RAPORTTI

Tietoturvatutkimus 2024

Miltä kyberturvallisuuden kenttä näyttää suomalaisyritysten silmin?

DNA Yrityksille

Sisällysluettelo

1. Vahva tietoturva on vastuun kantamista koko yhteiskunnasta

Valtioneuvosto julkaisi lokakuussa 2024 merkittävällä tavalla päivitetyn Suomen Kyberturvallisuusstrategian. Vertaaminen edelliseen vuonna 2019 julkaistuun versioon antaa vahvan viestin maailman muuttumisesta. Uhkakuvat ovat nyt selkeämpiä, lähempänä meitä jokaista, ja niistä puhutaan suorin sanoin. Suomalaisille ICT-päättäjille mukana on monta olennaista viestiä ja kehotusta.

Jokaisen Suomessa toimivan organisaation on tärkeää ymmärtää, että omasta tietoturvasta huolehtiminen on vastuun kantamista myös muiden organisaatioiden, koko Suomen ja koko maailman toimivuudesta. Yhteiskuntiemme digitalisoituminen on tuottanut liiketoiminnoille paljon hyvää ja avannut valtavasti uusia mahdollisuuksia. Samaan aikaan tietoverkoista ja digitaalisista alustoista riippuvaisten yhteiskuntien toimivuus edellyttää, että jokainen meistä osallistuu yhteisen turvallisuuden varmistamiseen.

Peräti 73 % DNA:n tietoturvatutkimukseen vastanneista ICT-päättäjistä on huolissaan suomalaisten yritysten kyberturvallisuudesta. Tämä on paitsi hälyttävää, myös erinomaista: hurja luku kertoo, että tietoturva otetaan Suomessa nyt todella vakavasti.

Tietoturvatutkimuksen tuloksista huokuu vahva ratkaisuhakuisuus. Investoinnit tietoturvaan ovat kasvaneet merkittävästi kuluneiden viiden vuoden aikana, ja tulevan vuoden aikana panostuksia kasvatetaan entisestään. Tämä on loistava asia. Samaan aikaan sekä meillä palveluntarjoajilla että jokaisella ICT-päättäjällä on entistäkin tärkeämpi tehtävä huolehtia siitä, että investoinnit kohdistuvat oikeisiin asioihin. Vastuunsa tunteva johto varmistaa, että käytössä on aina markkinoiden kärkeä edustavat ratkaisut ja teknologiat. Lisäksi johdon on huolehdittava siitä, että organisaation kyberturvatietoisuuden taso nousee, ja että mukana on koko henkilökunta.

Tekoälyn merkitys kasvaa, mutta avainasemassa tietoturvan toteutumisessa ovat ihmiset – ja näin tulee olemaan vielä pitkään. Vastuu on tälläkin alueella organisaatioiden johdolla: meidän tehtävämme on huolehtia siitä, että teknisen tietoturvan ohella myös osaaminen ja ymmärrys on kunnossa. Tietoturvakulttuuri luodaan yhdessä, ja se on meidän kaikkien tehtävä.

Olemme mielellämme edistämässä turvallisen digitaalisen yhteiskunnan kehittymistä.

Anna-Mari Ylihurula
Yritysliiketoiminnan johtaja
DNA Oyj

2. Tutkimuksen tavoite ja perustiedot

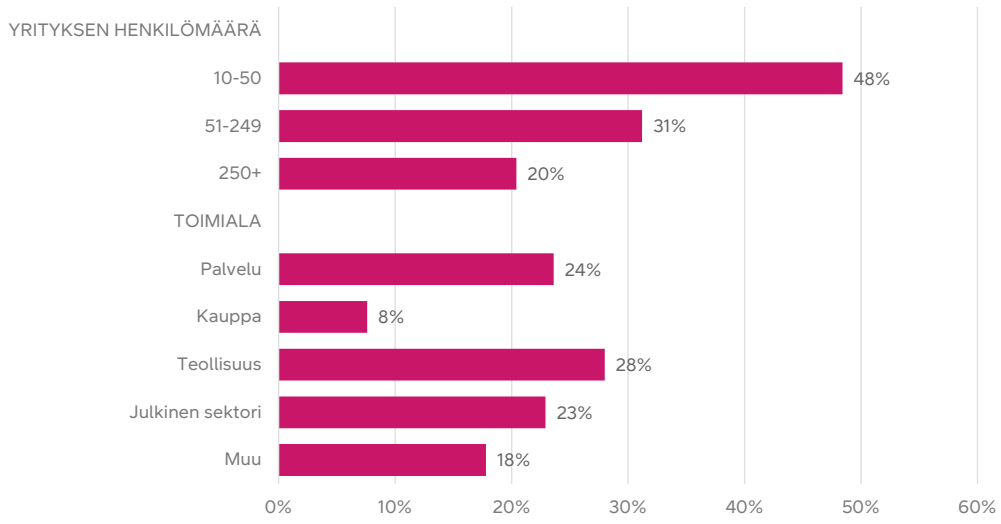
Tutkimuksessa selvitettiin, miten Suomessa toimivissa yrityksissä ja julkishallinnossa suhtaudutaan tietoturvaan ja kyberturvallisuuteen.

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 toteutettu kvantitatiivisena kyselytutkimuksena syyskuussa 2024, ja sen on toteuttanut DNA:n toimeksiannosta Dagmar Oy.

Tiedonkeruun ajankohta	09/2024
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=157 10-50 henkilöä työllistävät yritykset: N=75 51-249 henkilöä työllistävät yritykset: N=50 Yli 250 henkilöä työllistävät yritykset: N=32

Vastaajien jakauma



3. Yhteenveto tuloksista

ICT-päättäjät huolissaan

Tutkimukseen vastanneiden yritysten ICT-päättäjistä jopa 73 % ilmaisee huolensa Suomessa toimivien yritysten kyberturvallisuudesta. Huolenaiheita ovat muun muassa tietojen kalastelu, tietomurrot ja palvelunestohyökkäykset. Suurimmaksi yksittäiseksi kyberturvallisuuden uhkatekijäksi avoimissa vastauksissa korostui vieraan valtion aiheuttama uhka (erityisesti Venäjä).

Varautumisessa oltava hereillä

Suomessa toimivista yrityksistä suurin osa kokee, että niillä on riittävät valmiudet varautua nykyiseen kyberuhkatilanteeseen. Kuitenkin vain 22 % vastaajista kertoo, että heidän edustamansa yritys pystyy täysin varautumaan kyberuhkiin. Epävarmimpia varautumisestaan ovat pienet 10–50 henkilöä työllistävät yritykset.

Suurin osa investoi entistä enemmän tietoturvaan

Tietoturvaan on investoitu viimeisen viiden vuoden aikana huomattavasti: 67 % vastaajista kertoo, että yrityksen tietoturvainvestoinnit ovat tällä aikavälillä kasvaneet. Myös tietoturvaosaamiseen on investoitu viimeisen viiden vuoden aikana paljon: yli 60 % vastanneista sanoo, että investoinnit henkilöstön tietoturvaosaamiseen ovat kasvaneet.

Lisäksi tietoturvainvestointien kerrotaan olevan kasvussa myös ensi vuonna – sekä kokonaisuudessaan että henkilöstön osaamisen osalta. Harva yritys on vähentämässä investointejaan.

Investointikykyä löytyy, osaajia ei

Osaajapula on yrityksille valtava haaste: 67 % vastaajista nimeää osaajapulan haasteeksi hyvän kyberturvan saavuttamisessa. Saman haasteen kanssa kamppailevat yritykset koosta riippumatta.

Kukaan ei pärjää yksinään, sillä jopa 89 % vastaajista ilmoittaa hyödyntävänsä kumppaneita tietoturvan ja kyberturvallisuuden saralla. Mitä pienempi yritys on, sitä enemmän palveluita ostetaan kumppaneilta.

NIS2-direktiivi haastavaa saavuttaa täysin

Uuden NIS2-kyberturvadirektiivin* noudattaminen nähdään yrityksissä haastavana. 42 % vastaajista ei tiedä, koskeeko NIS2 heidän edustamaansa yritystä. Ja vain 15 % niistä, jotka vastasivat direktiivin velvoittavan yritystään, sanoo yrityksen yltävän täysin vaadittuun tasoon direktiivin soveltamista koskevaan määräaikaan mennessä. 59 % direktiivin piiriin kuuluvista vastaajista kertoo kuitenkin, että tulee pääsemään vaadittavaan tasoon osittain.

*EU:n ja sen jäsenvaltioiden kansallista kyberturvaa yhtenäistävän NIS2-direktiivin soveltaminen alkoi 18.10.2024. Suomessa kyberturvallisuuslaki on vielä eduskunnan käsittelyssä. Lailla pannaan kansallisesti täytäntöön NIS2-direktiivin vaatimukset.

Varautumis- tai palautumissuunnitelmia vain alle puolella

Yli 10 henkilön yrityksistä vain reilulla kolmanneksella (36 %) on ajantasainen kyberturvallisuusstrategia. Sellainen on 250 henkilön yrityksistäkin vain noin puolella. Useammalla yrityksellä on varautumissuunnitelma, mutta niiden määrä jää alle puoleen yrityksistä. 29 % yrityksistä ilmoittaa, ettei heillä ole kyberturvallisuusstrategiaa, eikä varautumis- tai palautumissuunnitelmaa. Nämä yritykset ovat pääsääntöisesti (72 %) pieniä, 10–50 henkilön yrityksiä.

Moni yritys kohtaa mahdollisen kriisin ilman harjoitusta

Niistä yrityksistä, joilla on varautumissuunnitelma, vain reilu kolmannes harjoittelee kriisitilanteita tai toiminnan palauttamista varten. Vastaava määrä harjoittelee myös kriisitilanteiden viestintää ja johtamista.

Hybridityöstä uudenlaisia uhkia

Hybridityö on tuonut yrityksiin lisää resurssitarvetta sekä synnyttänyt uudenlaisia uhkia. Riskit kasvavat henkilöstömäärän mukana: mitä enemmän työntekijöitä, sitä suurempi riski. Toisaalta pienemmät yritykset ovat resurssien osalta suuremmassa paineessa, sillä resursseja on ennestäänkin vähemmän. Isolla osalla yrityksistä on selkeä käsitys hybridityön tietoturvavaatimuksista. Silti yli puolet (64 %) pitää hybridityötä huomattavana tietoturvariskiä lisäävänä tekijänä. Samalla 72 % uskoo, että henkilöstön kouluttaminen ei ole riittävällä tasolla.

Linjauksia tekoälyn käyttöön vain noin kolmanneksella

ICT-päättäjien keskuudessa vallitsee konsensus siitä, että tekoälytyökalujen käytön ohjeistus on puutteellista suuressa osassa Suomessa toimivista yrityksistä. Syynä on pääasiassa vaikeus hallita työntekijöiden tekoälytyökalujen hyödyntämistä, jolloin uhkakuvana on liikesalaisuuksien päätyminen vääriin käsiin. Toisaalta sääntöjä ja linjauksia tekoälyn käyttöön on tehty vain noin joka kolmannessa tutkimukseen vastanneessa yrityksessä. Henkilöstömäärältään suuremmissa yrityksissä säännöt ja linjaukset ovat kuitenkin useammin tehtynä kuin henkilöstömäärältään pienemmissä yrityksissä.

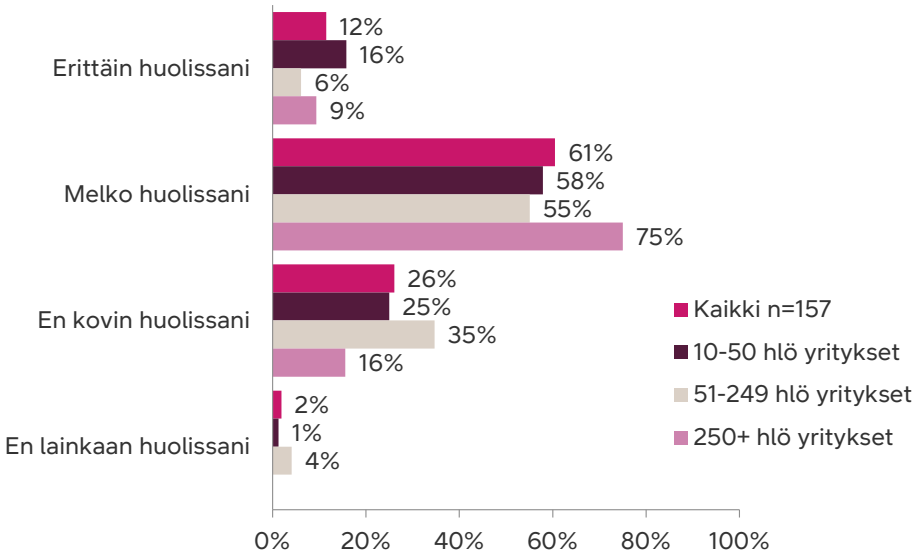
4. Tutkimustulokset

4.1 Kyberuhat ja huolenaiheet

Huoli kyberturvallisuudesta Suomessa

73 % ICT-päättäjistä on huolissaan Suomessa toimivien yritysten kyberturvallisuudesta. Mitä suurempi yritys, sitä suurempi on myös huoli. Yli 250 henkilöä työllistävistä yrityksistä lähes 85 % on aiheesta melko tai erittäin huolissaan.

Kuinka huolissasi olet Suomessa toimivien yritysten kyberturvallisuustilanteesta?



Kyberturvallisuuden huolenaiheet

Huolenaiheita ovat muun muassa tietojen kalastelu, tietomurrot ja palvelunestohyökkäykset. Suurimmaksi yksittäiseksi kyberturvallisuuden uhkatekijäksi avoimissa vastauksissa korostui vieraan valtion aiheuttama uhka (erityisesti Venäjä).

Mitkä kyberturvallisuuteen liittyvät uhkatekijät huolestuttavat eniten?

”Hyökkäyksen seurauksena yrityksen toiminnan keskeytyminen”

”Kiristyshaittaohjelma, vakoilu, disinformaatio, erilaiset huijaukset”

”Laitteiden henkilökohtainen käyttö: sovellukset, sivustot tai sähköpostit, jotka voivat aiheuttaa tietoturvariskejä. Verkkoyhteyksien salaus/avoimuus.”

”Tekoälyn avulla tehtävät kyberhyökkäykset”

”Tietomurrot ja tietojen päätyminen vääriin käsiin”

“Venäjän kyberhyökkäykset”

Huolenaihe	Osuus vastauksista %
Tietomurrot, tietovuodot ja yritysvakoilu	38 %
Ulkopuoliset valtiot ja toimijat (erityisesti Venäjä)	26 %
Laitteiden käyttö ja käyttäjät	15 %
Palvelunestohyökkäykset	9 %
Henkilötietojen varastaminen	6 %

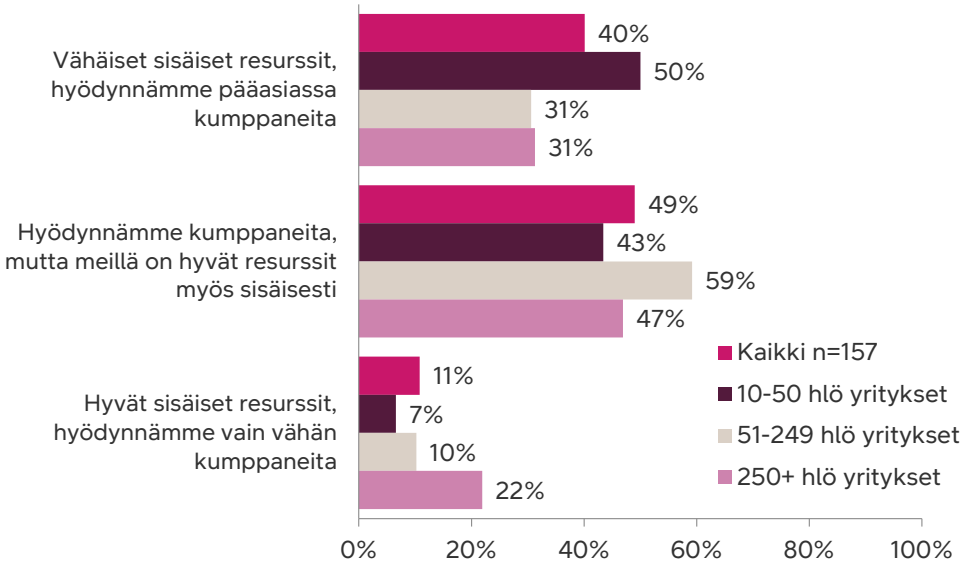
4. Tutkimustulokset

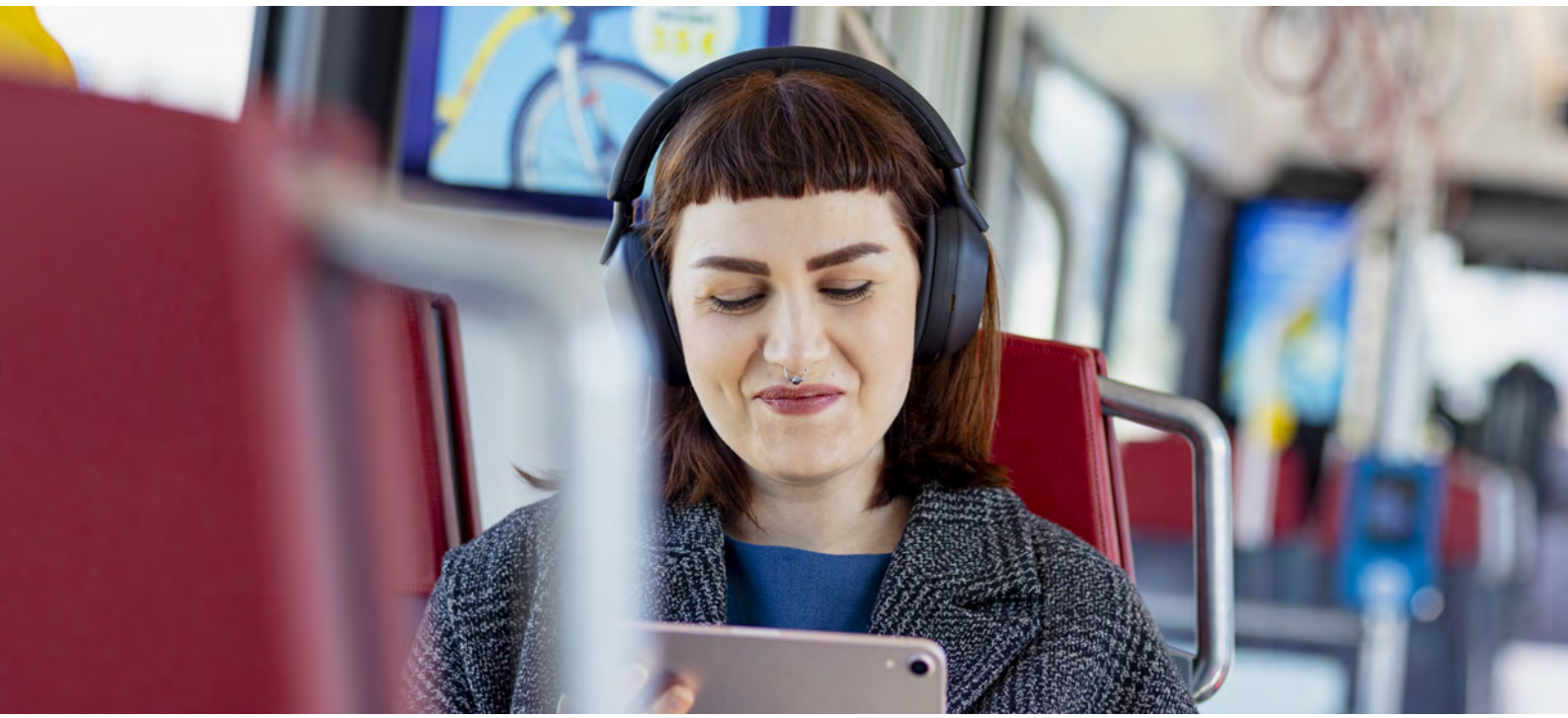
4.2 Investoinnit tietoturvaan

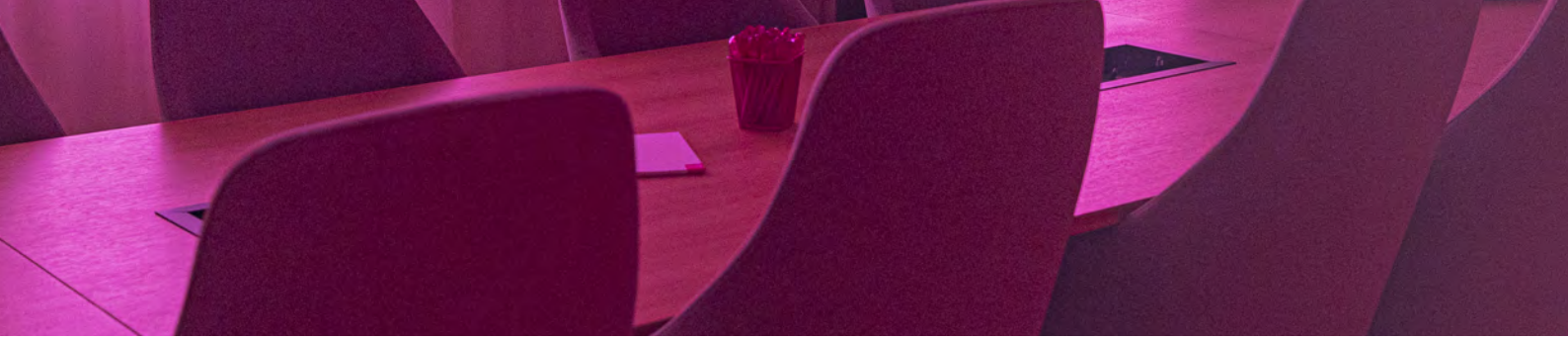
Kumppaneiden hyödyntäminen tietoturvaan ja kyberturvallisuuteen

Yritykset eivät pärjää yksinään. 89 % vastaajista ilmoitti hyödyntävänsä kumppaneita tietoturvan ja kyberturvallisuuden saralla. Mitä pienempi yritys on, sitä enemmän palveluita ostetaan kumppaneilta.

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





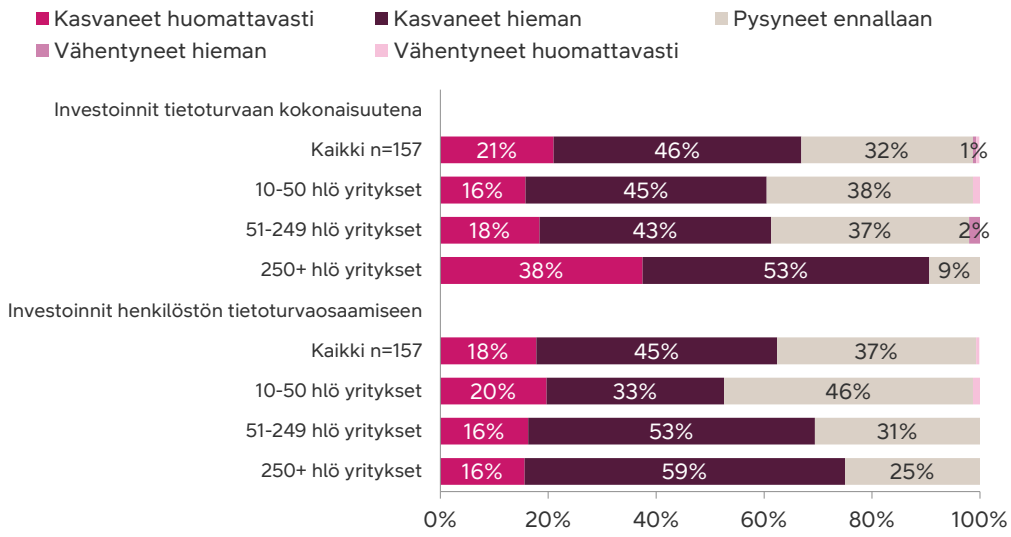


Tietoturvainvestointien kehitys viimeisen viiden vuoden aikana

67 % vastaajista kertoo, että yrityksen tietoturvainvestoinnit ovat kasvaneet viimeisen viiden vuoden aikana. Erityisesti suuret yritykset ovat kasvattaneet investointejaan. Myös tietoturvaosaamiseen on investoitu viimeisen viiden vuoden aikana paljon: yli 60 % vastanneista sanoo, että investointeja henkilöstön tietoturvaosaamiseen on lisätty.

> **Onnistunut tietoturva vaatii jatkuvaa seurantaa ja riskien arviointia muuttuvassa uhkaympäristössä.**

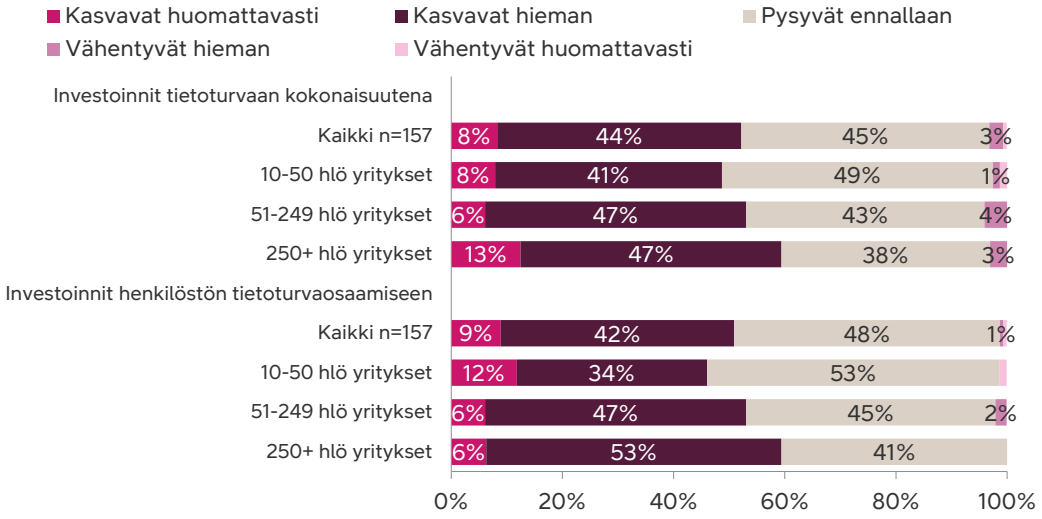
Miten yrityksesi tietoturvainvestoinnit ovat kehittyneet viimeisen viiden vuoden aikana? Vastaa tietoturvasta kokonaisuutena sekä henkilöstön tietoturvaosaamisen osalta.



Tietoturvainvestointien kehitysnäkymät vuoteen 2025

Yritysten tietoturvainvestoinnit ovat edelleen valtavassa kasvussa sekä kokonaisuutena että henkilöstön osaamisen osalta. Yritykset eivät ole juurikaan vähentämässä investointejaan tietoturvaan.

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

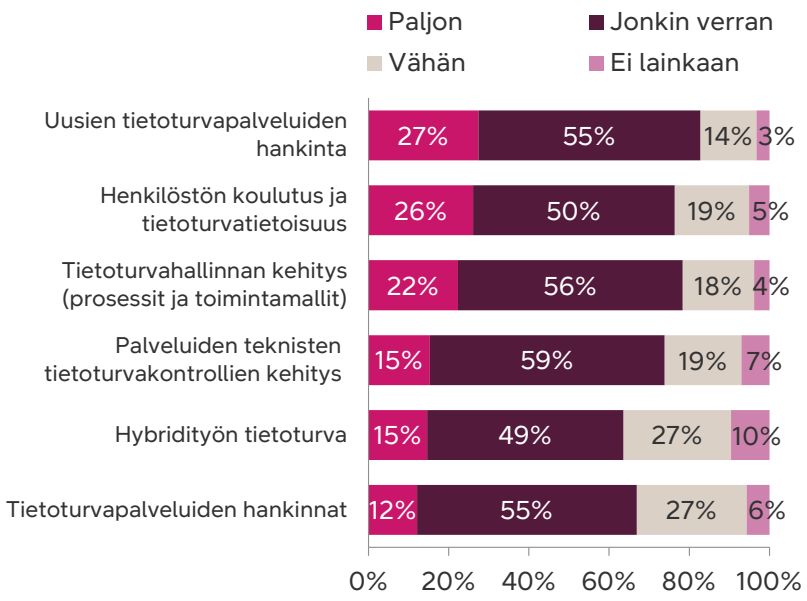


> **Tietoturvan saralla ei ole olemassa hopealuotia, eli ratkaisua, joka toimii kaikkeen.**

Panostettavat osa-alueet seuraavan vuoden aikana

Vastaajayritykset tulevat panostamaan seuraavan vuoden aikana moninaisesti tietoturvan eri osa-alueisiin. Suuremmilla yrityksillä panostustarve on luonnollisesti korkeampi muun muassa suuremman henkilöstömäärän vuoksi. Kuitenkin myös suuri osa pienistä yrityksistä tekee jonkin verran toimenpiteitä, esimerkiksi hankkimalla uusia tietoturvapalveluita ja panostamalla tietoturvahallinnan kehitykseen.

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



4.3 Analyysi: ”Tietoturvan rakentaminen on kuin maraton”, neuvoo asiantuntija

Tutkimuksen tuloksista selvisi, että yritykset ovat tällä hetkellä eniten huolissaan nousevasta uhasta Venäjältä, tietomurroista, tietojenkalastelusta sekä palvelunestohyökkäyksistä. Verkko- ja pilvipalveluiden liiketoimintajohtaja Kaapro Kanto jakaa näkemyksiään uhilta suojautumiseen ja tietoturvainvestointeihin. Miten oman yrityksen suojausta kannattaa lähteä rakentamaan?

73 prosenttia kyselytutkimukseen vastanneista IT-päättäjistä on huolissaan yritysten kyberturvallisuudesta. Huoli korostuu sitä mukaa, mitä suurempi yritys on kyseessä. Siksi ei ole yllättävää, että tulosten mukaan myös tietoturvainvestoinnit ovat kasvaneet ja näyttävät jatkavan kasvua myös tulevaisuudessa.

”Uhkakenttä maailmalla kehittyy todella nopeassa tahdissa. Tutkimuksessa päättäjät tunnistavat Venäjän uhan ja kyberrikollisuuden. Hyökkääjät voivat keskittyä yksittäiseen keinoon, mutta hyökkäykseltä puolustautuva organisaatio joutuu suojautumaan kaikilta mahdollisilta uhilta. Tämä tarkoittaa sitä, että tietoturvaa suojaavat toimenpiteet kasvavat erilaisten nousevien uhkien myötä”, selvittää DNA:n yrityspuolen verkko- ja pilvipalveluiden liiketoimintajohtaja **Kaapro Kanto**.

Kanto alleviivaa, että tietoturvainvestointien kohdalla yritysten kannattaa tehdä monivuotissuunnitelmia: on tärkeää ymmärtää yrityksen toimintaympäristön uhat ja priorisoida investointeja – kaikkeen kun ei voi, eikä kannata, investoida kerralla.

”Tietoturvan saralla ei ole olemassa hopealuotia, eli ratkaisua, joka toimii kaikkeen. Tietoturvan rakentaminen ja siihen tehtävät investoinnit ovat pitkä projekti. Tietoturvaan kannattaa suhtautua kuin maratoniin, jonka maasto tulee muuttumaan matkan varrella. Koska suunnitelmiin tulee muutoksia ja uudenlaisia päivitystarpeita, hyvät kumppanit ja osaajaverkosto ovat äärimmäisen tärkeä osa jokaisen yrityksen suojautumista.”

Hybridityön ja tekoälyn huomiointia petrattava tietoturvassa

Hybridityön mukanaan tuomat uudet käytänteet ja tekoälytyökalujen käyttö nousivat myös tutkimuksessa esille. Jopa 64 prosenttia vastanneista on täysin tai osittain samaa mieltä siitä, että hybridityö on yrityksille tietoturvariski. Kannon mielestä yritysten tulisi petrata varautumistaan hybridityön saralla.

”Useissa yrityksissä etätyöhön ja etätyön turvallisuuteen ei ole panostettu riittävissä määrin. Kotikonttorilla tehtävissä töissä käytetään vanhanaikaisia kontrolleja, kuten vain salasanoja tiettyihin sovelluksiin tai tietoihin pääsemiseksi, vaikka kaksivaiheinen tunnistautuminen olisi ehdottoman tärkeää suojauksen kannalta.”

Lähes kaikkien kyselyyn vastanneiden päättäjien mielestä tekoälytyökalujen tietoturvaohjeistus on puutteellista. Suurimman osan mielestä työntekijöiden käyttämien työkalujen hyödyntämistä on vaikea hallita, ja siksi liikesalaisuuksia voi päätyä vääriin käsiin. Tämän lisäksi vain joka kolmannella yrityksellä on säännöt ja linjaukset tekoälyn käyttöä varten.

”Kannustan jokaista yritystä pitämään huolta, että tekoälyn ja tekoälytyökalujen käyttöä ohjaavat selkeät periaatteet. Periaatteiden tulisi olla linjassa kaikkien muiden käytänteiden kanssa aina tietoturvasta erilaisiin käyttötapauksiin. Yrityksillä olisi hyvä olla tekoälytyöryhmä, jossa hyödynnetään tekoälyosaamista sekä lainsäädännön tuntemista turvallisten ohjeiden luomiseksi. Tämän lisäksi olisi hyvä myös listata sallitut työkalut, Kanto sanoo.

Tietoturvainvestoinnit haastavat yrityksiä

Tietoturvaan investoiminen on haastavaa, koska uhat kehittyvät jatkuvasti ja organisaatioiden on vaikea pysyä ajan tasalla uusimmista hyökkäystavoista. Tutkimuksen mukaan yrityksistä kuitenkin löytyy investointikykyä ja -halua, mutta osaajapula jarruttaa tietoturvan kehitystä.

Tämän lisäksi tietoturvatoimenpiteet voivat olla kalliita ja vaativat jatkuvaa ylläpitoa, mikä tekee kustannusten ja hyötyjen arvioinnista hankalaa. Tietoturvan hankintakriteerit ovat moninaisia: hinta on luonnollisesti useimmiten mukana hankintapäätöstä tehtäessä, mutta sitä arvioidaan suhteessa laatuun, luotettavuuteen ja palveluun.

”Tietoturvassa halvalla voi todella saada hyvää, mutta silloin on yleensä onnistuneesti osattu kiinnittää huomiota kokonaisratkaisuun. Liian usein organisaatiot ostavat yksittäisiä tietoturvapalveluita, jotka yritetään sovittaa osaksi tietoturva-arkkitehtuuria. Tällöin yksittäiset komponentit ratkaisevat yksittäisiä ongelmia. Näissä tilanteissa yleensä 10 edullista ratkaisua tulee hintavammaksi kuin yksittäinen isompi kokonaisuus”, Kanto alleviivaa.

Yritysten on tasapainoteltava liiketoiminnan joustavuuden ja tietoturvan tiukkuuden välillä, jotta ne eivät vaaranna toimintakykyään. Investoinneissa on huomioitava sekä tekniset ratkaisut että henkilöstön kouluttaminen, sillä ihmisten toiminta on usein tietoturvan heikoin lenkki.

”Onnistunut tietoturva vaatii jatkuvaa seurantaa ja riskien arviointia muuttuvassa uhkaympäristössä”, Kanto tiivistää.

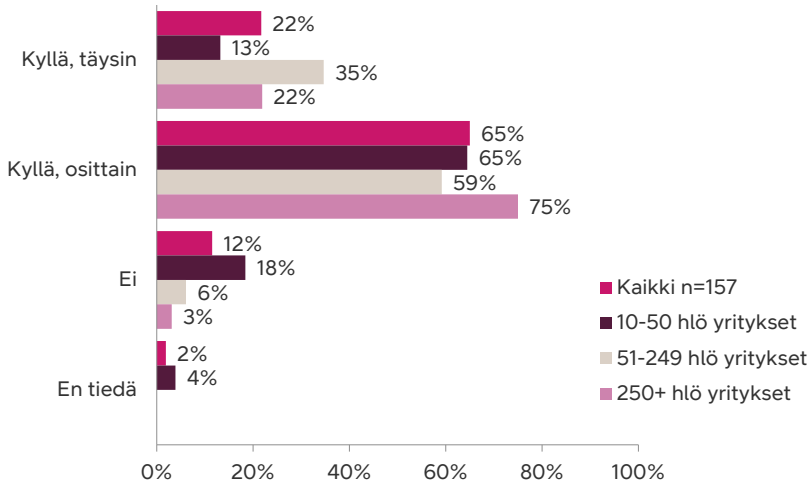
4. Tutkimustulokset

4.4 Varautuminen

Valmiudet varautua kyberuhkiin

Tutkimukseen vastanneista ICT-päättäjistä suurin osa kokee, että yrityksessä on riittävät valmiudet varautua nykyiseen kyberuhkatilanteeseen. Kuitenkin vain 22 % vastaajista kokee, että hänen edustamansa yritys pystyy täysin varautumaan uhkiin. Epävarmimpia varautumisestaan ovat pienet, 10–50 henkilön yritykset.

Koetko, että yrityksessäsi on riittävät valmiudet varautua nykyiseen kyberuhkatilanteeseen?



NIS2-direktiivi

Tietoisuus uudesta NIS2-kyberturvadirektiivistä on ajankohtaan* nähden matalalla tasolla. Vastanneista ICT-päättäjistä jopa 42 % ei tiedä, täytyykö yrityksen noudattaa NIS2-direktiivin mukaista paikallista lainsäädäntöä.

Uuden NIS2-kyberturvadirektiivin noudattaminen nähdään myös yrityksissä haastavana. Vain 15 % niistä, jotka vastasivat direktiivin velvoittavan yritystään, sanoo yrityksen yltävän täysin vaadittuun tasoon direktiivin soveltamista koskevaan määräaikaan mennessä. 59 % direktiivin piiriin kuuluvista vastaajista kertoo kuitenkin, että tulee pääsemään vaadittavaan tasoon osittain.

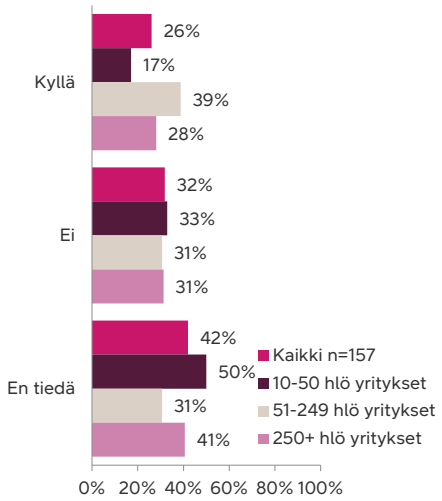
*EU:n ja sen jäsenvaltioiden kansallista kyberturvaa yhtenäistävän NIS2-direktiivin soveltaminen alkoi 18.10.2024. Suomessa kyberturvallisuuslaki on vielä eduskunnan käsittelyssä. Lailla pannaan kansallisesti täytäntöön NIS2-direktiivin vaatimukset. Tutkimus on toteutettu syyskuussa 2024.

NIS2-direktiivi

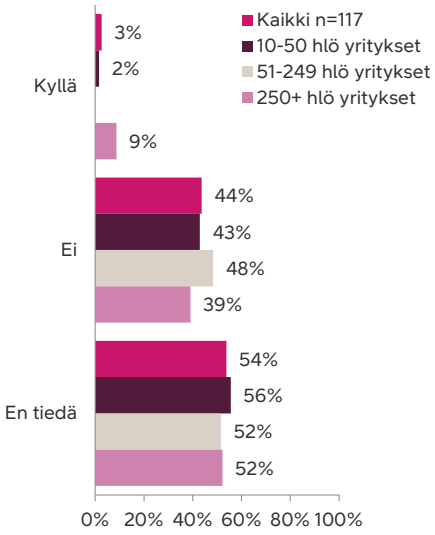
NIS2-kyberturvallisuusdirektiivissä määritellään kyberturvallisuusriskien hallintatoimenpiteiden ja raportointivelvoitteiden vähimmäistaso kaikilla direktiivin soveltamisalaan kuuluvilla toimialoilla. Astuessaan voimaan se koskee kriittisillä aloilla toimivia organisaatioita 50 henkilöä tai enemmän työllistävistä yrityksistä, jos niiden liikevaihto on yli 10 miljoonaa euroa. Jos henkilöstöä on 250 tai enemmän, organisaatio kuuluu automaattisesti NIS2:n soveltamisalaan.

Direktiivi asettaa toimijoille uuden minimitason kyberturvallisuusriskien vastuuseen alihankkijoita myöten ja lisää raportointivelvoitteita. Lisäksi yritysten täytyy kehittää perustason kyberhygieniakäytäntöjä ja panostaa kyberturvallisuuskoulutukseen.

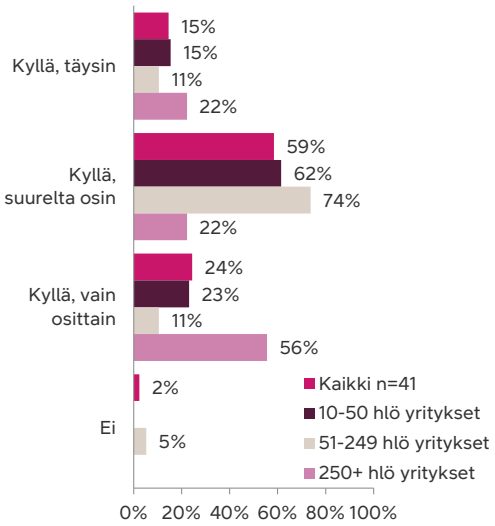
Täytyykö yrityksesi noudattaa eurooppalaisen NIS2-direktiivin mukaista paikallista lainsäädäntöä kyberresilienssin parantamiseksi?



JOS KYLLÄ Tuleeko yrityksesi yltämään NIS2-direktiivin vaatimaan tasoon lokakuuhun 2024 mennessä? n=41



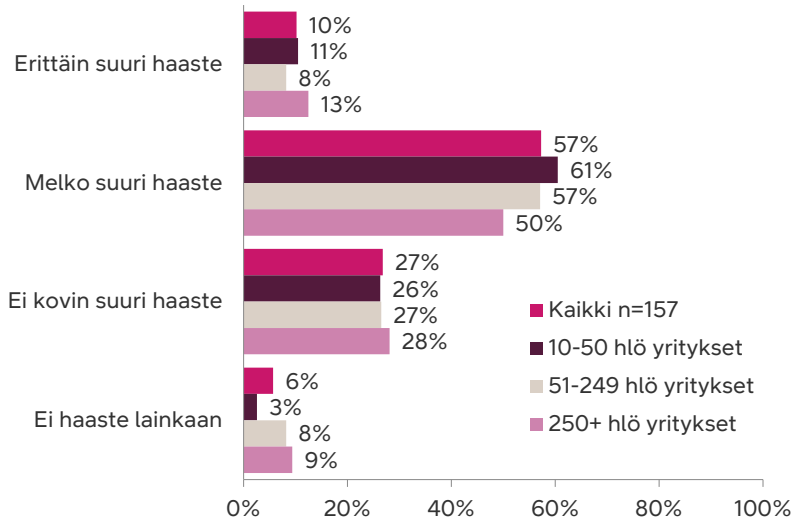
JOS EI TAI EN TIEDÄ Vaikuttaako NIS2-direktiivi yrityksesi toimintaan esimerkiksi alihankkijan roolissa? n=117



Osaajapulan vaikutus kyberturvatasoon

Osaajapula koetaan haasteeksi: 67 % vastaajista nimeää osaajapulan haasteeksi hyvän kyberturvan saavuttamisessa. Saman haasteen kanssa kamppailevat kaikenkokoiset yritykset.

Kuinka merkittävä haaste osaajapula on mielestäsi hyvän kyberturvatason saavuttamiseksi?

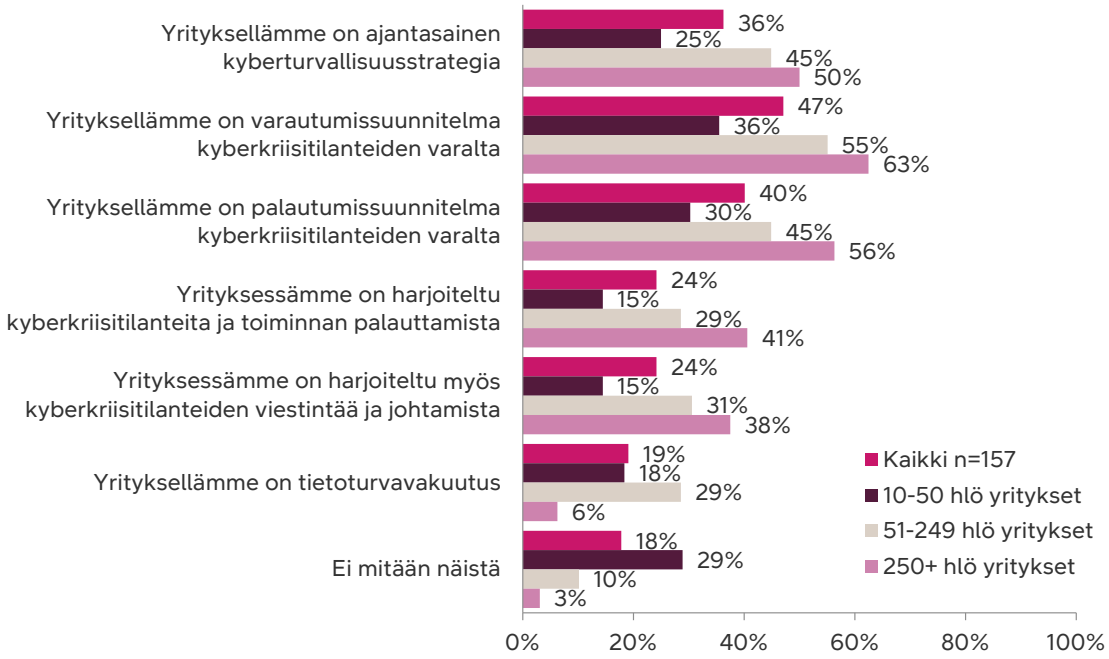


> **Hyvät kumppanit ja osaajaverkosto ovat äärimmäisen tärkeä osa jokaisen yrityksen suojautumista.**

Varautumisen toimenpiteet

Vain puolella yli 250 henkilöä työllistävistä yrityksistä on ajantasainen kyberturvallisuusstrategia. Hieman useammalla on kuitenkin varautumissuunnitelma. Kuitenkaan yli puolella yrityksistä ei ole varautumissuunnitelmaa kyberkriisitilanteiden varalle. Mitä pienempi yritys on, sen harvinaisempaa on uhkiin varautuminen. Vain yksi neljästä yrityksestä harjoittelee kyberkriisitilanteita varten, ja vain viidenneksellä yrityksistä on tietoturvavakuutus.

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



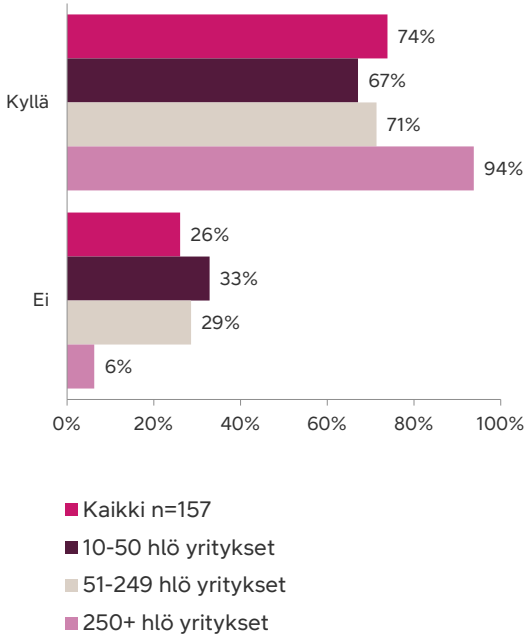
4. Tutkimustulokset

4.5 Hydridityö ja tekoäly

Hybridityön tekeminen

Suuremmissa yrityksissä tehdään enemmän hybridityötä kuin pienemmissä. Yli 250 henkilöä työllistävissä yrityksissä hybridityötä tehdään lähes kaikissa (94 %). Vähiten (67 %) hybridityötä tehdään 10–50 henkilöä työllistävissä yrityksissä.

Tehdäänkö yrityksessänne hybridityötä?

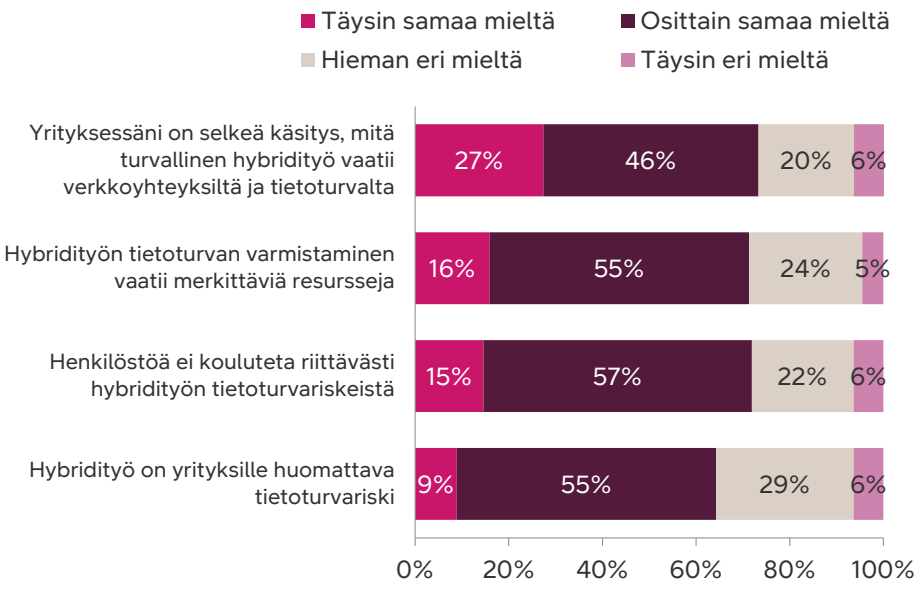


Hybridityö ja tietoturva

Hybridityö on tuonut yrityksiin lisää resurssitarvetta sekä synnyttänyt uudenlaisia uhkia. Riski kasvaa henkilöstömäärän mukana – mitä enemmän työntekijöitä on, sitä suurempi on myös riski. Toisaalta pienemmät yritykset ovat resurssien osalta suuremmassa paineessa, sillä resursseja on ennestäänkin vähemmän.

Suurella osalla yrityksistä on selkeä käsitys hybridityön tietoturvavaatimuksista. Hybridityötä pidetään huomattavana riskinä, mutta samalla koetaan, ettei henkilöstön kouluttaminen ole riittävällä tasolla.

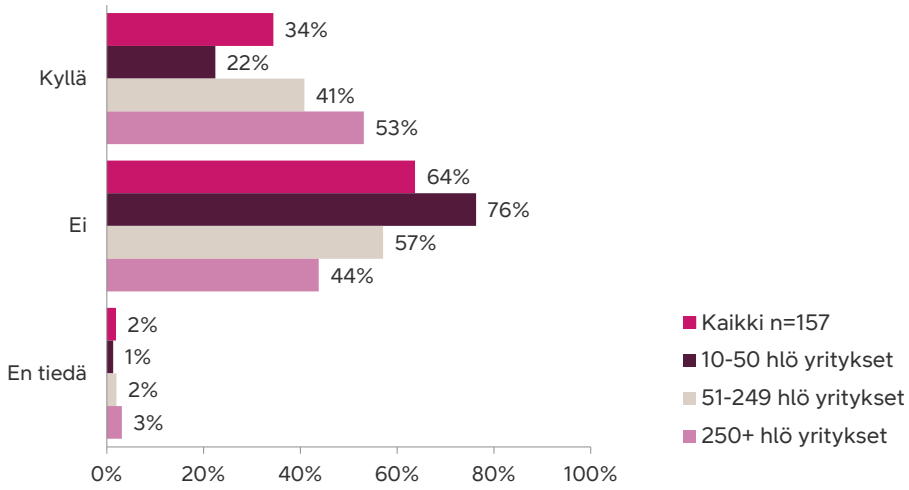
Kuinka hyvin seuraavat väittämät pitävät mielestäsi paikkansa?



Tekoälyn käytön säännöt ja linjaukset

Vain kolmannes yrityksistä on tehnyt säännöt ja linjaukset henkilöstölle tekoälyn käytöstä. Nämä linjaukset ovat todennäköisemmin kunnossa suurilla kuin pienillä yrityksillä. Silti vain puolella yli 250 henkilöä työllistävistä yrityksistä löytyy olemassa olevat linjaukset.

Onko yrityksessänne tehty säännöt ja linjaukset henkilöstölle AI:n eli tekoälyn käyttöön liittyen?

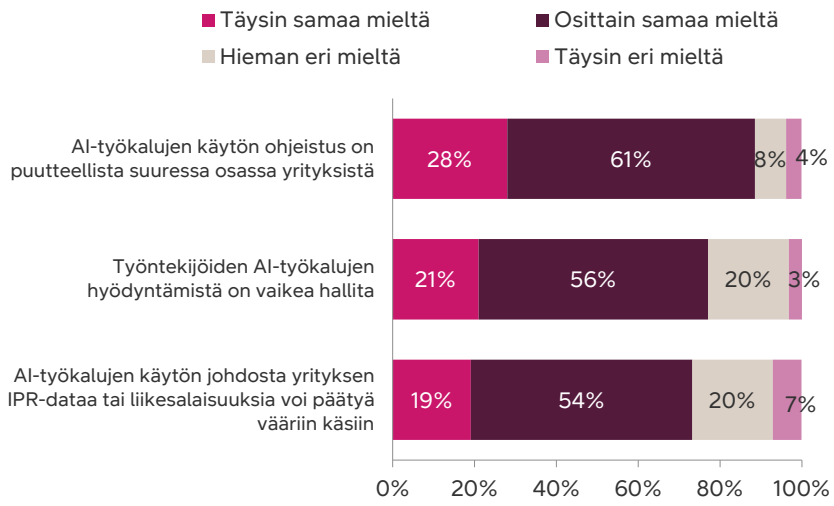


Tekoäly ja tietoturva

Lähes kaikkien ICT-päättäjien mielestä tekoälytyökalujen ohjeistus on puutteellista suuressa osassa yrityksiä. Suurimman osan mielestä työntekijöiden tekoälytyökalujen hyödyntämistä on vaikea hallita, ja siksi liikesalaisuuksia voi päätyä vääriin käsiin. Luonnollisesti mitä enemmän henkilöstöä on, sitä vaikeampaa on myös työkalujen hallinta.

> **Kannustan jokaista yritystä pitämään huolta, että tekoälyn ja tekoälytyökalujen käyttöä ohjaavat selkeät periaatteet.**

Kuinka hyvin seuraavat väittämät pitävät mielestäsi paikkansa?



Kyberturvan kulmakivet: Näistä osista rakentuu toimiva tietoturvakokonaisuus

Yritysten kohtaamat kyberuhat ovat moninaisia ja kehittyvät jatkuvasti, mikä tekee tehokkaista tietoturvaratkaisuista välttämättömiä. Onneksi tarjolla on laaja kirjo tuotteita ja palveluita, jotka auttavat yrityksiä suojautumaan. Näihin ratkaisuihin kuuluvat muun muassa kehittyneet palomuurit, pilvipohjaiset tietoturvaratkaisut, haittaohjelmien torjuntajärjestelmät sekä henkilöstön tietoturvakoulutukset.

Tutkimus osoittaa, että ICT-päättäjien mielestä yritysten tietoturvan tasossa olisi parantamisen varaa, vaikka tietoturvainvestoinnit ovat kasvaneet viime vuosina merkittävästi. Yritysten kannattaa aloittaa kattavan kyberturvan rakentaminen riskien arvioinnilla ja nykyisen tietoturvatason kartoituksella. Ensimmäinen askel on tunnistaa yrityksen liiketoimintakriittisimmät tiedot ja järjestelmät sekä niiden suojaustarpeet. Tätä kaikkea kutsutaan varautumiseksi.

”Varautuminen on tärkeää, jotta yritys osaa ennakoida tuntemattomat liiketoimintahäiriöt. Jos yrityksen toiminta on missään määrin aikakriittistä, on parasta olla jonkunlainen suunnitelma siitä, miten toimitaan, kun jotain yllättävää tapahtuu. Kyberkriisejä ja niiden hallintaa kannattaa harjoitella vähintään työpöytäharjoituksena. Tästä voi sitten edetä järeämpiin simulaatioihin”, kertoo **Kaapro Kanto**.

Kartoituksen ja varautumisen katselmoinnin jälkeen on syytä varmistaa perusasioiden, kuten palomuurien, virustorjunnan ja ajantasaisten ohjelmistopäivitysten, olevan kunnossa. Monivaiheinen tunnistautuminen ja vahvat salasanakäytännöt ovat helppoja mutta tehokkaita keinoja parantaa tietoturvaa.

”Yleinen tietoturvaosaaminen ja trendien seuraaminen on tärkeintä – jokaisella yrityksellä ei ole pakko olla palkkalistoillaan tietoturvapomoa. Hyvät kumppanit auttavat tietoturvan saralla pitkälle. Myös koko henkilöstön koulutus ja tietoisuuden lisääminen ovat erittäin olennaisia asioita”, toteaa Kanto.

Millaisella tietoturvapalveluiden varustustasolla suurin osa yrityksistä sitten pärjää? Tärkeimpiä teknisiä ratkaisuja ovat muun muassa:

- **Päätelaitteiden tietoturva** suojaa tietokoneet, tabletit, matkapuhelimet ja palvelimet tietomurroilta sekä haittaohjelmilta.
- **Pääsynhallinta** luo käyttäjille yhden sähköisen identiteetin, jolle voidaan sallia työtehtävien kannalta tarkoituksenmukaiset pääsyoikeudet yrityksen verkkoon ja tietojärjestelmiin.
- **Suojattu VPN-palvelu** avaa työntekijöille tietoturvallisen VPN-etäyhteyden yrityksen palveluihin ja tietoihin myös etätyöpisteeltä.
- **Kaksivaiheinen tunnistautuminen** parantaa etäyhteyden tietoturvaa, sillä kirjautuminen tulee vahvistaa salasanan lisäksi toisella tavalla.
- **Managed SASE** yksinkertaistaa merkittävästi monipaikkaisen hybridityön turvallisuutta ja hajallaan olevien pilvipalveluiden hallintaa.
- **Älykäs palomuuripalvelu** puolestaan varmistaa, että jokainen internet-, pilvi- ja yritysverkkoyhteys on turvallinen.
- **Palvelunestohyökkäyksiltä (DDoS) suojautuminen** turvaa yrityksesi digitaaliset palvelut tahalliselta ylikuormitukselta tai kaatumiselta.

Kyberturvan rakentaminen on iso ja tärkeä prosessi, joka vaatii teknisiä ratkaisuja ja suunnitelmallisuutta. Toimintavarma tietoturva syntyy ennakoinnista, oikeiden kumppaneiden valinnasta ja arjen prosessien sujuvasta integroinnista tietoturvakäytäntöihin.

Miten aloittaa matka kohti tietoturvallisempaa arkea?
Tutustu kattaviin tietoturvapalveluihimme ja ota yhteyttä!

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 3,7 miljoonaa matkaviestin- ja kiinteän verkon liittymäasiakkuutta. Vuonna 2023 liikevaihtomme oli 1 067 miljoonaa euroa ja yhtiössä työskentelee noin 1 700 henkilöä ympäri Suomea.

DNA on osa Telenoria, joka on Pohjoismaiden johtava tietoliikenneyhtiö. 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