation ICT-palveluihin	0,87	0,92	0,77	0,91	0,75	0,83	0,89

sallitaan vain VPN-yhteydellä.							
47. Organisaatiolla on olemassa tarvittavat tekniset ratkaisut ja menettelyt haittaohjelmien tunnistamiseen ja estämiseen.	0,95	0,94	0,95	0,95	0,91	0,95	1
48. Organisaation tiedoista ja järjestelmistä otetaan säännöllisesti varmuuskopiot.	0,92	0,92	0,99	0,89	0,88	0,92	0,98
49. Varmuuskopioiden palautusta testataan säännöllisesti.	0,59	0,6	0,67	0,55	0,5	0,56	0,7
50. Tietojärjestelmien käytöstä ja tietojen luovutuksista kerätään riittävät lokitiedot.	0,71	0,69	0,72	0,73	0,55	0,78	0,78
51. Käytössä olevien tietojärjestelmien teknisiin haavoittuvuuksiin liittyviä tiedotteita seurataan ja niihin reagoidaan.	0,94	0,93	0,92	0,93	0,93	0,95	0,98
52. Tietoturvallisuuteen ja tietojärjestelmiin liittyviä auditointeja tehdään säännöllisesti.	0,56	0,44	0,51	0,52	0,45	0,76	0,83
53. Tietoturva- ja tietosuojavaatimukset ovat osa	0,87	0,82	0,83	0,94	0,86	0,94	0,93

hankintavaatimuksia ja sopimuksia.							
54. Tietoturva- ja tietosuojavaatimukset otetaan huomioon myös järjestelmien ja palveluiden kehittämisessä sekä ylläpidossa.	0,83	0,8	0,88	0,86	0,7	0,87	0,95

Kyselyn osa-alueista tietoturvallisuus yltää kokonaiskeskiarvollaan (0,80) toiseksi korkeimmalle sijalle tietosuojan jälkeen. Hyvää tulosta selittää se, että kaikista digiturvallisuuden osa-alueista tietoturvallisuutta on kehitetty pisimpään ja sitä koskeva lainsäädäntö (tiedonhallintalaki) on koskenut koko julkista hallintoa vuoden 2020 alusta lähtien.

Kysymyksistä paras kokonaiskeskiarvo koskee haittaohjelmien torjuntaa (0,95) sekä johdon hyväksymiä tietoturvapolitiikoita ja tietoturvaa ohjaavia asiakirjoja koskeva väittämä (0,95). Vaatimattomimmat tulokset ovat kohdissa ”Tietoturvallisuuteen ja tietojärjestelmiin liittyviä auditointeja tehdään säännöllisesti”, joka on kuitenkin kehittynyt merkittävästi kahden vuoden takaisesta (0,51 → 0,56) ja ”Organisaatiolla on olemassa henkilöiden taustatarkistuksiin liittyvä menettely, joka kattaa oman ja palvelutoimittajien henkilöstön” joka sekin on kehittynyt parempaan huomattavasti (0,48 → 0,59). Lisäksi varmuuskopioiden testaamisessa on parantamisen varaa (0,59).

Toimialoista korkein keskiarvo on valtionhallinnolla ja ryhmällä muut (0,86) ja alin korkeakouluilla (0,73). Toimialojen väliset keskiarvoerot ovat siten kohtaisen suuria. Kehitystä parempaan on kuitenkin tapahtunut kaikissa organisaatiotyypeissä paitsi kuntayhtymissä, jossa oli pieni lasku.

Kehitys vuoteen 2023 verrattuna

Osa-alueen keskiarvo on kehittynyt kokonaisuudessaan parempaan kahden vuoden takaisesta, 0,76 → 0,80.

Kehitys organisaatiotyypeittäin:

Kunnat 0,73 → 0,76

Kuntayhtymät 0,81 → 0,79

Hyvinvointialueet ja muut sote-toimijat 0,72 → 0,81

Korkeakoulut 0,67 → 0,73

Valtiohallinto 0,84 → 0,87

Muut 0,72 → 0,79

Eniten kehitystä tapahtui hyvinvointialueilla. Tämä voi olla seurausta hyvinvointialueiden toimintojen vakiintumisesta ja yhtenäisestä kehittämisestä. Myös Sosiaali- ja terveysministeriö on tukenut hyvinvointialueiden digiturvan kehittämistä Digiturvan kokonaiskuvapalvelun tulosten perusteella kohdennetusti, joten tämä selittänee osaltaan HVA-sektorin tulosten kehittymistä.

Tietoturvallisuuden kehittämiskohteet

Kehittämiskohde – Taustatarkistukset
Henkilöiden taustatarkistuksiin liittyvään prosessiin tulee kiinnittää huomiota erityisesti kunnissa ja korkeakouluissa. Vaikka suhteellisesti näissä organisaatiotyypeissä tehdään vähemmän taustatarkistuksia, tulee organisaatiolla olla menettely sellaisten roolien tunnistamiseen, joissa taustatarkistus tulee tehdä sekä prosessi tarkistuksen toteuttamiseksi, kun tarve havaitaan. Menettelyiden ja suunnitelmien tulee huomioida myös toimitusketjut.

Kehittämiskohde – Varmuuskopiointi ja niiden tarkistaminen
Toimiva varmuuskopiointi, jonka merkitys on kasvanut sitä mukaa kun lunnashaittaohjelmahyökkäykset ovat yleistyneet. Organisaation tulisi varmistaa säännöllisesti tehtävällä palautusharjoituksella kriittisten palveluiden ja niissä olevien tietojen saatavuus ja eheys. Ulkoistettujen palvelujen osalta tulee varmistaa, että palvelun tarjoajan prosessit ovat toimivat ja riittävät tiedon turvaamiseksi myös poikkeavissa tilanteissa.

Kehittämiskohde – Lokittaminen
Kattavat lokitiedot ja niiden käytettävyys. Lokitietojen tärkeys on noussut useasta eri syystä: niiden avulla voidaan tunnistaa ja ennakoida organisaatioon kohdistuvia hyökkäyksiä, selvittää toteutuneita hyökkäyksiä ja varmistaa tietojen asianmukainen käyttö eri tietojärjestelmissä. Lokitietojen riittävyys ja käyttökelpoisuus pitää varmistaa myös ulkoistetuissa palveluissa.

Kehittämiskohde – Haavoittuvuuksien hallinta ja auditointi
Haavoittuvuuksien hallinnan ja auditointitoiminnan kehittäminen. Yhä useampi tietomurto ja henkilötietojen tietoturvaloukkaus on syntynyt ICT-palveluista löytyneen ohjelmistollisen haavoittuvuuden takia. Tietoverkkorikolliset ja kybervakoilijat käyttävät entistä aggressiivisemmin ja nopeammin hyödykseen haavoittuvuuksia, etenkin ns. nollapäivähaavoittuvuuksia. Tietojärjestelmissä piilevien haavoittuvuuksien tunnistaminen edellyttää sekä haavoittuvuuksien hallinnan kehittämistä että säännöllisesti suoritettavia tietoturva-auditointeja tai -tarkastuksia kriittisimmissä järjestelmissä.

Kehittämiskohde – Käyttövaltuuksien säännöllinen tarkistus
Käyttövaltuuksien ajantasaisuuden varmistaminen tulee toteuttaa säännöllisesti. Tähän on hyvä olla suunniteltu, ohjeistettu ja koulutettu menettely. Näin varmistetaan, että käyttövaltuudet ovat mahdollisimman hyvin ajan tasalla eikä käyttövaltuuksien tarkistaminen kuormita henkilöstöä ja esihenkilöitä liikaa.

2.2.5 Tietosuoja

Taulukossa 6 esitetään tietosuojaosion 15 väittämän vastauskeskiarvot.

Taulukko 6. Tietosuoja – kysymyskohtaiset keskiarvot

Tietosuoja / Väittämä	Kaikki organisaatiot 203 kpl	Kunta 93 kpl	Kuntayhtymä 22 kpl	Hyvinvointialue ja muut Sotetoimijat 21 kpl	Korkeakoulu 14 kpl	Valtionhallinto 43 kpl	Muu 10 kpl

55. Organisaatiolla on tiedossa, mitä henkilötietoja se käsittelee (TsA 4 art. 1 kohta).	0,92	0,91	0,95	0,85	0,88	0,97	0,98
56. Henkilötietojen käsittelyn oikeusperusteet on tunnistettu (TsA 6, 9 ja 10 art. TsL 6 ja 29 §, TtsL 2, 3, 5 ja 6 luku).	0,93	0,9	0,98	0,93	0,96	0,95	1
57. Organisaatio on tunnistanut, milloin se toimii rekisterinpitäjänä ja milloin se toimii käsittelijänä (TsA 4 art. 7-8 kohta).	0,92	0,89	0,99	0,94	0,96	0,92	1
58. Sopimukset henkilötietojen käsittelystä on tehty ja sopimusten hallinta on kunnossa (TsA 28 art).	0,78	0,7	0,81	0,83	0,79	0,85	1
59. Yhteisrekisterinpitäjyystilanteet tunnistetaan ja yhteisrekisterinpitäjyyttä koskevista vastuista on sovittu (TsA 26 art., huom. myös EDPB:n ohje).	0,74	0,64	0,74	0,79	0,88	0,82	0,89
60. Henkilötietojen käsittelyyn liittyvät oman organisaation sisäiset roolit ja vastuut on tunnistettu ja vahvistettu (TihL 4.2. §, TsA 37 art.).	0,85	0,8	0,93	0,93	0,84	0,84	0,9
61. . Tietosuojavastaavan asema ja rooli on määritelty (TsA 37 – 39 art.).	0,94	0,92	0,99	0,95	0,95	0,97	0,95
62. Seloste käsittelytoimista on laadittu (TsA 30 art.).	0,81	0,75	0,84	0,81	0,86	0,88	0,9
63. Organisaatiolla on tiedossa missä tietojärjestelmissä henkilötietoja käsitellään.	0,89	0,88	0,95	0,83	0,88	0,9	0,95
64. Rakenteeton tieto on tunnistettu ja sen hallinta on kuvattu.	0,47	0,45	0,52	0,5	0,39	0,49	0,63
65. Informointikäytännöt on määritelty ja niitä noudatetaan (TsA 12-14 art. Laki	0,78	0,7	0,81	0,85	0,84	0,85	0,86

digitaalisten palveluiden tarjoamisesta (306/2019).							
66. Organisaatiolla on olemassa prosessi vaikutustenarvioinnin tarpeen tunnistamiseksi (TsA 35 (1) art.).	0,71	0,63	0,64	0,9	0,86	0,74	0,86
67. Organisaatiolla on olemassa henkilötietojen tietoturvaloukkausten hallintaprosessi (TsA 33-34 art.).	0,92	0,89	0,89	0,96	0,96	0,96	0,95
68. Jos henkilötietoja siirretään kolmansiin maihin, organisaatio on selvittänyt siirron edellytykset (TsA 5 luku).	0,77	0,72	0,78	0,75	0,77	0,85	0,86
69. Organisaatiossa tietosuojasta huolehtiminen on muuttunut toiminnaksi, kulttuuriksi ja asenteeksi (TSA 5 art.).	0,69	0,63	0,75	0,6	0,64	0,78	0,83

Lähes jokainen organisaatio tuntee käsittelemänsä henkilötietotyypit ja on tunnistanut niiden käsittelyn oikeusperusteet. Näiden väittämäkohtaiset keskiarvot ovat 0,92 ja 0,93. Suurin haaste on rakenteettoman tiedon tunnistamisessa ja hallinnassa (0,47).

Tietosuoja-osion kokonaiskeskiarvo (0,81) on koko kyselyn korkein ja toimialojen väliset erot ovat varsin pienet. Korkein keskiarvo on ryhmässä Muut (0,90) ja pienin kunnissa (0,76).

Kehitys vuoteen 2023 verrattuna

Tämän osa-alueen keskiarvo on hiukan hieman parantunut kahden vuoden takaisesta 0,78 → 0,81. Pientä pudotusta on tapahtunut kaikilla toimialoilla.

Kehitystä parempaan on mm. väittämässä sopimuksista ja niiden hallinnasta henkilötietojen käsittelijän kanssa 0,74 → 0,78, yhteisrekisterinpitäjyyttä koskevassa väittämässä 0,68 → 0,74.

Eniten parannusta on tapahtunut väittämässä henkilötietojen siirrossa kolmansiin maihin 0,69 → 0,77. Tämä on todennäköisesti seurausta Euroopan ja Yhdysvaltojen välisen Data Privacy Frameworkin hyväksynnästä EU:ssa 2023.

Lisäksi hyvää kehitystä on tapahtunut myös väittämässä prosessista tietosuojan vaikutustenarvioinnin tarpeen tunnistamiseksi 0,64 →0,71.

Käytännössä tietosuoja-osiossa ovat myös kaikki muut väittämät kehittynyt parempaan. Tietosuoja-osion keskiarvo on kuitenkin ollut EU:n yleisen tietosuoja-asetuksen ansiosta korkealla tasolla jo pitkään, joten isoja keskiarvoparannuksia ei voi tapahtua.

Tietosuojan kehittämiskohteet

Kehittämiskohde -DPIA ja TIA
Tietosuojan vaikutustenarviointi sekä tietojen siirrot kolmansiin maihin. Vaikka tilanne on kehittynyt selkeästi parempaan suuntaan, organisaatioiden tulee tunnistaa korkean riskin henkilötietojen käsittelytapausten lisäksi tilanteet joissa tapahtuu tai voi tapahtua henkilötietojen siirtoa kolmansiin maihin. Maailmanpoliittinen tilanne voi aiheuttaa merkittäviä uhkia tilanteissa, joissa rekisterinpitäjä on tavalla tai toisella riippuvainen toimijoista, jotka ovat kolmansista maista. Organisaatioiden tulee varautua mahdollisiin muutoksiin globaalissa mittakaavassa ja olla valmis reagoimaan, mikäli henkilötietojen siirto kolmansiin maihin täytyy pysäyttää nopeutetulla aikataululla.

Kehittämiskohde – Kokonaisvaltainen tietosuoja ja rakenteeton henkilötieto
Tietosuojan kokonaisvaltainen tarkastelu. Organisaatioiden tulee tunnistaa käsittelemänsä henkilötiedot sekä niiden käsittelyperusteet. On tärkeää laatia linjaukset siitä, missä järjestelmissä tai palveluissa (esim. pilvipalvelut) henkilötietoja käsitellään. Jos käsittelyssä havaitaan puutteita, organisaatioiden tulee kartoittaa kehittämistarpeet ja laatia kehittämissuunnitelma.

Erityistä huomiota tulee kiinnittää rakenteettoman henkilötiedon hallintaan. Rakenteetonta henkilötietoa voi löytyä esim. sähköposteista, verkkolevyiltä, henkilöstön kotihakemistoista, puhelu- tai videotallenteet, chat-historiat, kuvagalleriat jne.

2.2.6 Kyberturvallisuus

Kyberturvallisuus-osion 10 väittämän vastauskeskiarvot ovat taulukossa 7.

Taulukko 7. Kyberturvallisuus – kysymyskohtaiset keskiarvot

Kyberturvallisuus / Väittämä	Kaikki organisaatiot n. 200 kpl	Kunta 93 kpl	Kuntayhtymä 22 kpl	Hyvinvointialue ja muut Sotetoimijat 21 kpl	Korkeakoulu 14 kpl	Valtionhallinto 43 kpl	Muu 10 kpl
70. Organisaatio on huomioinut digitaalisen turvallisuuden osana kokonaisarkkitehtuuria.	0,71	0,69	0,74	0,63	0,7	0,72	0,98
71. Organisaatiolla on riittävät resurssit ja osaaminen digitaalisen turvallisuuden kehittämiseen osana kokonaisarkkitehtuuria.	0,55	0,42	0,73	0,54	0,61	0,62	0,83

73. Organisaatio on tunnistanut oman roolinsa YTS:n mukaisissa tehtävissä sekä kansallisesta että kansainvälisestä näkökulmasta.	0,7	0,59	0,66	0,9	0,59	0,87	0,75
74. Organisaatiossa on tunnistettu ne kriittiset palvelut, joilla on merkittävä vaikutus toisten organisaatioiden tai yhteiskunnan toimintaan.	0,81	0,73	0,81	0,93	0,85	0,89	0,89
75. Organisaatiossa on kattavasti tunnistettu kriittisten palveluiden riippuvuudet ulkoisista palvelutoimittajista.	0,77	0,73	0,86	0,79	0,71	0,81	0,9
76. Organisaation kriittisten palveluiden palveluntuottajien kanssa yhteistyössä arvioidaan ja hallitaan riskejä säännöllisesti.	0,54	0,5	0,58	0,54	0,45	0,63	0,7
77. Kriittisten toimittajien ja alihankkijoiden kanssa käsitellään digiturvallisuutta säännöllisesti toimittaja/palvelunhallintakokouksissa.	0,59	0,55	0,65	0,7	0,36	0,68	0,7
78. Organisaatio on varautunut ja laatinut suunnitelman siihen kohdistuvan mustamaalaus- tai vaikuttamiskampanjan varalta.	0,47	0,36	0,36	0,56	0,5	0,63	0,53
79. Organisaatio seuraa säännöllisesti toimintaympäristönsä digitaalisen turvallisuuden tilannekuvaa.	0,73	0,63	0,76	0,83	0,68	0,82	0,85

80. Organisaatiolla on toiminnalliset ja tekniset menettelyt tietojenkäsittely-ympäristönsä digitaalisen turvallisuuden valvontaan ja havainnointiin.	0,65	0,6	0,73	0,78	0,66	0,68	0,8

Korkein kysymyskohtainen keskiarvo koskee organisaatioiden valmiuksia tunnistaa sellaiset kriittiset palvelut, jotka vaikuttavat myös muiden tahojen toimintaan (0,81). Heikoin tulos on puolestaan organisaatioihin kohdistuviin mustamaalauskampanjoihin varautumisessa (0,47).

Osion kokonaiskeskiarvo (0,65) on koko kyselyn alhaisin. Toimialoista korkein keskiarvo on ryhmässä Muut (0,79) ja heikoin kunnissa (0,58). Osion kehitys on kuitenkin muihin osioihin verrattuna paras vuoden 2024 aikana.

Kehitys vuoteen 2023 verrattuna

Tällä osa-alueella keskiarvo on noussut kahden vuoden takaisesta, jolloin se oli 0,61. Toimialoista parannusta on tapahtunut eniten hyvinvointialueilla, mutta myös korkeakouluissa kehitys on ollut merkittävä. Alla organisaatiotyypeittäin muutokset:

Kunnat 0,57 → 0,58

kuntayhtymät 0,68 → 0,69

Hyvinvointialueet ja muut sote-toimijat 0,56 → 0,72

Korkeakoulut 0,49 → 0,61

Valtiohallinto 0,70 → 0,74

Muu 0,72 → 0,79

Väittämä, jonka keskiarvossa on tapahtunut eniten parannusta, on *”Organisaatio seuraa säännöllisesti toimintaympäristönsä digitaalisen turvallisuuden tilannekuvaa*” (0,53 → 0,73). Osiossa on myös yksi uusi kysymys: *Organisaatiolla on toiminnalliset ja tekniset menettelyt tietojenkäsittely-ympäristönsä digitaalisen turvallisuuden valvontaan ja havainnointiin* (keskiarvo 0,65)

Kyberturvallisuuden kehittämiskohteet

Kehittämiskohde – Digiturvan arkkitehtuuri
Digi- ja väestötietovirasto on kehittänyt digitaalisen turvallisuuden arkkitehtuuria. Suosittelemme tutustumaan ja hyödyntämään arkkitehtuuria Digitaalisen turvallisuuden arkkitehtuuri - Digi- ja väestötietovirasto - Suomi.fi kehittäjille

Kehittämiskohde – Digiturvan tietopankki ja palveluhakemisto
Digi- ja väestötietovirasto on kehittänyt Digiturvan tietopankin ja digiturvan palveluhakemiston. Suosittelemme tutustumaan molempiin. Sekä tietopankin että palveluhakemiston sisällöt

päivittyvät kokoajan, joten sivustoja kannattaa seurata määräajoin. Digiturvan tietopankin löydät täältä: Kyberturvallisuuden ja digitaalisen turvallisuuden tietopankki - Suomi.fi kehittäjille

Digiturvan palveluhakemiston löydät täältä: Digiturvan palveluhakemisto - Suomi.fi kehittäjille

Kehittämiskohde – Sidosryhmä- ja verkostoyhteistyö
Digitaalisen turvallisuuden kehittäminen yhteistyössä palvelutuottajien kanssa. Organisaation tulisi kehittää digiturvallisuuden eri osa-alueita yhteistyössä palvelutuottajiensa kanssa joko aloittamalla palvelutoimittajatapaamiset tai lisäämällä digiturvallisuusteemat nykyisten tapaamisten agendalle.

Lisäksi suosittelemme verkostoitumaan ja tekemään yhteistyötä muiden organisaatioiden kanssa. Verkostoja tarjoaa esim. Digi- ja väestötietovirasto: VAHTI-verkosto VAHTI-verkosto - Digi- ja väestötietovirasto - Suomi.fi kehittäjille

Lisäksi verkostoja tarjoaa esim. Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus Traficomin Kyberturvallisuuskeskus | Kyberturvallisuuskeskus

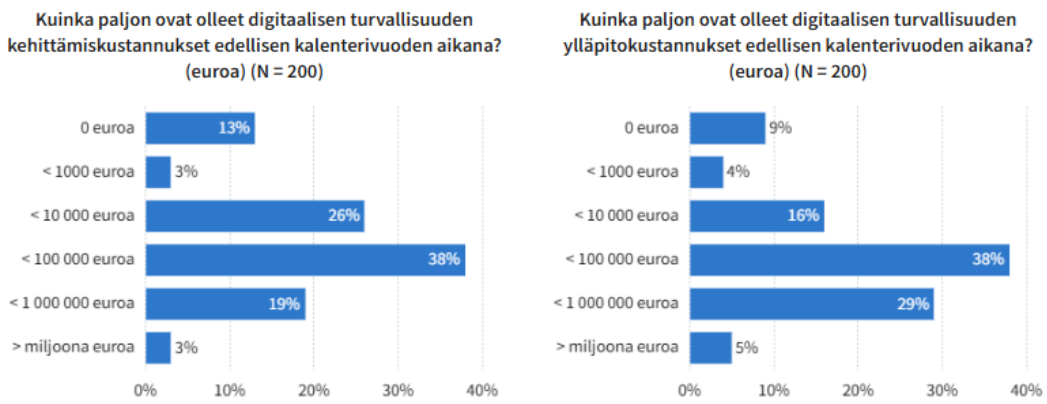
Myös kunnilla ja hyvinvointialueilla on omia verkostoja.

Kehittämiskohde – Toimintaympäristön muutokset huomioiva riskienhallinta
Uhkatilanteen seuranta ja siihen liittyvien riskien hallinta. Organisaatioiden toimintaympäristö on kaikilta osin muuttumassa nopeammin kuin koskaan aikaisemmin, ja lisäksi vauhti tuntuu kiihtyvän jatkuvasti. Tämä tarjoaa uudenlaisia teknologisia mahdollisuuksia kehittää organisaation toimintaa, mutta myös organisaatioon kohdistuvat uhat ovat merkittävässä muutoksessa. Jotta organisaatio voi hyödyntää mahdollisuuksia, tunnistaa uhat ja hallita niihin liittyvät riskit, sen tulee kyetä seuraamaan ja arvioimaan toimintaympäristönsä muutoksien vaikutuksia säännöllisesti. Tämän kyvykkyyden kehitystä voidaan työstää kokonaisuutena, jossa linkittyvät niin johtamisen tarpeet, kyberturvallisuus, kuin myös riskienhallinnan seurantatarpeet.

Kehittämiskohde – Mis- ja disinformaatioon varautuminen
Varautuminen informaatiovaikuttamiseen. Vaikuttamisyritykset organisaation julkikuvaan ja maineeseen ovat lisääntyneet erityisesti maailmanpoliittisen tilanteen muutoksen ja sosiaalisen median kanavien. tekoälypalveluiden yms. lisääntyessä. Jokaisen organisaation tulisi varautua kielteiseen informaatiovaikuttamiseen ja laatia toimintasuunnitelmat niiden varalle.

2.2.7 Rahalliset ja ajalliset panostukset

Kuva 3 digitaalisen turvallisuuden kehittämis- ja ylläpitokustannukset



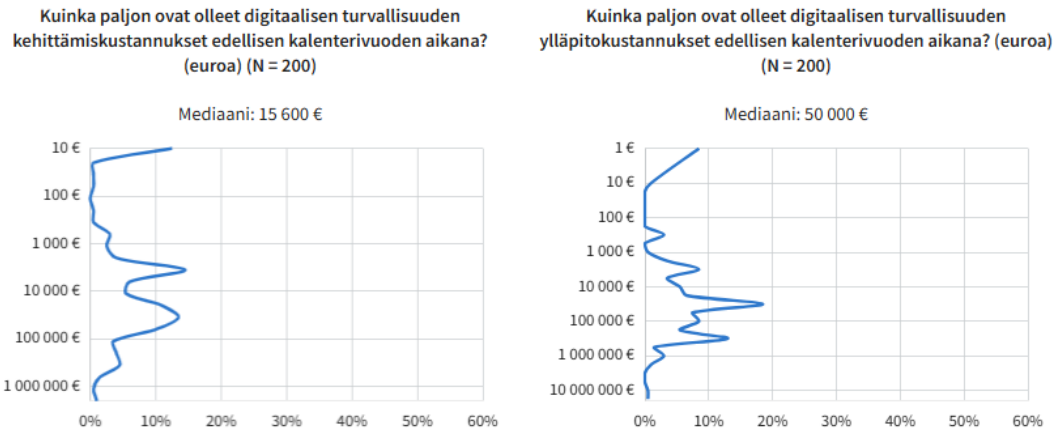
Suurin osa vastaajista (38 %) ilmoitti digitaalisen turvallisuuden kehittämiskustannuksiksi alle 100 000 €. Viidennes vastaajista käytti kehittämiseen yli 100 000 €. Tästä voidaan päätellä, että merkittävä osa vastaajista kohtuullisesti digitaalisen turvallisuuden kehittämiseen. Tästä huolimatta johtamisen osa-alueen vastausten perusteella moni organisaatio kokee digiturvaan käytetyt resurssit riittämättömiksi.

13 % vastaajista ilmoitti käyttävänsä 0 euroa digitaalisen turvallisuuden kehittämiseen. Tämä on huolestuttava tulos. Tulos viitannee resurssipulaan, mutta samalla tulos voi viitata tietoisuuden puutteeseen tai digitaalisen turvallisuuden aliarviointiin.

Ylläpitokustannuksista yleisin taso asettuu kehittämiskustannusten tavoin luokkaan alle 100 000 € (38 %). Yli 100 000 € ylläpitoon käyttäviä organisaatioita on kuitenkin 10 prosenttiyksikköä enemmän kuin samassa kategoriassa olevia kehittämiskustannusten osalta. Lisäksi ylläpitoon yli miljoona euroa käyttäviä on hieman enemmän kuin kehittämisen puolella. Ylläpitokustannukset ovat siten hieman korkeammat kuin kehittämiseen käytetyt rahalliset resurssit. Tämä tukee kokonaiskuvapalvelun muita tuloksia, eli Suomessa julkisen hallinnon kyber- ja digitaaliseen turvallisuuteen on panostettu jo vuosia pitkäjänteisesti ja on siksi kohtalaisen hyvällä tasolla. Vaikka kehitettävääkin vielä on.

Vastaajista 9 % sanoo käyttävänsä digiturvan ylläpitoon 0 €. Tämä viitannee siihen, että jotkut organisaatiot eivät ole tietoisia digiturvatarpeistaan ja ylläpitoon liittyvistä kustannuksista. Tai digiturvaan käytettäviä kustannuksia ei ole tunnistettu osaksi digiturvakustannuksia.

Tuloksista voidaan päätellä, että monissa organisaatioissa digiturvan kehittäminen jää vähälle, vaikka uhkaympäristö muuttuu ja kehittyy koko ajan. Lisäksi sääntely lisääntyy koko ajan. Molempien ilmiöiden pitäisi johtaa jatkuvaan suunnitelmalliseen kehittämiseen. Koska ylläpitoon käytetään merkittävästi enemmän rahallisia resursseja kuin kehittämiseen, voi tämä johtaa kehittämisen ja ylläpidon väliseen epätasapainoon. Epätasapaino voi johtaa kyber- ja digiturvan hallinnolliseen ja teknologiseen jälkeenjääneisyyteen, sillä kyber- ja digitaalinen turvallisuusympäristö muuttuu jatkuvasti.

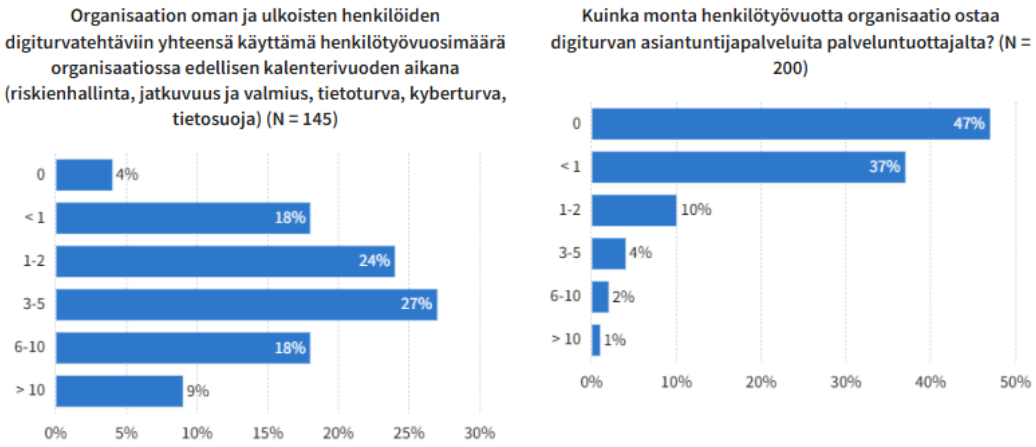


Kuva 4 rahalliset panostukset ja mediaani

Yllä olevassa kuvassa edellä kuvatut kehittämiseen ja ylläpitoon liittyvät kustannukset on kuvattu toisenlaisella kuvaajalla. Organisaatioiden vastausten mediaani kehittämiskustannuksissa on 15 600€ ja ylläpitokustannusten mediaani on 50 000€.

2.2.8 Henkilöresurssit

Kuva 5 organisaatioiden omat ja ostetut henkilöresurssit

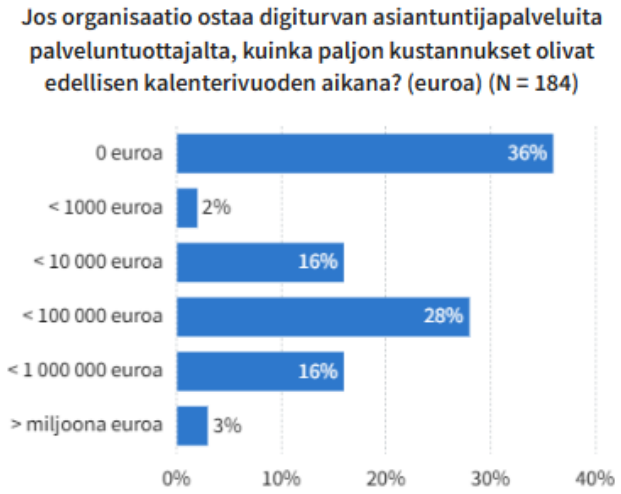


73 % organisaatioista käyttää kaikkiin digiturvan osa-alueiden tehtäviin alle kuusi henkilötyövuotta. Tämä voi rajoittaa kykyä ennakoida ja hallita digiturvaan liittyviä riskejä. Vain 9 % käyttää yli 10 htv digiturvatehtäviin mikä osoittaa, että vahvasti resursoituja organisaatiota on vähän. Keskikokoisia panostuksia (3–5 htv) ovat yleisimpiä, mikä viittaa kohtalaiseen kyvykkyyteen ylläpitää ja kehittää digitaalista turvallisuutta omassa toimintaympäristössä.

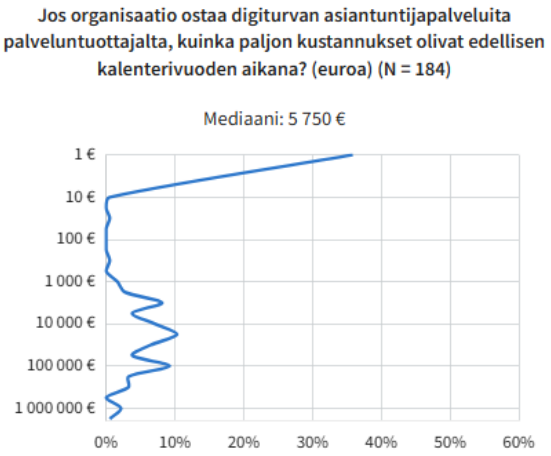
Lähes puolet organisaatioista ei hanki digiturvaosaamista organisaation ulkopuolelta ja 37 % vastaajista ostaa alle yhden henkilötyövuoden. Harva organisaatio siis tukeutuu ostopalveluihin digitaalisen turvallisuuden ylläpidossa ja kehittämisessä. Painotus on siis vahvasti omassa tekemisessä.

Kokonaiskuvapalvelun johtamisen osa-alueen tulosten pohjalta moni organisaatio kokee, ettei sillä ole riittävästi osaavaa henkilöstöä digiturvaan. Oman henkilöstön riittävyyden varmistaminen ja sopivassa suhteessa tehty ostopalveluiden hankinta tukee organisaation osaamisen kehittymistä ja varmistaa organisaation resilienssin kehittymisen suhteessa kyber- ja digiturvan uhkaympäristön kehittymiseen.

Kuva 6 digiturvan ostopalveluiden kustannukset



Vaikka digiturvaan liittyvät ostopalvelut ovat suhteellisen matalalla tasolla, käytetään ostopalveluihin kuitenkin merkittäviä rahallisia panostuksia, mikä käy edellä olevasta kuvasta. 36 % vastaajista käyttää ostopalveluihin 0 euroa. Seuraavaksi suurin ryhmä ovat organisaatiot, jotka käyttävät ostopalveluihin yli 10 000 € mutta alle 100 000 €. Yli 100 000 € ostopalveluihin käyttäviä organisaatioita on 16 %. Muutama organisaatio käyttää ostopalveluihin yli miljoona euroa.



Kuva 7 digiturvan ostopalveluihin käytetyt kustannukset ja mediaani

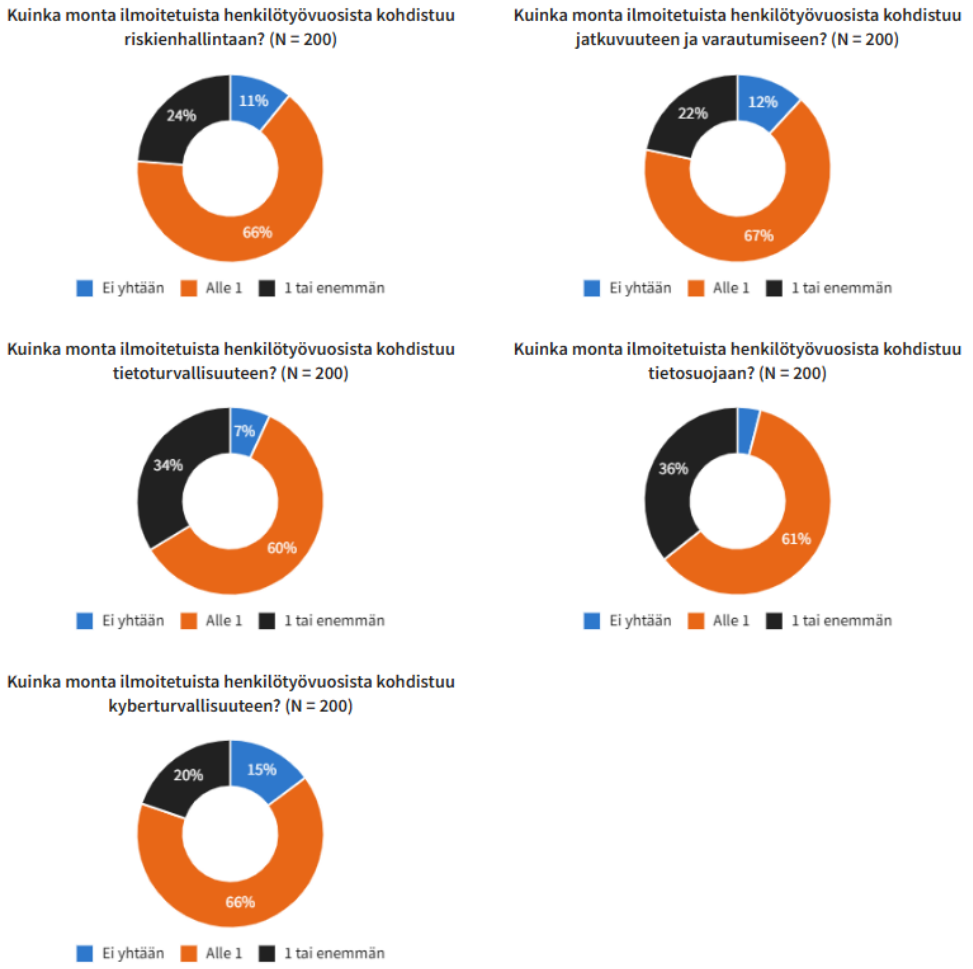
Yläpuolella oleva kuva kertoo digiturvan ostopalveluihin liittyvien kustannusten jakautumista organisaatioiden vastausten perusteella. Mediaani ostopalveluiden osalta on 5750€.

Alla olevassa kuvassa näytetään organisaatioiden käyttämät henkilötyövuodet digiturvan osa-aluekohtaisesti. Valtaosa vastaajista käyttää alle 1 htv resursseja osa-alueittain. Tietoturva ja tietosuoja ovat vahvimmin resursoitu. Tämä voi olla seurausta siitä, että ne ovat olleet vahvasti reguloituja pitempään.

Kyberturvan osa-alue on heikoiten resursoitu, mikä on havaittavissa myös osa-alueen tuloksissa sitä koskevissa väittämissä. Riskienhallinta ja jatkuvuus ja varautuminen ovat myös yllättävän heikosti resursoitu, vaikka ne ovat perustavanlaatuisia resiliensin osalta. Kyber- ja digiturvauhat lisääntyvät koko ajan, joten kyberturvallisuuden osa-alueen, riskienhallinnan ja jatkuvuuden ja varautumisen resursointia tulisi kehittää pitkäjänteisesti.

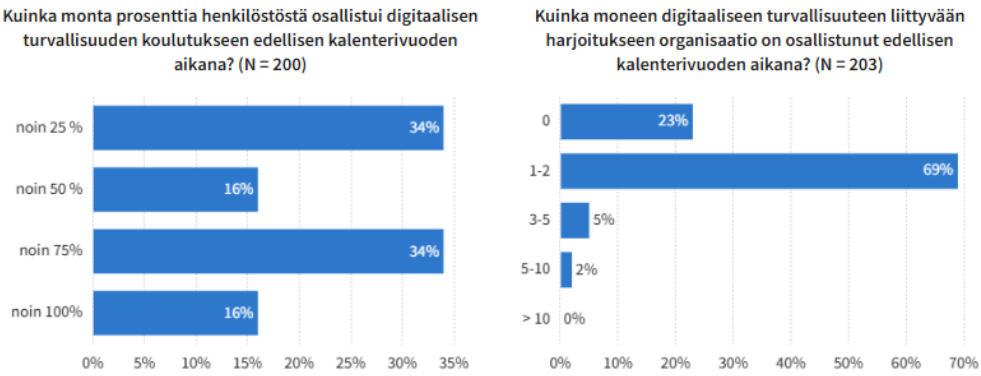
Kokonaisuutena henkilötyövuosien osalta on havaittavissa, että digiturvaresurssit ovat edelleen monessa organisaatiossa kriittisen matalia.

Kuva 8 digiturvan eri osa-alueisiin käytetyt henkilöresurssit



2.2.9 Osaamisen kehittäminen

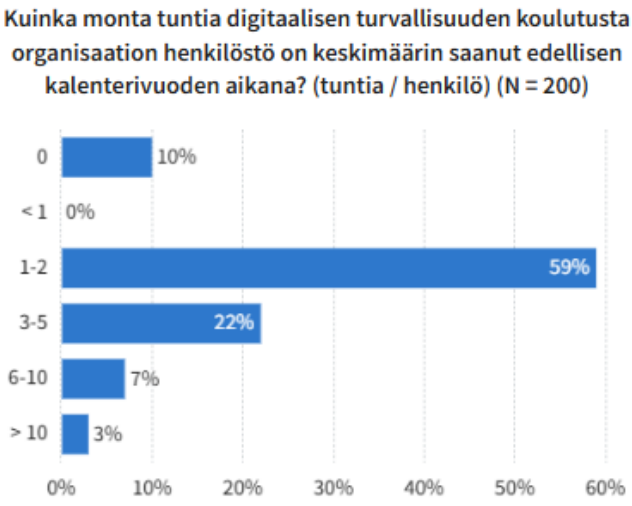
Kuva 9 Organisaatioiden digiturvakoulutukset ja harjoittelu



Vastausten perusteella organisaatiot jakautuvat kahteen kategoriaan. Niihin organisaatioihin, jotka kouluttavat n. 25 % henkilöstöstä ja niihin, jotka kouluttavat n. 75 % henkilöstöstä. Vain 16 % vastaajista kouluttaa koko henkilöstön.

Lähes 70 % vastaajista osallistuu 1–2 harjoitukseen vuodessa. 23 % ei harjoittele lainkaan. Tehokas ja kattava harjoittelukulttuuri on vain 7 % organisaatioista. Nämä vastaajat harjoittelevat 3–10 kertaa vuodessa.

Kuva 10digiturvakoulutusten tuntimäärät



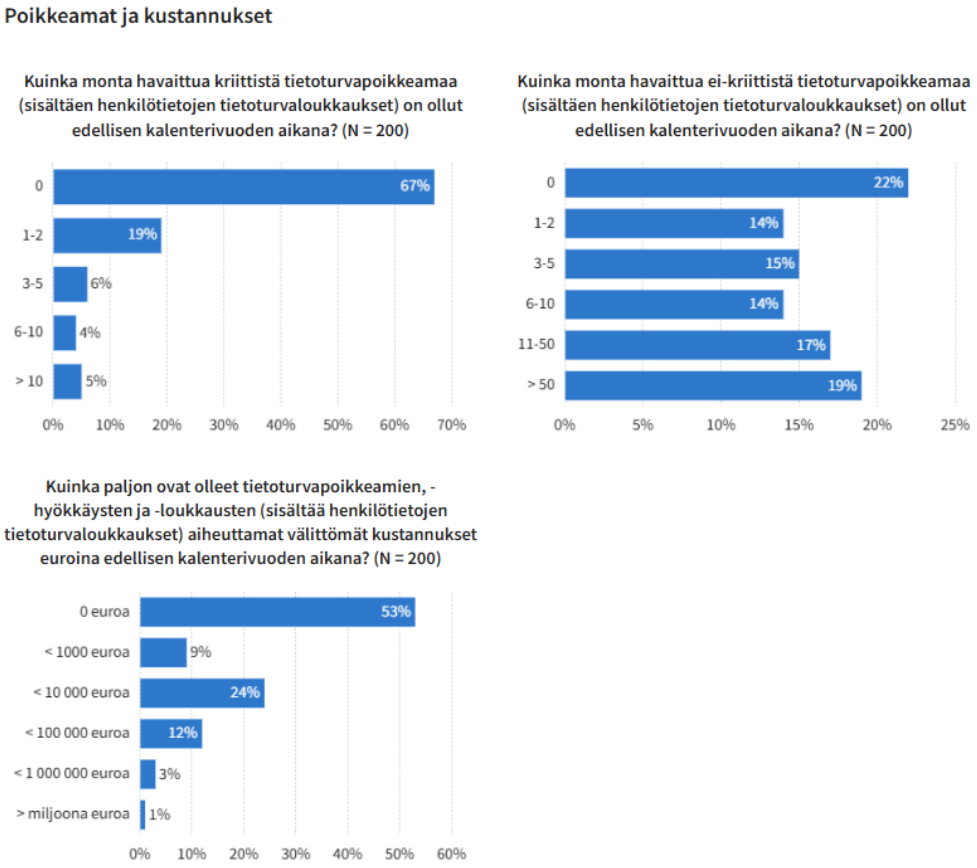
Edellä oleva kuva digiturvakoulutusten tuntimäärästä havainnollistaa sitä, että koulutusta annetaan suhteellisen vähän suurimmassa osassa organisaatioita. Kun huomioi kaikki digiturvan osa-alueet, toimintaympäristöt, kyber- ja digiturvan uhkakuvien kehityksen sekä regulaation kehittyminen, tuntuu 1–2 tuntia koulutusta vuodessa hyvin alhaiselta määrältä. Varsinkin kun pääsääntöisesti vain 25–75 % henkilöstöstä saa ko. koulutusta.

Puutteellinen koulutus johtaa osaamisen kehittymisen jälkeen jäämiseen, josta seuraa havaintokyvyn ja resilienssin heikentyminen. Koulutukseen panostaminen on suhteellisen kustannustehokas tapa ylläpitää ja kehittää organisaation kyber- ja digiturvakulttuuria sekä varmistaa organisaation havaintokyky poikkeamille sekä asianmukainen, oikea-aikainen ja tehokas toiminta poikkeama- ja häiriötilanteissa. Pelkkä kouluttaminen ei kuitenkaan riitä, vaan osaaminen kehittyy aktiivisella harjoittelulla, johon osallistutaan kaikilta organisaation tasoilta. Harjoittelu on paras ja tehokkain tapa varmistaa, että organisaatiokulttuuri kehittyy ja häiriö sekä poikkeamatilanteissa osataan toimia oikein ja tehokkaasti. Näin myös kyetään hillitsemään häiriöiden ja poikkeamien todennäköisyyttä sekä niiden vaikutuksia.

2.2.10 Poikkeamat ja kustannukset

Alla olevassa kuvassa esitellään vastaajaorganisaatioiden näkemyksiä kriittisistä ja ei kriittisistä tietoturvapoikkeamista, jotka sisältävät myös henkilötietoihin kohdistuneet tietoturvaloukkaukset. Lisäksi kuvassa esitetään tietoturvapoikkeamien aiheuttamat välittömät kustannukset.

Kuva 11 kriittisten ja ei-kriittiset tietoturvapoikkeamat ja niiden kustannukset



Vähintään joka kolmas vastaajaorganisaatio on kokenut vähintään yhden kriittisten poikkeaman, mikä on merkittävä määrä. Kuitenkin 67 % organisaatioista ei ole kokenut yhtään kriittistä poikkeamaa. Koska kriittiset poikkeamat hyvin todennäköisesti havaitaan, on tämä tulos todennäköisesti luotettava.

22 % organisaatioista ei ole havainnut yhtään ei-kriittistä poikkeamaa. Tämä voi viitata puutteelliseen monitorointiin ja havaintokykyyn. 19 % vastaajista on tunnistanut yli 50 ei-kriittistä poikkeamaa. Tämä viittaa siihen, että viidenneksellä vastaajista on kehittynyt havaintokyky.

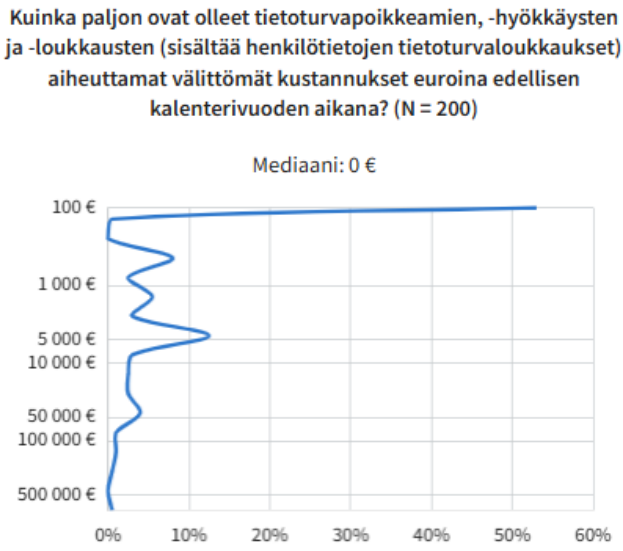
Suurin osa organisaatioista, 78 % on havainnut vähintään yhden ei-kriittisen poikkeaman vuoden aikana. Tämä viittaa siihen, että kyber- ja digiturvan hallinta sekä kehittäminen edellyttää pitkäjänteistä ja suunnitelmallista työtä.

Poikkeamien kustannukset eivät jakaudu tasaisesti. Yli puolet vastaajista ei ole tunnistanut suoria kuluja tietoturvapoikkeamista. Toisaalta osalle vastaajista aiheutuu merkittäviä kustannuksia poikkeamista. Yli miljoonan euron menetykset ovat harvinaisia, mutta niiden olemassaolo muistuttaa kyber- ja digiturvariskien realisoitumisen vakavuudesta.

Kun tarkastelee vastaajaorganisaatioiden henkilöresursseja, kehittämis- ja ylläpitokustannuksia, koulutusmääriä, harjoittelua ja havaittuja poikkeamia ja niiden

kustannuksia, vaikuttaa siltä että havaitsemis- ja kustannusraportointikyvykkyys vaihtelee merkittävästi. Tällä on suora vaikutus organisaatioiden riskienhallinnan tehokkuuteen. Tilanteen parantaminen edellyttää mittaristojen ja prosessien kehittämistä, valvonnan kehittämistä, kouluttamisen ja harjoittelun lisäämistä sekä tehokkaampaa kustannusten seurantaa digiturvan ylläpidon ja kehittämisen sekä kriittisten ja ei-kriittisten kustannusten osalta. Lisäksi on hyvä huomioida, että tietoturvapoikkeamista voi seurata myös epäsuoria kustannuksia, jotka voivat olla merkittäviä.

Alla olevassa kuvassa kustannusten jakautuminen vastaajaorganisaatioiden kesken kuvataan toisella tavalla. Mediaani kustannusten osalta on 0€, mikä on seurausta siitä ettei yli puolet vastaajista ole tunnistanut kustannuksia laisinkaan. Toisaalta vastaajien joukossa on organisaatiota, jotka ovat tunnistaneet huomattavasti suurempia kustannuksia tietoturvapoikkeamista.



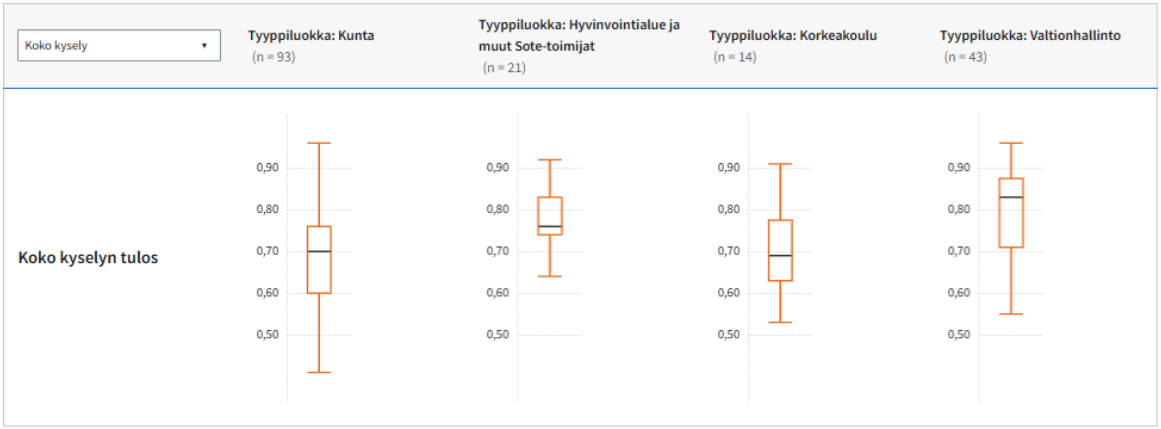
Kuva 12 Tietoturvapoikkeamien aiheuttamat välittömät kustannukset

3 Organisaatiotyyppien vertailu

Tässä osiossa vertaillaan neljän keskeisen vastaajaorganisaatiotyypin vastauksia keskenään. Organisaatiotyypit ovat kunnat, hyvinvointialueet, korkeakoulut ja valtiohallinto.

Alla olevassa kuvaajassa janan yläpään ja alapään viikset kuvaavat kyseisen vastaajaryhmän suurinta ja pienintä arvoa ja siten myös vastausten keskiarvojen hajontaa. Janan keskellä oleva suorakaide kuvaa kvartaaliväliä, johon asettuu 50 % keskimmäisistä vastauskeskiarvoista. Laatikon yläpuolella on siis yläkvartaali, 75 % vastauksista on näitä tuloksia pienempi. Laatikon alapuolella on alakvartaali, laatikon alareunan alapuolella on 75 % on tätä keskiarvoa parempia. Musta viiva kuvaa vastausten mediaania.

Kuvaaja koko kyselyn tulos digitaalinen turvallisuus

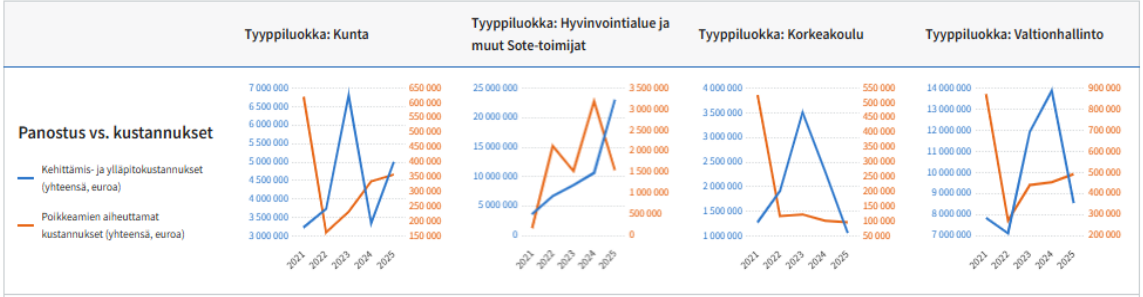


Kuntien vastauksissa on eniten hajontaa, mutta samalla kaikkein parhaimmat keskiarvot löytyvät ryhmistä kunnat ja ryhmästä valtiohallinto. Muilla organisaatiotyypeillä vastausten keskiarvojen hajonta on pienempää kuin kunnissa. Erityisen tasainen hajonta on hyvinvointialueilla mikä tarkoittaa, että digiturvan taso on hyvinvointialueilla suhteellisen yhdenmukainen koko maassa.

Korkein mediaani on valtiohallinnossa ja matalin korkeakouluissa. Kvartaalivälit jokaisessa organisaatiotyyppiluokassa osoittaa, että koko julkisessa hallinnossa digitaalinen turvallisuus on suhteellisen hyvällä tasolla, vaikka kehitettävääkin on erityisesti kunnossa ja korkeakouluilla.

Panostukset vs. kustannukset

Kuvaaja. Digiturvaan kohdistetut kehittämis- ja ylläpitoresurssit suhteessa tietoturvapoikkeamien aiheuttamat kustannukset



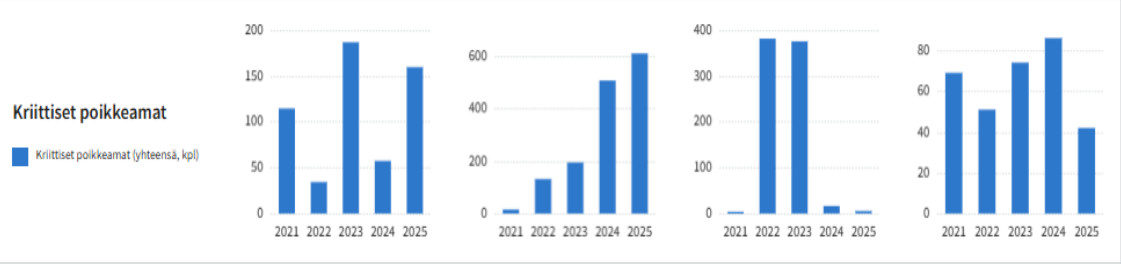
Yleisenä trendinä on nähtävissä, että niin panostukset digiturvaan kuin kuin tietoturvapoikkeamien aiheuttamat kustannukset ovat nousussa. Digitaalinen turvallisuus edellyttää jatkuvaa ja ennakoivaa resurssointia. Ennaltaehkäisevällä investoinnilla digiturvaan voidaan säästää kustannuksista pitkällä aikavälillä.

Kunnissa ja korkeakouluissa digiturvan kehittämiseen ja ylläpitoon käytetään merkittävästi vähemmän resursseja kuin valtiohallinnossa ja hyvinvointialueilla. Poikkeamien aiheuttamat kustannukset korostuvat hyvinvointialueilla.

Kuvaajassa on nähtävissä reaktiivinen kehitysmalli. Digiturvaan liittyviä panostuksia kasvatetaan vasta poikkeamien aiheuttamien kustannusten kasvun jälkeen. Investointien kasvu ei kuitenkaan pysty nopeasti hillitsemään poikkeamista aiheutuvia vahinkoja.

Kriittiset poikkeamat

Kuvaaja. Kriittiset poikkeamat yhteensä, kunnat, HVA:t, Korkeakoulut, Valtiohallinto



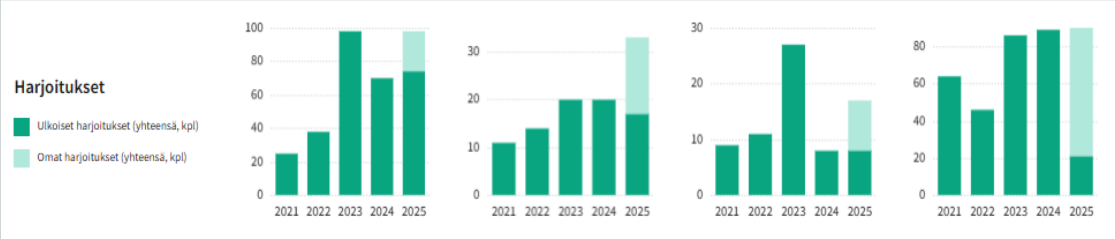
Kriittisten poikkeamien kehitys on ollut vaihtelevaa. Ilmoitettujen tilastojen valossa kunnissa havaittuja kriittisiä poikkeamia on havaittu jälleen enemmän rauhallisemman vuoden jälkeen. Hyvinvointialueilla havainnot ovat kasvaneet vuosittain. Korkeakouluissa havaittuja kriittisiä poikkeamia ei on ollut viime vuosian vähemmän. Valtiohallinnossa kriittisiä poikkeamia on yhteen laskettuna vähän. Tilastossa on kuitenkin hyvä huomioida, että yhteenlasketut havainnot koostuvat eri kokoisista ilmoittajajoukoista. Hyvinvointialueita vastaajissa oli 21, jotka havaitsivat vuoden 2024 aikana yli 600 kriittistä poikkeamaa. 93 kuntaa havaitsi yli 150 kriittistä poikkeamaa vuonna 2024. 14 korkeakoulua havaitsi muutamia kriittisiä poikkeamia. 43 valtionhallinnon toimijaa havaitsi hieman yli 40 kriittistä poikkeamaa.

Hyvinvointialueiden korkeaa poikkeamamäärää selittänee se, että iso osa hyvinvointialueilla havaituista poikkeamista ovat kriittisiä. Hyvinvointialueilla on lisäksi korkea kyvykkyys havaita poikkeamia ja ilmoittaa niistä suunniteltua prosessia noudattaen, jolloin poikkeamat kyetään tilastoimaan asianmukaisesti. Lisäksi hyvinvointialueilla poikkeamien hallinta voi olla monimutkaista, koska toimintaympäristö on hyvin monimutkainen. Poikkeama voi pahimmillaan johtaa myös palvelutarjonnan häiriöihin, joka on

Yleisesti on havaittavissa, että havaittujen kriittisten poikkeamien trendi on kasvava ja tämä edellyttää ennakoivaa ja suunnitelmallista digiturvan kehittämistä. Kehittämisen tulee perustua tunnistettuun riskiympäristöön. Organisaation johdon tulee seurata kriittisten poikkeamien kehitystä sekä ohjata organisaation resursseja riskienhallinnan perusteella.

Harjoitukset

Kuvaaja. Harjoitustoiminta, ulkoiset harjoitukset ja omat harjoitukset yhteensä. Kunnat, HVA:t, Korkeakoulut, Valtiohallinto



Harjoittelutoiminta Suomalaisessa julkisessa hallinnossa on korkealla tasolla, mutta kehitettävää edelleen on. Vastaajamäärät huomioiden kunnat ja korkeakoulut osallistuvat keskimäärin 1 harjoitukseen vuosittain, hyvinvointialueet 1,5 harjoitukseen vuosittain ja valtiohallinnon organisaatiot kahteen harjoitukseen vuosittain.

Valtiohallinnossa korostuu organisaatioiden omat harjoitukset. Myös hyvinvointialueilla ja korkeakouluissa harjoitellaan omatoimisesti suhteessa enemmän kuin kunnissa.

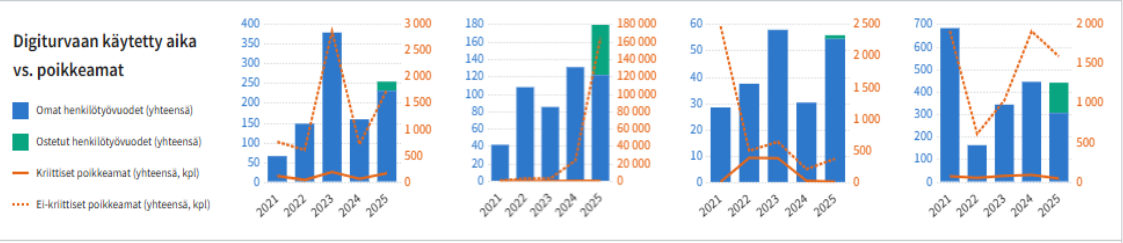
Hyvä kehityskohde harjoittelun osalta on mm. TAISTO-harjoitus, jonka digi- ja väestötietovirasto järjestää vuosittain marraskuussa. TAISTO on helppo ja kustannustehokas tapa harjoitella digiturvaa. TAISTO on maksuton ja siihen voi osallistua useita harjoitusryhmiä yksittäisestä organisaatiosta.

Harjoittelutoiminta on keskeinen tapa toteuttaa digi- ja kyberturvaa, joten kannustamme organisaatioita suunnittelemaan vuosittaisen harjoitusohjelman, jonka organisaation johto hyväksyy ja resursoi riittävästi.

Lisätietoa harjoitustoiminnasta saa mm. Digiturvan tietopankista: Harjoitustoiminta - Kyberturvallisuuden ja digitaalisen turvallisuuden tietopankki - Suomi.fi kehittäjille

Digitaaliseen turvallisuuteen käytetty htv vs. poikkeamat

Kuvaaja. Digiturvaan käytetyt henkilötyövuodet suhteessa tietoturvapoikkeamiin. Kuvaajassa kunnat, HVA:t, Korkeakoulut, Valtiohallinto



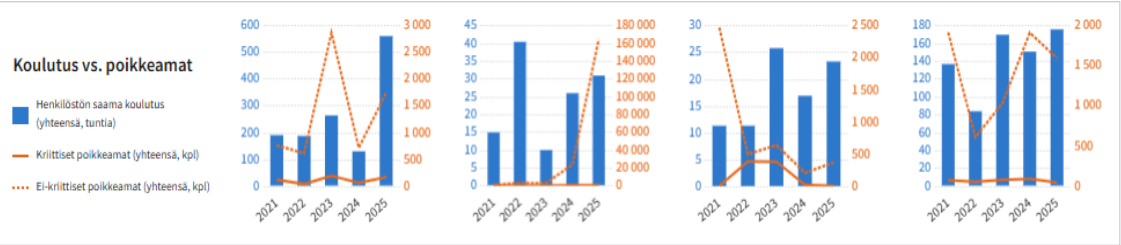
Vuoden 2025 kampanja oli ensimmäinen, jossa kysyttiin erikseen ostettujen resurssien määrää. Siksi ostetut resurssit eivät näy ennen vuotta 2025. Kuvaaja osoittaa kuinka kaikilla aloilla henkilöresurssien trendi on kasvava. Kuvaaja osoittaa myös kuinka vähän organisaatioissa havaitaan kriittisiä poikkeamia. Koska kriittiset poikkeamat ovat tilanteita, jotka eivät jää organisaatioilta huomaamatta, on tulokset todennäköisesti suhteellisen luotettavia.

Kuvaaja osoittaa myös, miten paljon suhteessa hyvinvointialueilla havaitaan ei-kriittisiä poikkeamia verrattuna muihin aloihin. Tämä johtuu mahdollisesti toimialan luonteesta, jossa lähtökohtaisesti keskitytään henkilötietojen käsittelyyn, mikä altistaa poikkeamille. Lisäksi hyvinvointialueet ovat erittäin kyvykkäitä havaitsemaan poikkeamat ja raportoimaan niistä.

Kuvaajan perusteella voidaan havaita, että henkilöresurssien lisääminen johtaa kriittisten poikkeamien vähenemiseen ja ei-kriittisten poikkeamien havaitsemisen lisääntymiseen. Riittävillä henkilöresursseilla on siten merkittävä vaikutus organisaation jatkuvuudenhallintaan ja oman havaintokyvyn ylläpitoon.

Koulutus vs. poikkeamat

Kuvaaja. Digiturvan koulutukset henkilöstölle suhteessa tietoturvapoikkeamiin. Kuvaajassa kunnat, HVA:t, Korkeakoulut, Valtiohallinto



Kyber- ja digiturvaan liittyvä koulutuksen trendi on kasvava, mikä on hyvä, sillä kyber- ja digiturva on jokaisen asia. Kuvaaja osoittaa myös, miten koulutuksen lisääminen kehittää varsinkin ei-kriittisten poikkeamien havaintokykyä. Koulutuksen määrällä ei kuitenkaan tunnu olevan suoraa selkeää vaikutusta kriittisten ja ei-kriittisten poikkeamien määrään. Tämä voi johtua siitä, että poikkeamien taustalla ei ole niinkään henkilöstön osaaminen vaan esimerkiksi kiire ja puutteelliset resurssit.

Koska koulutuksella on kuitenkin merkittävä vaikutus kyber- ja digiturvakulttuuriin, toimintatapoihin ja mm. organisaation havaintokykyyn, tulee koulutusta tarjota koko

henkilöstölle. Koulutuksen tarjoamisessa on hyvä tunnistaa koulutettavien henkilöiden tarpeet ja kohdentaa koulutukseen käytetyt resurssit tarkoituksenmukaisesti.

Suosittelemme laatimaan koko organisaation kattavan koulutussuunnitelman, jossa huomioidaan erilaiset tarpeet ja koulutettavien henkilöiden toimintaympäristö. Koulutusohjelman laatimisessa on hyvä hyödyntää organisaation riskienhallinnan tuottamaa informaatiota ja huomioida koulutuksissa tunnistetut riskit, hallintakeinot ja jäännösriskit, jotta koulutuksista saadaan paras mahdollinen vaikuttavuus.

DIGI- JA VÄESTÖTIETO-VIRASTO

Puh. **0295 536 000** (vaihde) | Yhteystiedot, katso **www.dvv.fi**