RAPORTTI

Tietoturvatutkimus 2025

Suomalaisyritykset ymmärtävät kyberuhat – käytännöissä vielä petrattavaa

DNA Yrityksille

Sisällysluettelo

1. Osaaminen, kumppanit ja yhteinen tahto ovat kyber-turvallisuuden kulmakivet

Kyberturvallisuus koskettaa jokaista organisaatiota Suomessa – riippumatta niiden koosta tai toimialasta. Digitalisaatio ja teknologian kehitys tarjoavat valtavia mahdollisuuksia, mutta samalla ne kytkevät meidät osaksi kokonaisuutta, jossa haavoittuvuudet heijastuvat laajalle: aivan jokaiseen palveluun ja käyttäjään. Siksi kyberturvallisuutta ei voi tarkastella vain IT-kysymyksenä, vaan olennaisena osana yritysten liiketoiminnan jatkuvuutta ja koko Suomen turvallisuutta.

Vuoden 2025 tietoturvatutkimuksen tulokset alleviivaavat tätä yhteisvastuun näkökulmaa. Tulokset kertovat kasvaneesta tietoisuudesta, mutta myös siitä, että arjen käytännöissä on paljon parannettavaa. Esimerkiksi vain reilu neljännes yrityksistä harjoittelee kyberkriisitilanteiden varalle. Paperilla suunnitelmat ovat monessa organisaatiossa kunnossa, mutta ilman harjoittelua tositilanteiden varalle olemme vasta puolitiessä.

Harjoittelun tarvetta lisää hybridityön maustama arki: kun työtä tehdään ja asioita hoidetaan kiireessä toimistojen, kotien ja julkisten tilojen välillä, vahinkojen ja väärinkäytösten riskit kasvavat. Ongelman ydin ei ole hybridityö itsessään vaan tarkkaavaisuutemme rajat, sillä suurin osa kyberhyökkäyksistä lähtee ihmisen epähuomiossa tekemästä virheestä. Nämä riskit eivät ole vain yksittäisten yrityksien ongelmia, sillä ne voivat heijastua toimitusketjujen kautta koko kansantalouteemme.

Yksi tutkimuksen tärkeimmistä huomioista kohdistuu osaajapulaan. Se koskettaa sekä suuria että pieniä organisaatioita. Erityisesti kokeneista kyberturvaosaajista on huutava pula. Pullonkaulan ratkaisemiseksi yhä useammat yritykset hakevat tukea osaavilta kumppaneilta, korostaen yritysten välisen yhteistyön jatkuvasti kasvavaa merkitystä. Harva organisaatio pärjää yksin, mutta yhdessä olemme vahvempia. Meillä jokaisella on vastuu vahvistaa kansallista kyberresilienssiämme.

Tutkimuksen tulokset kertovat tarinaa Suomesta, joka on tietoinen uhkakuvista, mutta jonka on vahvistettava käytännön kyvykkyyttään. Kyberresilienssi rakentuu paitsi teknologiasta, myös jatkuvasta harjoittelusta, riskien aktiivisesta hallinnasta, yhteistyöstä ja kumppanien hyödyntämisestä. Tärkeintä on jatkaa oppimista, oli kyse oman osaamisen kehittämisestä, teknologian hyödyntämisestä tai erilaisten uhkien ymmärtämisestä.

Tietoturva on maraton, jonka jokainen askel vie meitä kohti turvallisempaa digitaalista yhteiskuntaa. Meillä on kaikki edellytykset onnistua: osaaminen, kumppanit ja yhteinen tahto.

Anna-Mari Ylihurula,
DNA:n yritysliiketoiminnan johtaja

2. Tutkimuksen tavoite ja perustiedot

Tässä tutkimuksessa selvitettiin, miten Suomessa toimivissa yrityksissä ja julkishallinnon organisaatioissa suhtaudutaan tietoturvaan ja kyberturvallisuuteen.

Tutkimuksen avulla pyritään lisäämään ymmärrystä siitä, millaisena ICT-päättäjät näkevät kyberuhkien tilanteen, millaisella tasolla yrityksen varautumisen uskotaan olevan, miten tietoturvaan liittyvät investoinnit ovat kehittyneet sekä mitä hybridityöhön ja tekoälytyökalujen käyttöön liittyvästä tietoturvasta ajatellaan.

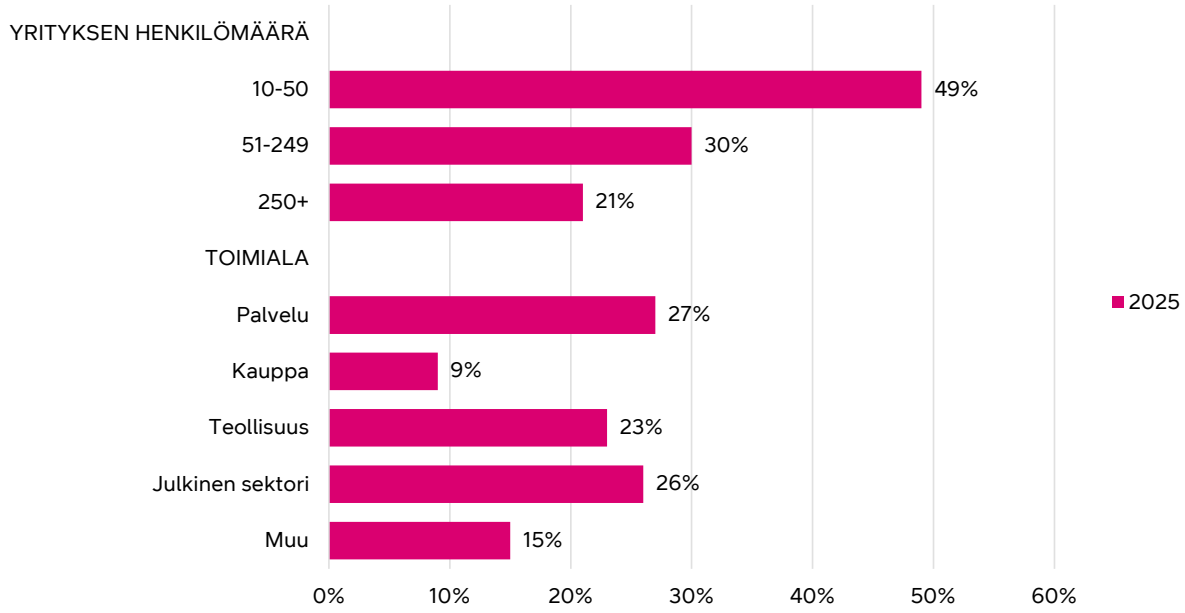
Tutkimus on tehty kvantitatiivisena kyselytutkimuksena elokuussa 2025, ja sen on toteuttanut DNA:n toimeksiannosta Dagmar Oy.

Raportissa tehdään suuntaa antavaa vertailua vuoden takaiseen, syyskuussa 2024 toteutettuun tutkimukseen. Menetelmä, kohderyhmä ja sisältö ovat vertailukelpoisia.

Perustiedot

Tiedonkeruun ajankohta	08/2025
Tutkimuksen kohderyhmä	ICT-päättäjät ja -johtajat Suomessa toimivista yrityksistä ja julkishallinnon toimijoista, jotka työllistävät vähintään 10 henkilöä
Menetelmä	Kvantitatiivinen kyselytutkimus, joka on toteutettu verkko- ja puhelinkyselynä
Vastaajamäärä	N= 156 10–50 henkilöä työllistävät yritykset: N=76 51–249 henkilöä työllistävät yritykset: N=47 Yli 250 henkilöä työllistävät yritykset: N=33

Vastaajien jakauma



3. Tutkimustulokset

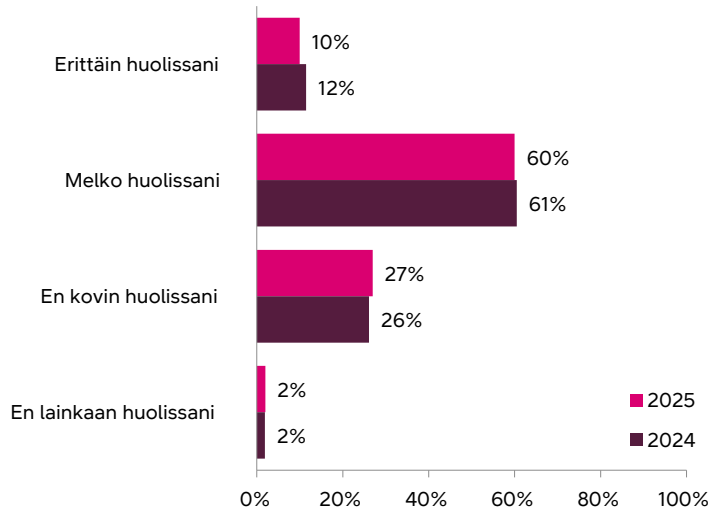
3.1 Kyberuhat ja huolenaiheet

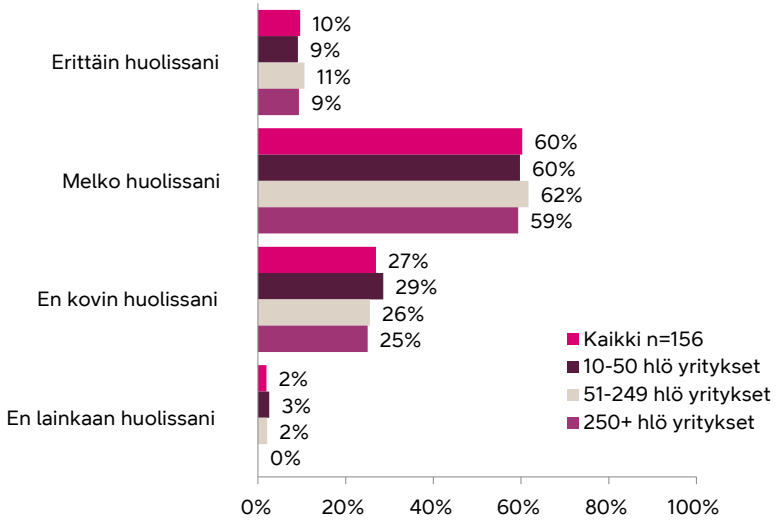
Huoli kyberturvallisuudesta Suomessa

70 % ICT-päättäjistä on huolissaan Suomessa toimivien yritysten kyberturvallisuudesta. Huoli on pysynyt viime vuoteen nähden samalla tasolla. Huoli koskee sekä isoja että pieniä yrityksiä.

> **On äärimmäisen hyvä asia, että yritykset ovat huolissaan kyberturvallisuudesta. Se tarkoittaa, että ymmärrämme kyberuhat sekä laajemman turvallisuustilanteen.**

Kuinka huolissasi olet Suomessa toimivien yritysten kyberturvallisuustilanteesta?





Kyberturvallisuuden huolenaiheet

Avoimissa vastauksissa huolenaiheina nousivat useimmin esiin tietomurrot, tietovuodot ja yritysvakoilu, toiseksi eniten valtiolliset toimijat (erityisesti Venäjä) sekä kolmantena palvelunestohyökkäykset. Huolta herättivät myös laitteiden käyttöön ja käyttäjiin liittyvä osaamattomuus ja huolimattomuus sekä pelko henkilötietojen varastamisesta.

Viime vuoteen verrattuna huolenaiheet ovat pirstaloituneempia, mikä näkyy prosentuaalisena laskuna useassa kategoriassa sekä samanaikaisesti Muut-kategorian suurena nousuna. Muut-kategoriassa esiintyi paljon mainintoja erilaisista teemoista, kuten esimerkiksi tekoäly, disinformaatio sekä yleinen varautumattomuus ja uhkatilanteen ymmärryksen puute.

Mitkä kyberturvallisuuteen liittyvät uhkatekijät huolestuttavat eniten? (Avoin kysymys)

”Asiakkaiden tietojen kaappaaminen, maksujen blokkaaminen ja sähköpostien käytön estäminen.”

”Ei ole mitään yksittäistä huolenaihetta. Kokonaisuudessaan jos joku pääsee käsiksi järjestelmiin, niin se huolestuttaa.”

”Osaamattomuus ja osaamisten keskittyminen isoihin firmoihin.”

”Palveluestohyökkäykset lamauttavat toiminnan aika kokonaisvaltaisesti.”

”Ulkoisten valtioiden/valtiollisten toimijoiden tekemät kyberhyökkäykset, toisaalta kyberrikollisuus varsinkin ammattimaisella tasolla.”

”Omat työntekijät, huolimattomuus.”

Kyberturvallisuuden huolenaiheet	2025	2024
Tietomurrot, tietovuodot ja yritysvakoilu	32%	38%
Valtiolliset toimijat (erityisesti Venäjä)	18%	26%
Palvelunesto-hyökkäykset	13%	9%
Laitteiden käyttö ja käyttäjät	9%	15%
Henkilötietojen varastaminen	6%	6%
Muut	22%	6%

Taulukossa on kuvattu avoimet vastaukset kategorisoituna.

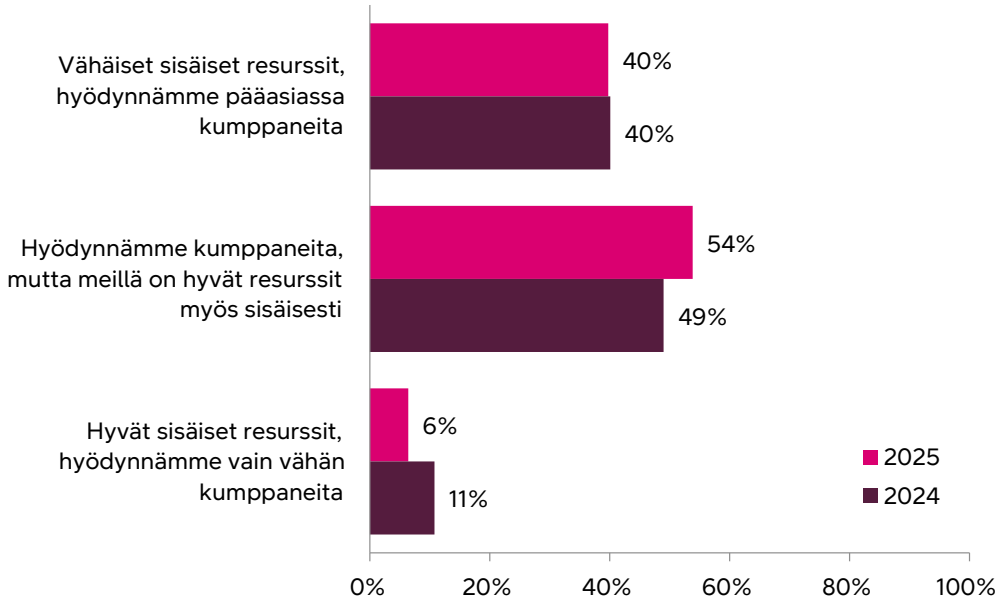
3.2 Investoinnit ja osaaminen

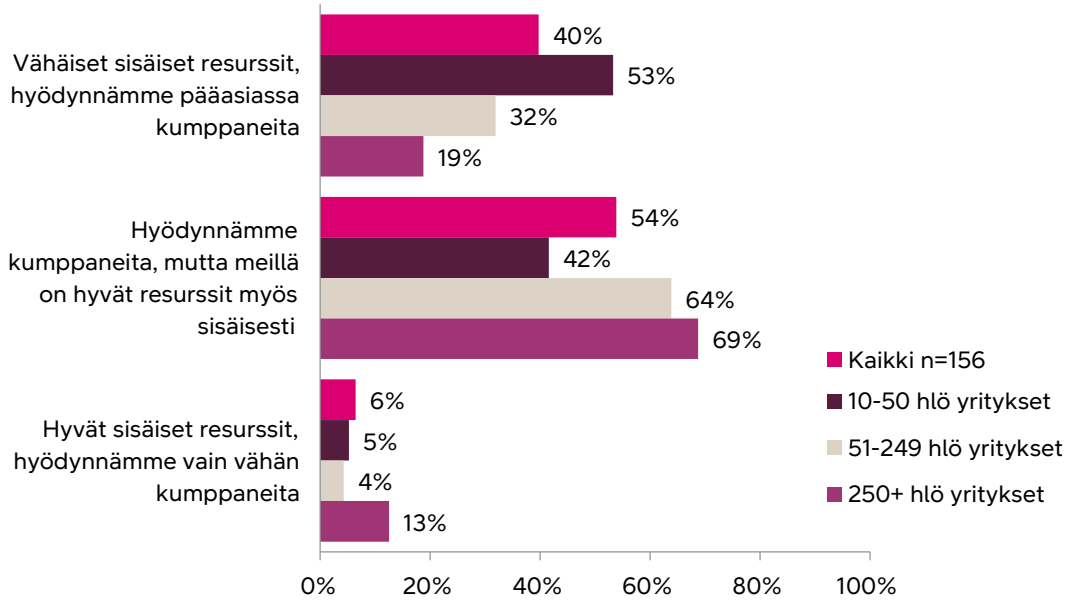
Kumppaneiden hyödyntäminen tieto- ja kyberturvallisuudessa

Kumppaneita hyödynnetään tieto- ja kyberturvallisuuden saralla hieman enemmän kuin edellisvuonna. Tämä korostuu erityisesti niissä yrityksissä, joissa on hyvät sisäiset resurssit. Tutkimus osoittaa, että lähes kukaan ei pärjää yksin, vaan kumppaneiden rooli on tärkeä.

94 % vastaajista ilmoitti hyödyntävänsä kumppaneita tieto- ja kyberturvallisuudessa joko pääasiassa tai jonkin verran. Vain 6 % ilmoitti, että hyödyntää kumppaneita vain vähän.

Mikä seuraavista väittämistä kuvaa parhaiten yrityksesi tapaa hyödyntää kumppaneita tietoturvaan ja kyberturvallisuuteen liittyen?



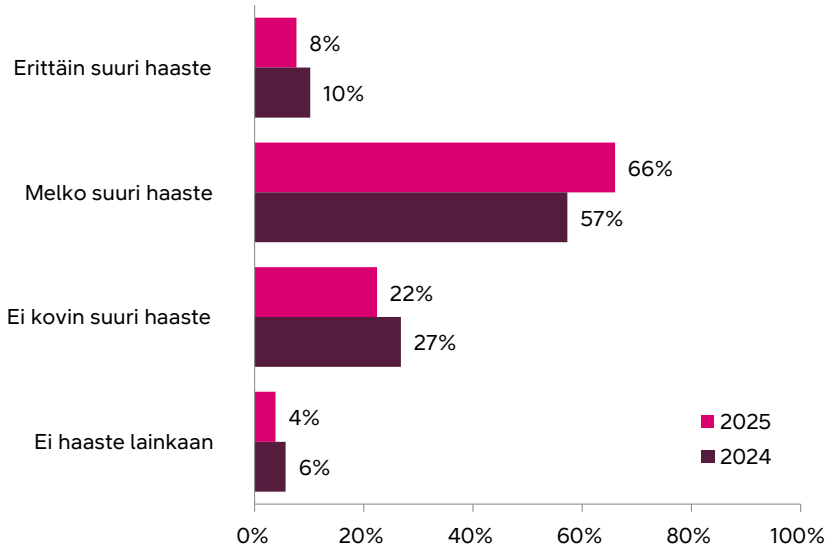


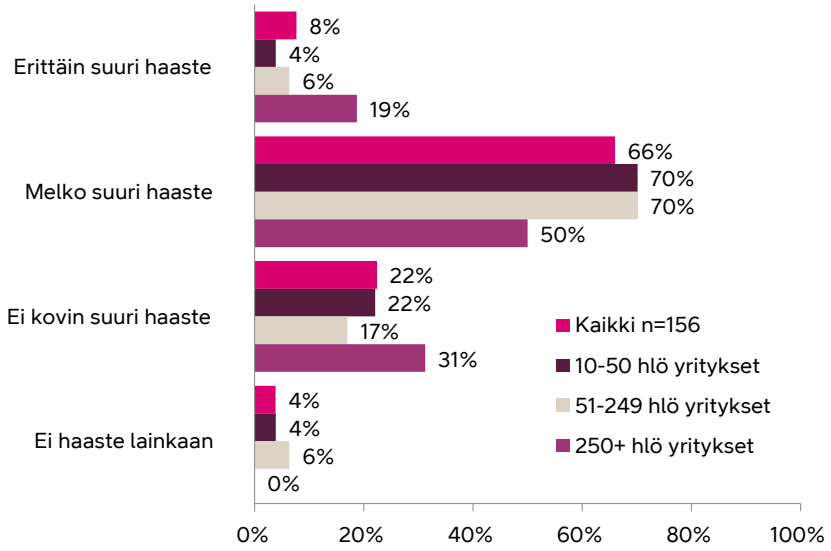
Osaajapulan vaikutus kyber-turvan tasoon

Osaajapula on valtava haaste yrityksille ja sen painoarvo on kasvanut vuodesta 2024. Osaajapulan kanssa kamppailevat kaiken kokoiset yritykset, mutta erityisesti pienemmät yritykset kokevat osaajapulan isoja yrityksiä tuntuvammin.

> **Markkinassa tarve osaajille on suurempi kuin mitä koulutus pystyy tuottamaan. Tämän lisäksi haetaan erityisesti jo kaiken kokeneita ammattilaisia.**

Kuinka merkittävä haaste osaajapula on mielestäsi hyvän kyberturvatason saavuttamiseksi?



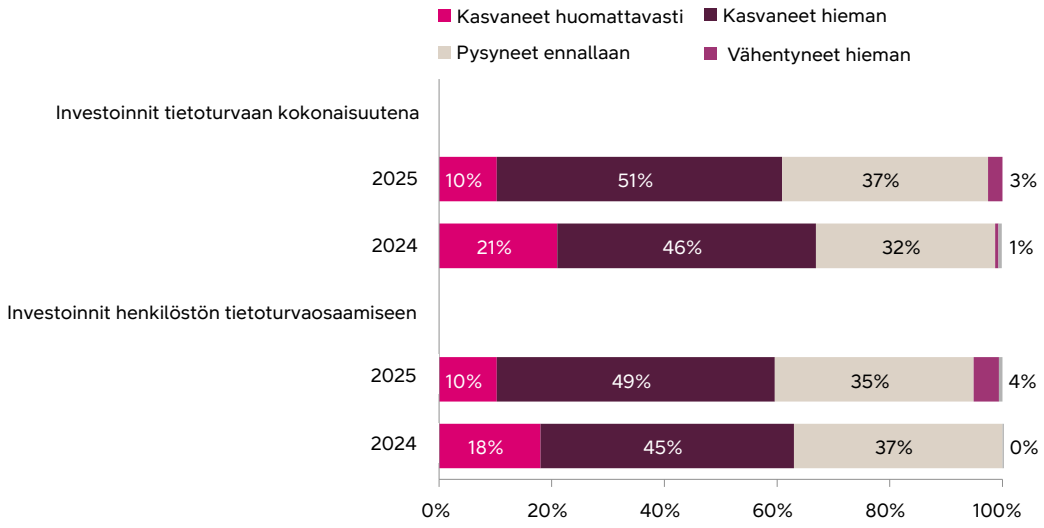


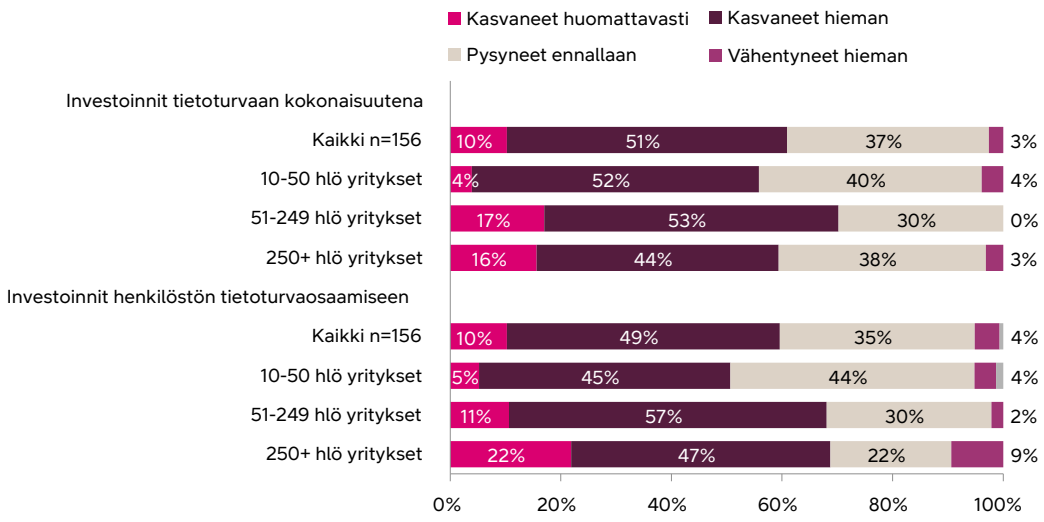
Tietoturvainvestointien kehitys viimeisen viiden vuoden aikana

Tietoturvainvestoinnit ovat kasvaneet viimeisen viiden vuoden aikana. Näyttää kuitenkin siltä, että kasvukulma on loivenemassa viime vuoteen nähden. Muutokset tietoturvaan tehtävien investointien määrissä ovat hyvin samanlaisia yrityskoosta riippumatta.

> **Ensin investoidaan vahvasti teknologioihin ja tietoturvatilanteen parantamiseen, ja sen jälkeen siirrytään käyttöönottovaiheeseen. Kun alkuinvestoinnit on tehty, pitää huolehtia, että niistä saadaan hyöty irti.**

Miten yrityksesi tietoturvainvestoinnit ovat kehittyneet viimeisen viiden vuoden aikana? Vastaa tietoturvasta kokonaisuutena sekä henkilöstön tietoturvaosaamisen osalta.

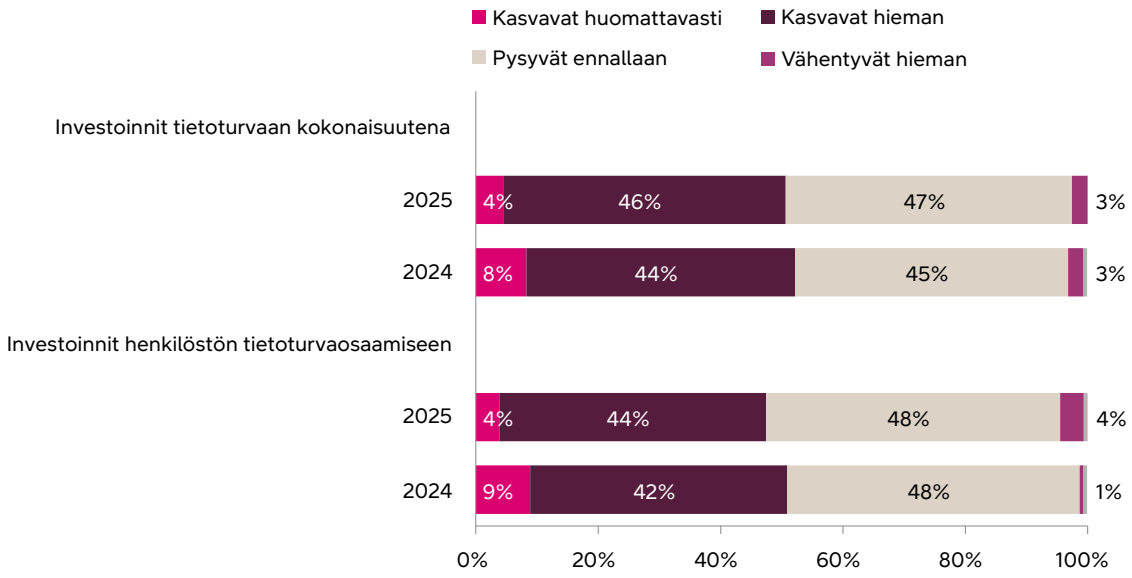


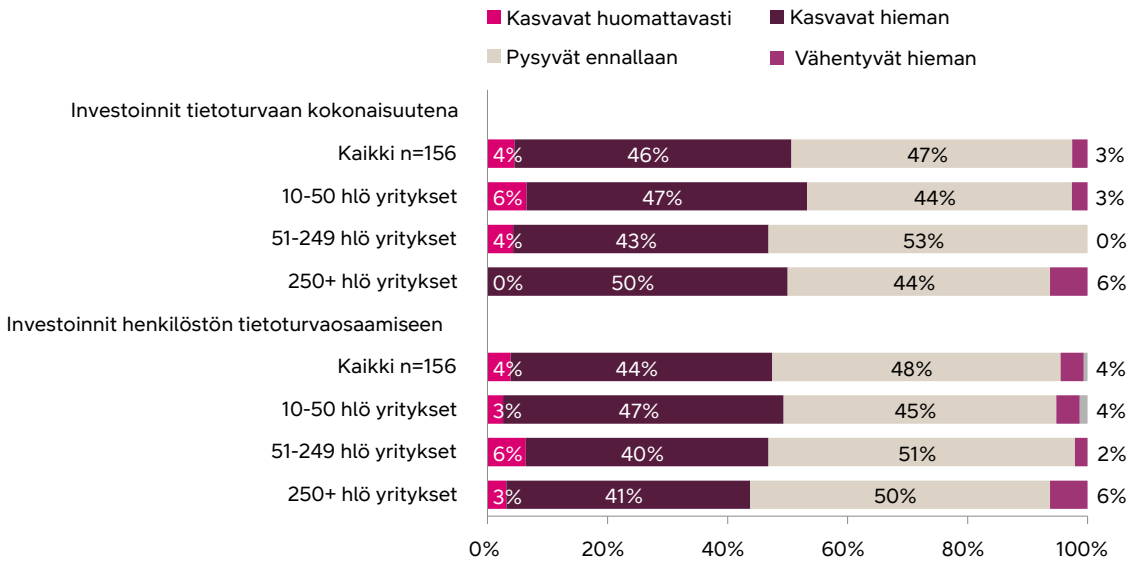


Tietoturvainvestointien kehitysnäkymät seuraavalle vuodelle

Tietoturvainvestoinnit ovat edelleen selvässä kasvussa, mutta investointeja huomattavasti kasvattavien yritysten määrä on hieman maltillisempi verrattuna viime vuoteen niin kokonaisuuden kuin henkilöstön tietoturvaosaamisenkin kannalta.

Miten investoinnit tietoturvaan muuttuvat yrityksessäsi, kun vertaat ensi vuotta tähän vuoteen? Vastaa tietoturvasta kokonaisuutena sekä henkilöstön tietoturvaosaamisen osalta.

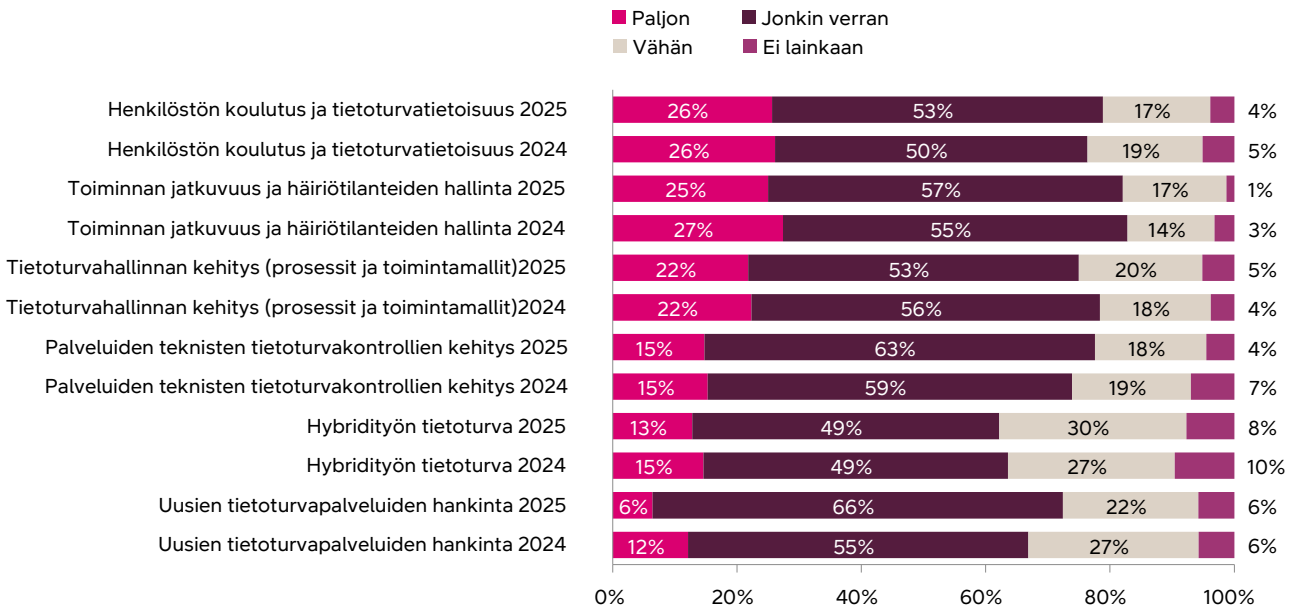


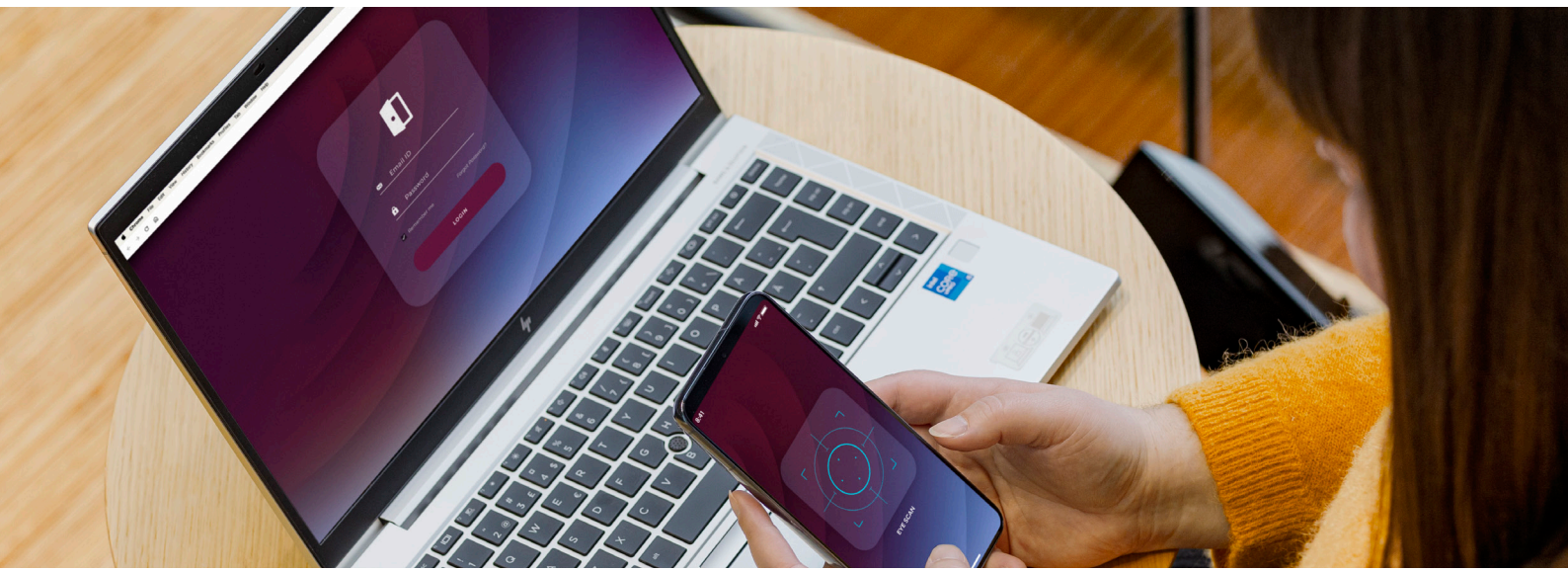


Näihin panostetaan seuraavan vuoden aikana

Tietoturvan saralla suunnitellaan yhä paljon panostuksia kuin edellisvuonnakin. Yritykset investoivat erityisesti henkilöstön koulutukseen ja tietoturvatietoisuuteen, toiminnan jatkuvuuteen ja häiriötilanteiden hallintaan sekä tietoturvahallinnan prosesseihin ja toimintamalleihin.

Kuinka paljon yrityksessänne aiotaan panostaa seuraaviin tietoturvaan liittyviin osa-alueisiin seuraavan vuoden aikana?

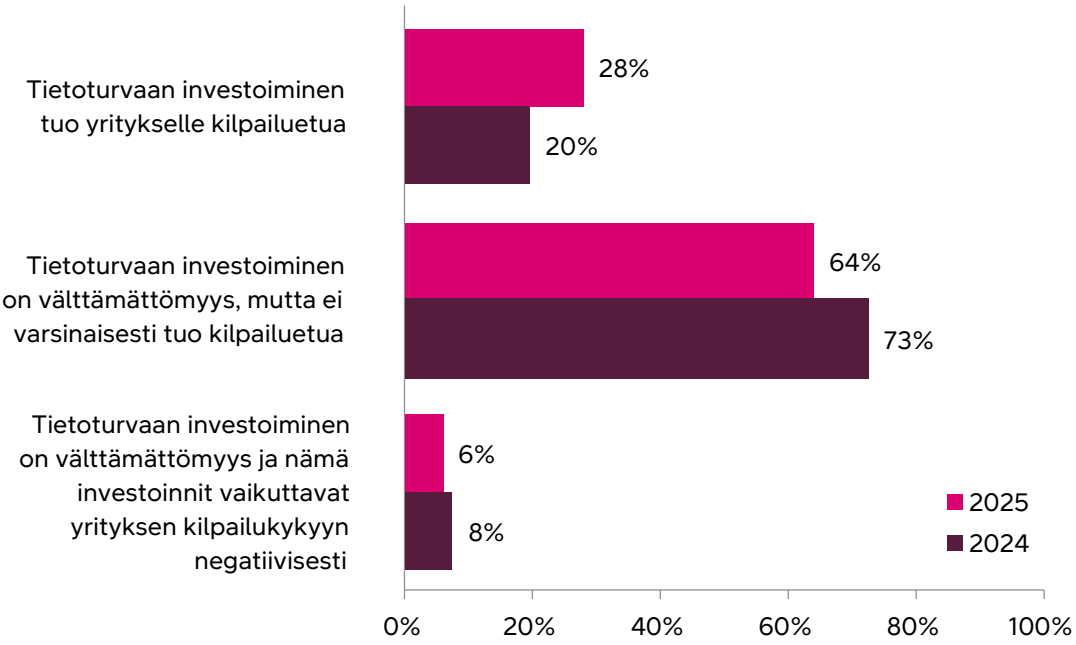


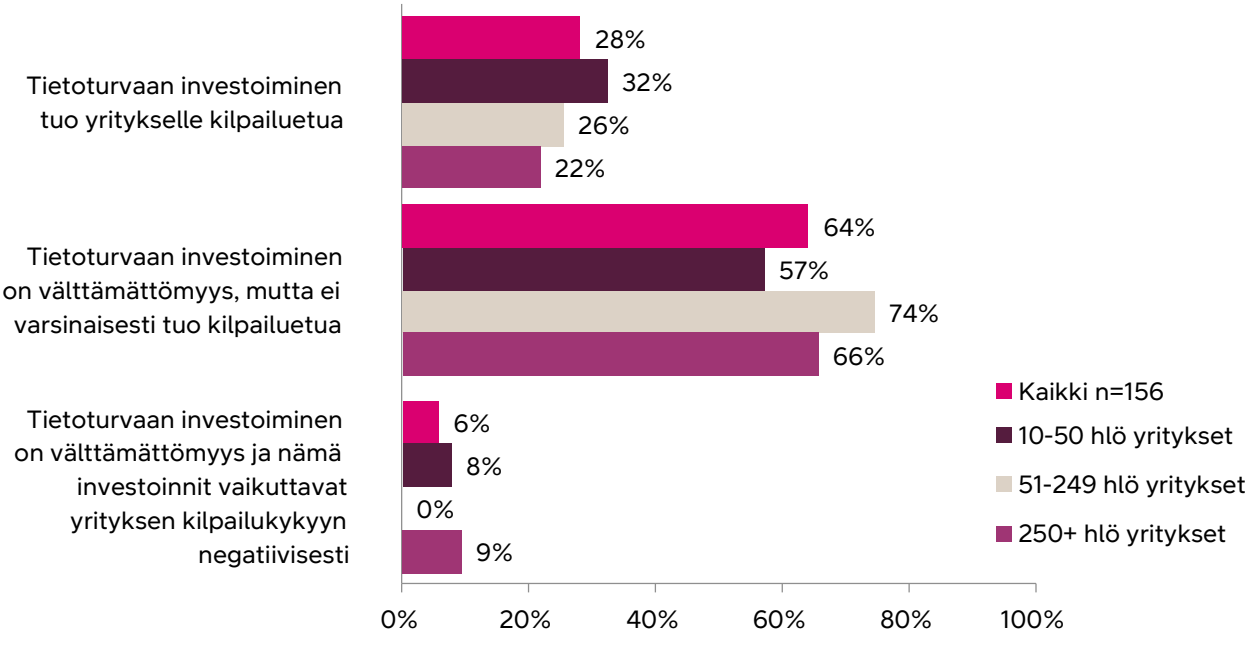


Kilpailuetua tietoturvasta

Jo 28 % päättäjistä uskoo tietoturvainvestointien tuovan yritykselle kilpailuetua. Luku on kasvanut 8 prosenttiyksikköä vuodesta 2024. Eniten kilpailuetua kokevat saavansa 10–50 henkilöä työllistävät yritykset. 64 % päättäjistä pitää tietoturvaa välttämättömyytenä, mutta ei usko sen tuovan varsinaisesti kilpailuetua.

Ajattele tietoturvaan tehtäviä investointeja yrityksessäsi. Mikä seuraavista kuvaa ajattelua yrityksessäsi?





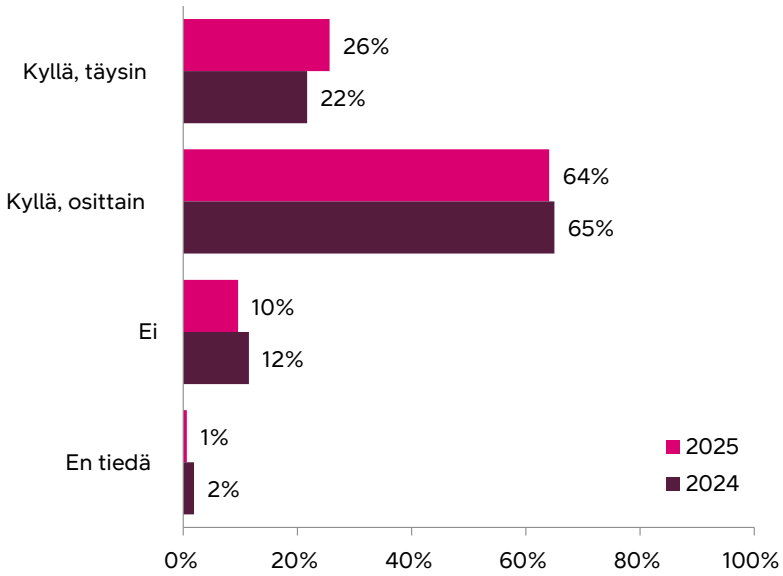
3.3 Varautuminen

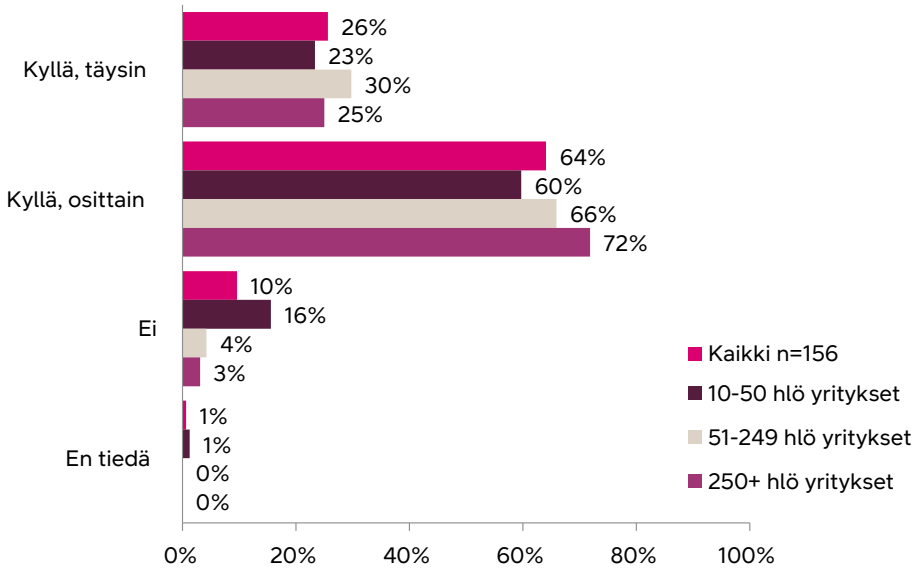
Valmiudet varautua kyberuhkiin

Suurin osa Suomessa toimivista yrityksistä kokee, että heillä on vähintään osittaiset valmiudet varautua nykyiseen kyberuhkatilanteeseen. Valmiudet ovat pysyneet hyvin samalla tasolla vuoteen 2024 verrattuna. Kuitenkin vain noin neljännes vastaajista koki, että heidän yrityksensä pystyy täysin varautumaan kyberuhkiin. Epävarmimpia varautumisestaan ovat pienet, 10–50 henkilöä työllistävät yritykset.

> **Kääntäisin tuloksen ympäri: jopa kolme neljästä tietää, että kyberturvallisuudessa on kehitettävää. Se tarkoittaa, että leijonan osa yrityksistä on tietoturvan suhteen riittävän kypsällä tasolla, jotta he tietävät, että varautumista tulee vielä kehittää.**

Koetko, että yrityksessäsi on riittävät valmiudet varautua nykyiseen kyberuhkatilanteeseen?



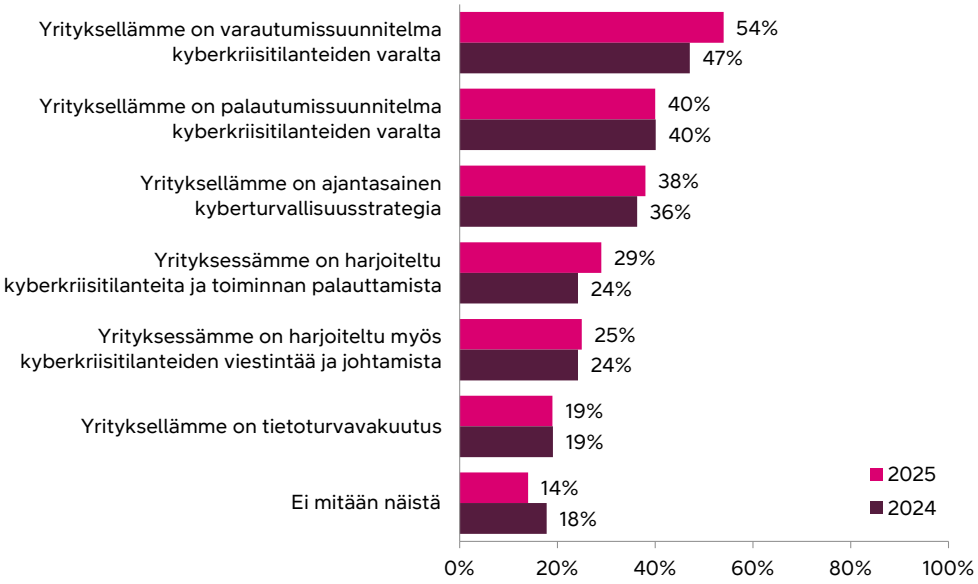


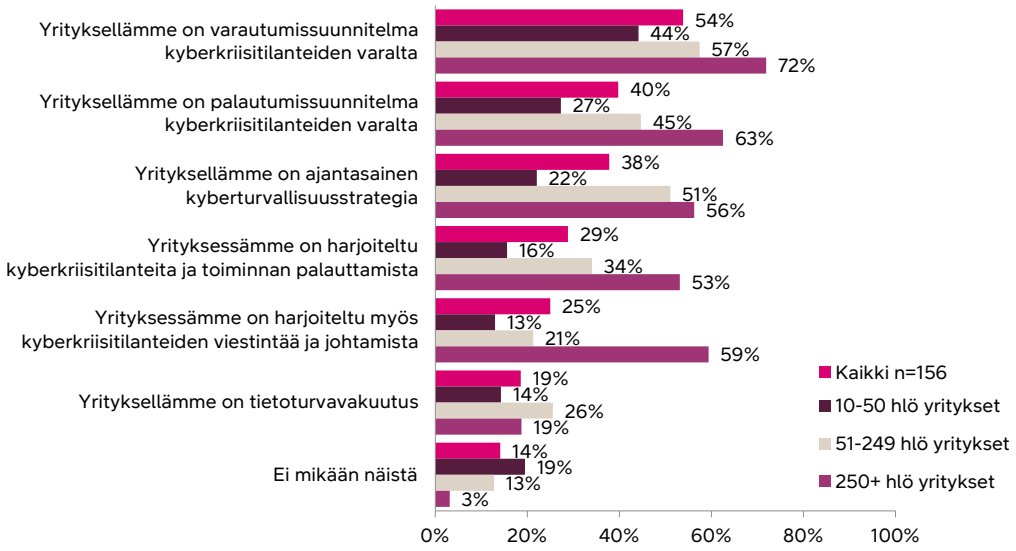
Varautumisen toimenpiteet

Yhä useammalla yrityksellä (54 %) on varautumissuunnitelma viime vuoteen verrattuna (47 %), mutta silti vajaalla puolella yrityksistä ei ole varautumissuunnitelmaa laisinkaan. Yli 250 henkilöä työllistävissä yrityksissä varautumisen toimenpiteitä tehdään selvästi useammin kuin pienemmissä yrityksissä. Kyberkriisitilanteita ja toiminnan palauttamista harjoitellaan edelleen vain alle kolmasosassa yrityksistä, vaikka harjoittelevien osuus on hieman kasvanut viime vuodesta.

> **Paperilla suunnitelmat voivat olla hyviä, mutta ilman harjoittelua ne jäävät happotestaamatta.**

Mitä seuraavista tietoturvaan liittyvistä toimenpiteistä yrityksellänne on tai mihin on varauduttu?





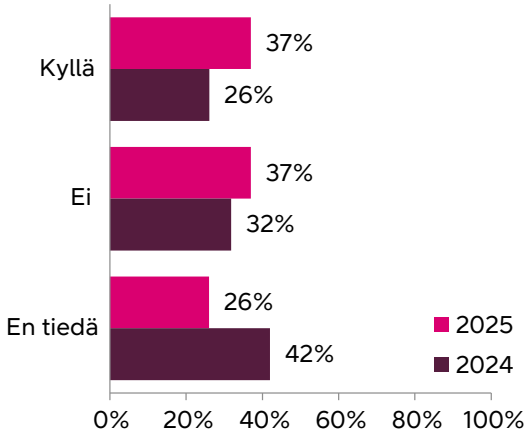
NIS2-direktiivi

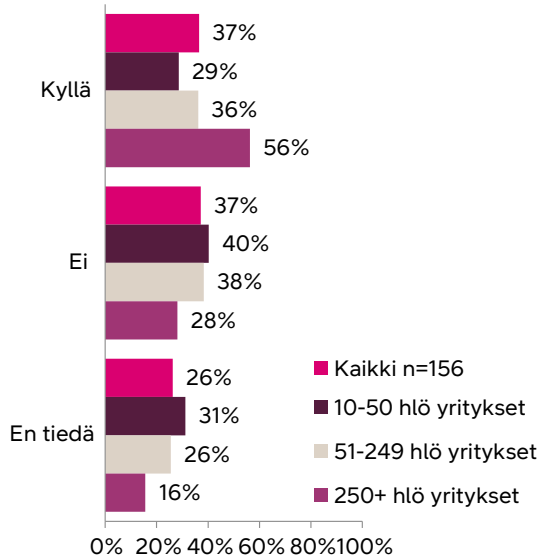
Tietoisuus NIS2-direktiivistä on kasvanut selvästi kansallisen kyberturvallisuuslain tultua voimaan vuoden 2025 huhtikuussa. Direktiivin tavoitteena on parantaa EU:n jäsenvaltioiden kyberturvallisuutta yhtenäisillä säännöillä.

81 % lain velvoittamista yrityksistä kokee täyttävänsä kyberturvallisuuslain vaatimat velvoitteet ainakin suurelta osin. Pienemmät yritykset tuntuvat olevan varmempia kyvystään täyttää velvoitteet kuin isommat yritykset.

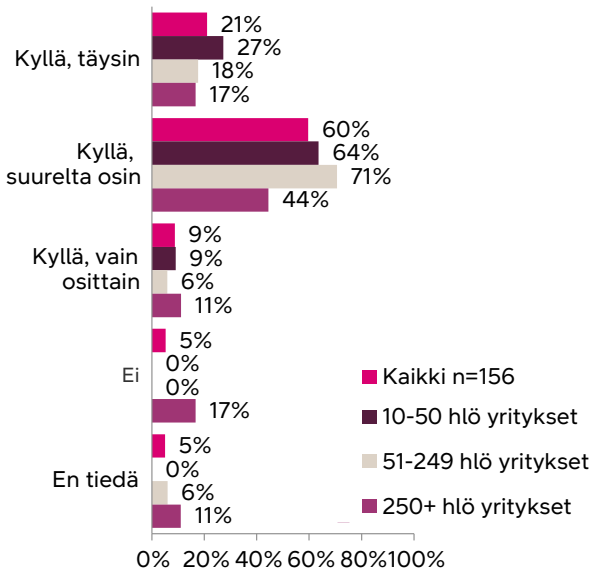
> **Regulaatio toimii kyberturvallisuuden kirittäjänä: Se pakottaa organisaatiot miettimään kyberturvaa entistä useammalta taholta ja tekemään konkreettisia toimia.**

Täytyykö yrityksesi noudattaa NIS2-direktiiviin pohjautuvaa, huhtikuussa 2025 voimaan tullutta kansallista kyberturvallisuuslakia?





JOS KYLLÄ: Täyttääkö yrityksesi kyberturvallisuuslain määrittämät uudet riskienhallinta- ja raportointivelvoitteet tällä hetkellä? N=57



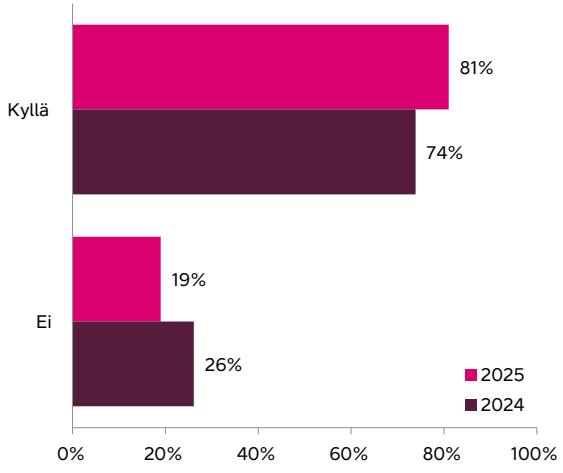
3.4 Hybridityö ja tekoäly

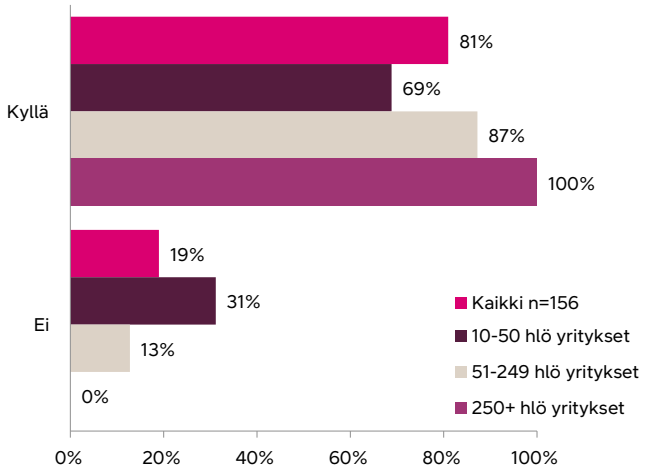
Hybridityön tietoturva

Hybridityön tekeminen on lisääntynyt yrityksissä hieman viime vuoteen nähden. Mitä enemmän henkilöstöä yrityksessä on, sitä yleisempää on myös hybridityön tekeminen. Hybridityön riskit tiedostetaan viime vuotta paremmin ja henkilöstön koulutus tietoturvariskien saralla nähdään tärkeämpänä.

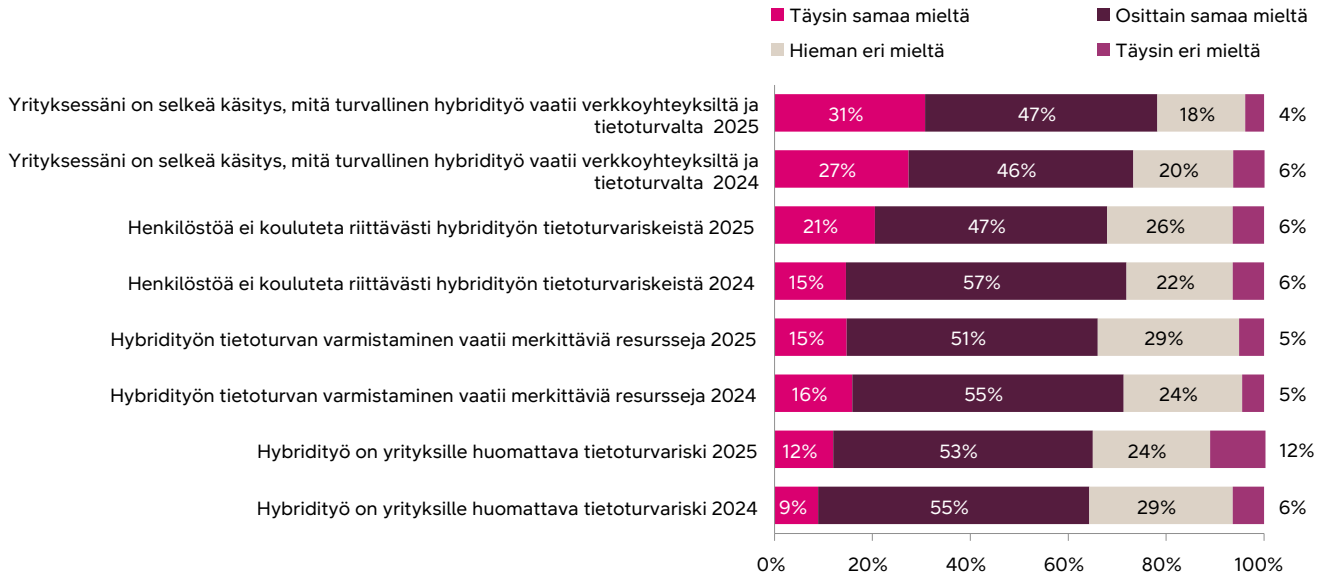
Mitä suurempi yritys on kyseessä, sitä selkeämpi käsitys yrityksessä on turvallisen hybridityön vaatimilta verkkoyhteyksiltä ja tietoturvalta. Pienemmissä yrityksissä koetaan isoja yrityksiä useammin, että hybridityön tietoturvan varmistaminen vaatii merkittäviä resursseja.

Tehdäänkö yrityksessänne hybridityötä?





Kuinka hyvin seuraavat väittämät pitävät mielestäsi paikkansa?



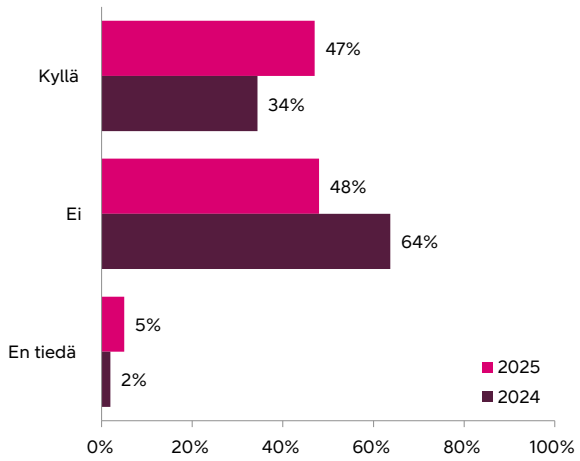
Tekoälyn linjaukset ja tietoturva

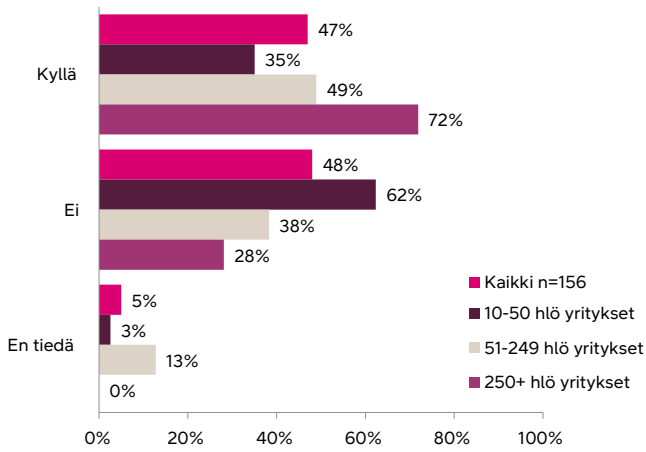
Sääntöjen ja linjausten tekeminen tekoälytyökalujen käytölle on yleistynyt viime vuoteen verrattuna. Mitä suurempi yritys, sitä todennäköisemmin säännöt ja linjaukset ovat kunnossa. Silti lähes puolelta yrityksistä säännöt vielä puuttuvat.

Tekoälytyökalujen haasteet koetaan edelleen yhtä suurina kuin edellisvuonna. 83 % vastanneista pitää tekoälytyökalujen ohjeistusta puutteellisena ja 70 % uskoo, että yrityksen IPR-dataa tai liikesalaisuuksia voi joutua vääriin käsiin tekoälytyökalujen käytön takia.

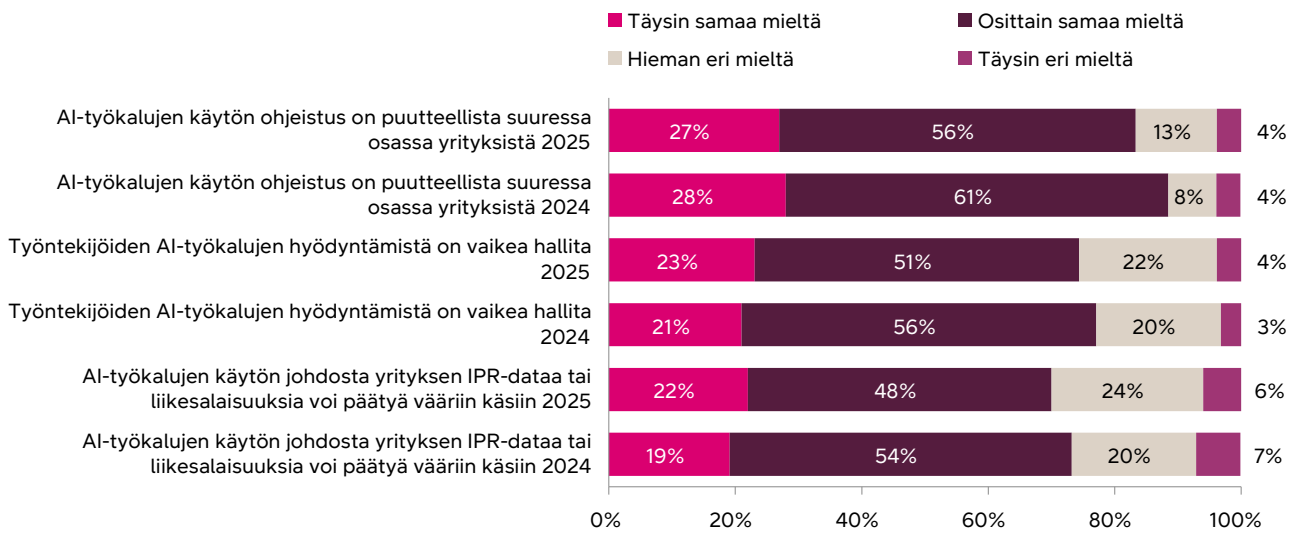
> **Nyt jo paljon pinnalla ollut tekoäly tulee varmasti olemaan suurin muutos, eikä kukaan vielä osaa ennustaa kaikkia tapoja, joilla se tulee vaikuttamaan meihin.**

Onko yrityksessänne tehty säännöt ja linjaukset henkilöstölle tekoälyn käyttöön liittyen?





Kuinka hyvin seuraavat väittämät pitävät mielestäsi paikkansa?



4. Asiantuntijan analyysi

”Kyberturvallisuuden suhteen ei voi olla koskaan tarpeeksi varautunut”

”On äärimmäisen hyvä asia, että yritykset ovat huolissaan kyberturvallisuudesta. Se tarkoittaa, että ymmärrämme kyberuhat sekä laajemman turvallisuustilanteen. Kun tilannetietoisuus on kohdillaan, se tarkoittaa, että viranomaisten viestit ovat menneet yrityksille perille”, kuvailee **Kaapro Kanto**, DNA:n yritysliiketoiminnan verkko- ja pilvipalveluiden liiketoimintajohtaja.

Viime vuoden tapaan tutkimuksessa nousi esille suomalaisyrityksiä selvästi huolestuttava uhkatekijä: valtiolliset toimijat.

”Tämänhetkinen geopoliittinen tilanne pitää varautumisen tason korkeana: varautumista harjoitellaan, kyberturvallisuuteen investoidaan ja geopoliittinen uhkakuva tiedostetaan. Kun Euroopassa käydään sotaa, on selvää, että myös kyberkentällä sivuvaikutukset ovat mahdollisia.”

Tutkimuksessa valtiollisten toimijoiden lisäksi suurimmiksi huolenaiheiksi nousivat tietomurrot, tietovuodot ja yritysvakoilu. Suuret organisaatiot tunnistavat ja hallitsevat riskit jo melko kypsästi, mutta pk-yrityksissä resurssien rajallisuus vaikeuttaa priorisointia.

“Isoissa yrityksissä kyberturvaprosessit ovat kehittyneitä, mutta pienemmissä toimijoissa kipuillaan edelleen sen kanssa, miten riskit pitäisi tunnistaa ja hallita. Toimitusketjujen kautta nämä haavoittuvuudet voivat asettaa myös suuremmat organisaatiot alttiimmiksi riskeille.”

Käytännön harjoittelussa parantamisen varaa, mutta velvoitteet ymmärretään

Kyberresilienssin kannalta tutkimuksen huolestuttavimpia havaintoja on, että vain reilu neljännes yrityksistä harjoittelee kyberkriisitilanteita käytännössä.

”Paperilla suunnitelmat voivat olla hyviä, mutta ilman harjoittelua ne jäävät happotestaamatta. Tämä aukko näkyy erityisesti hybridityön arjessa: kun työ kulkee kodin, toimiston ja julkisten tilojen välillä, riski tietovuodoista ja väärinkäytöksistä kasvaa. Kyse ei ole pelkästään yksittäisten yritysten ongelmasta, vaan Suomen kokonaisturvallisuuden näkökulmasta vakavasta haasteesta.”

Kannon mukaan kuitenkin NIS2-direktiivi ja huhtikuussa 2025 voimaan tullut kansallinen kyberturvallisuuslaki ovat nostaneet tietoisuutta yritysten tietoturvavelvoitteista. Hänen mukaansa regulaatio toimii kyberturvallisuuden kirittäjänä: Se pakottaa organisaatiot miettimään kyberturvaa entistä useammalta taholta ja tekemään konkreettisia toimia.

Kumppanit auttavat hellittämään osaajapulaa

Terveen huolen lisäksi suomalaisyritysten tilannetietoisuus näkyy investointeina. Investoinnit tietoturvaan ovat kasvaneet yhtäjaksoisesti viiden vuoden ajan, vaikka nyt kasvu onkin näyttänyt hidastumisen merkkejä. Kyse ei kuitenkaan ole säästölinjasta, vaan kehityksen luonnollisista sykleistä.

”Ensin investoidaan vahvasti teknologioihin ja tietoturvatilanteen parantamiseen, ja sen jälkeen siirrytään käyttöönottovaiheeseen. Kun alkuinvestoinnit on tehty, pitää huolehtia, että niistä saadaan hyöty irti ja teknologiat sekä kumppanuudet otetaan täysipainoisesti käyttöön”, Kanto selittää.

Yksi asia, johon moni yritys olisi valmis investoimaan ovat kokeneet tietoturvaosaajat – mutta heitä ei niin vain löydykään. Osaajapula koetaan valtavaksi haasteeksi kaikenkokoisissa yrityksissä.

”Markkinassa tarve osaajille on suurempi kuin mitä koulutus pystyy tuottamaan. Tämän lisäksi haetaan erityisesti jo kaiken kokeneita ammattilaisia, kun taas koulusta valmistuvat nuoret eivät heti täytä resurssitarvetta. Meneillään on jatkuva viive: valmistuneilla kestää ennen kuin he saavat teorian käytäntöön, ja samalla ammattilaisten tarve kasvaa koko ajan.”

Tätä ongelmaa taklataan tutkimuksen mukaan kumppaneiden avulla: 94 % vastaajista ilmoitti hyödyntävänsä kumppaneiden tukea tietoturvaan ja kyberturvallisuuteen liittyen joko pääasiassa tai jonkin verran.

> **Kyse ei ole pelkästään yksittäisten yritysten ongelmasta, vaan Suomen kokonaisturvallisuuden näkökulmasta vakavasta haasteesta.**

Päättäjien tietoturvatietoisuus on kypsällä tasolla

Vain noin neljännes tutkimukseen vastanneista kokee pystyvänsä varautumaan täysin kyberuhkiin. Mitä se tarkoittaa suomalaisyritysten kokonaisturvallisuuden kannalta?

”Kun mietitään kyberuhkiin varautumista, niin mitä enemmän on tietoinen ja mitä enemmän ymmärtää tämänhetkistä tilannetta, sitä varmempi on yleensä siitä, ettei koskaan voi olla tarpeeksi varautunut. Kääntäisin tuloksen mieluummin ympäri: jopa kolme neljästä tietää, että kyberturvallisuudessa on kehitettävää. Se tarkoittaa, että leijonan osa yrityksistä on tietoturvan suhteen riittävän kypsällä tasolla, jotta he tietävät, että varautumista tulee vielä kehittää.”

Kannon mukaan tutkimuksen tulokset kertovat realistisen kuvan kyberturvallisuudesta kansallisella tasolla. Kyberturvaa kehitetään systemaattisesti ja samalla ymmärretään, että uhkakenttä muuttuu koko ajan. Entä millaisia muutoksia kyberturvakenttään on odotettavissa seuraavien viiden vuoden aikana?

”Nyt jo paljon pinnalla ollut tekoäly tulee varmasti olemaan suurin muutos, eikä kukaan vielä osaa ennustaa kaikkia tapoja, joilla se tulee vaikuttamaan meihin. Tämän lisäksi meihin tulee vaikuttamaan regulatiivisen kentän yhtenäistyminen, kun EU-maiden rajat kyberturvassa madaltuvat ja voimme alkaa rakentamaan yhdessä Euroopan laajuista kybersuojaa. Kyberturvallisuus ei ole vain tekninen kysymys, vaan osa kokonaisturvallisuutta.”

5. Yhteenveto tuloksista

Päättäjät ovat huolissaan kyberturvallisuudesta

Suomessa toimivien yritysten ICT-päättäjistä 70 % on huolissaan kyberturvallisuudesta. Huoli on pysynyt viime vuoteen nähden yhtä korkealla tasolla. Tämä on linjassa yleisen kyberturvallisuustilanteen kanssa: Suojelupoliisi huomioi myös elokuisessa tiedotteessaan uhkatason pysyneen koholla. Suurimpina huolenaiheina tutkimuksessa nousivat esiin tietomurrot, tietovuodot ja yritysvakoilu, toiseksi suurimpana valtiolliset toimijat sekä kolmantena palvelunestohyökkäykset.

Varautumisvalmiudessa ei suurta muutosta

Suurin osa yrityksistä kokee, että niillä on vähintään osittaiset valmiudet varautua nykyisiin kyberuhkiin. Kuitenkin vain 26 % yrityksistä uskoo pystyvänsä varautumaan niihin täysin. 64 % taas arvioi valmiuksiensa olevan vain osittaiset. Valmiudet ovat pysyneet samalla tasolla vuoteen 2024 verrattuna.

Varautumistoimenpiteet eivät juurikaan ole yleistyneet

Ennakointi, riskien tunnistaminen ja niiden arviointi ovat osa varautumista. Ainoa viime vuodesta hieman yleistynyt toimenpide on varautumissuunnitelman laatiminen: nyt 54 % yrityksistä on oma varautumissuunnitelma, kun viime vuonna vastaava luku oli 47 %. Muut toimenpiteet ovat harvinaisempia: vain vajaa kolmannes harjoittelee kyberkriisitilanteita ja toiminnan palauttamista, ja vain noin viidennes on hankkinut tietoturvavakuutuksen.

Investoinnit tietoturvaan ovat yhä kasvussa

Puolella yrityksistä on suunnitelmana kasvattaa kokonaisinvestointeja tietoturvaan vuonna 2026. Lähes yhtä moni aikoo panostaa henkilöstön osaamiseen. Vaikka kasvuodotukset investointeihin ovat loiventuneet viime vuoteen verrattuna, kukaan ei ilmoita vähentävänsä niitä. Eniten panostuksia harkitaan henkilöstön tietoturvatietoisuuteen, toiminnan jatkuvuuteen ja häiriötilanteiden hallintaan sekä prosessien kehittämiseen.

Tietoturva nähdään aiempaa useammin kilpailuetuna

Jo 28 % päättäjistä uskoo tietoturvainvestointien tuovan yritykselle kilpailuetua. Luku on kasvanut 8 prosenttiyksikköä vuodesta 2024. 64 % päättäjistä pitää tietoturvaa välttämättömyytenä, mutta ei usko sen tuovan varsinaisesti kilpailuetua.

Osaajapula ei laannu

Osaajapula on yhä merkittävä haaste yrityksille ja sen painoarvo on kasvanut viime vuodesta. 74 % vastaajista pitää sitä esteenä hyvän kyberturvan saavuttamiselle (2024: 67 %). Erityisesti pk-yritykset kärsivät osaajien puutteesta. Kumppaneiden rooli onkin merkittävä: 94 % yrityksistä hyödyntää kumppaneita tietoturvaan liittyvissä asioissa joko pääasiassa tai jonkin verran.

NIS2-direktiivi on lisännyt tietoisuutta

Tietoisuus NIS2-direktiivistä on kasvanut selvästi kansallisen kyberturvallisuuslain tultua voimaan vuoden 2025 huhtikuussa. Direktiiviin pohjautuva kyberturvallisuuslaki koskee 37 % kyselyyn vastanneista yrityksistä. Näistä yrityksistä joka viides kokee täyttävänsä velvoitteet täysin ja neljä viidestä ainakin osittain. Kehitys on merkittävää: vielä vuonna 2024 42 % yrityksistä ei tiennyt, kuuluuko oma yritys sääntelyn piiriin. Nyt vastaava osuus on laskenut 26 prosenttiin.

Hybridityö kirittää kybertietoisuutta

Hybridityön yleistyessä yrityksillä on parempi käsitys siihen liittyvistä tietoturvavaatimuksista, mutta samalla uhkakuvat tiedostetaan entistä paremmin. Moni kokee, ettei henkilöstöä kouluteta riittävästi, mikä lisää riskejä.

Tekoälyn sääntöjä on määritelty yhä useammassa yrityksessä

Tekoälyn käyttöön liittyviä sääntöjä ja linjauksia on tehty jo lähes puolessa yrityksistä (2024: 34 %). Silti työntekijöiden tekoälyn käyttöä on vaikea hallita, ja keskeisenä riskinä nähdään edelleen salassa pidettävien tietojen päätyminen vääriin käsiin. Huolenaiheet ovat pysyneet samoina kuin vuonna 2024.

6. Yhteistyöllä kestävää tietoturvaa: suojaa liiketoimintasi kokonaisvaltaisesti

Tietoturva ei ole vain yksittäinen ratkaisu, työkalu tai teknologia – se on kokonaisuus, joka vaikuttaa suoraan liiketoiminnan jatkuvuuteen, luotettavuuteen ja asiakkaiden luottamukseen. Siksi tarvitaan kumppani, joka ymmärtää sen merkityksen.

DNA tarjoaa kattavan valikoiman tietoturvapalveluita, joiden avulla yrityksesi pysyy suojattuna. Asiantuntijamme auttavat sinua rakentamaan juuri yrityksellesi sopivan kokonaisuuden, jota on helppo hallita ja kehittää liiketoimintasi tarpeiden muuttuessa.

Näin voit keskittyä liiketoimintaasi tietäen, että taustalla on kumppani, joka huolehtii sen turvaamisesta kaikissa tilanteissa.

Tutustu tietoturvapalveluihimme ja lataa käyttöösi maksuttomat tietoturvaoppaat pk-yrityksille ja suurille organisaatioille!

DNA on yksi Suomen johtavista tietoliikenneyhtiöistä. Tehtävämme yhteiskunnassa on yhdistää tärkeimmät. Tarjoamme yhteydet, palvelut ja laitteet koteihin sekä töihin ja pidämme näin huolta yhteiskunnan digitalisaatiosta. DNA:n asiakkaat ovat jo vuosien ajan olleet mobiilidatan käyttömäärissä maailman kärkijoukossa. DNA:lla on noin 3,8 miljoonaa matkaviestin- ja kiinteän verkon liittymäasiakkuutta. Vuonna 2024 liikevaihtomme oli 1 100 miljoonaa euroa ja yhtiössä työskentelee noin 1 600 henkilöä ympäri Suomea.

DNA on osa Telenoria, joka on yksi Pohjoismaiden johtavista tietoliikenneyhtiöistä. Tämä antaa meille mahdollisuuden tarjota asiakkaillemme entistä laajemman ja vahvemman valikoiman erilaisia yhteyksiä, tietoturvapalveluita sekä asiantuntemusta. Yhdessä 18 000 asiantuntijan voimin kehitämme ja ylläpidämme palveluitamme niin suomalaisille kuin pohjoismaisille asiakkaillemme.

part of telenor

DNA Yrityksille