

Telia Tietoturva- tutkimus 2023

Tutkimusraportti
Yritykset ja julkishallinto

Sisällys

Toimitusjohtajan alkusanat	5
Tutkimusraportti: Yritykset ja julkishallinto	7
1. Tutkimusprojektin tavoite ja toteutus	8
2. Tämänhetkinen turvallisuuden tunne	13
3. Digiturvallisuuden tärkeys ja siihen liittyvät uhkat	17
4. Digitaaliseen turvallisuuteen liittyvät ratkaisut	27
Ota yhteyttä	36



Yrityspäätäjien mielestä
tietoliikenneverkkojen
kotimaisuuden merkitys
on noussut keskeiseen
asemaan digitaalisen
turvallisuuden kivijalkana.



Kyberturvallisuus huolestuttaa yrityspäättäjiä Nato-Suomessa

Katkenneita kaasuputkia ja tietoliikennekaapeleita, välineellistettyä maahanmuuttoa ja jatkuvaa uhkailua – mitä seuraavaksi? Ei ihme, että suomalaisyritykset nostavat yhteiskuntaa lamauttavat kyberhyökkäykset uhkakuvien kärkeen.

Vuosittaisen ison turvallisuustutkimuksemme tulokset ovat jälleen hätkähdyttävää luettavaa. Kun Venäjä aloitti kaksi vuotta sitten julman hyökkäyssodan Ukrainaan, turvallisuudesta tuli yhdessä yössä kestopuheenaihe niin julkisessa keskustelussa kuin suomalaistutkimuksissa.

Turvalliset ja luotettavat tietoliikenneyhteydet ovat yrityksille elinehto. Koko yhteiskunta pyörii vuosi vuodelta enemmän niiden varassa, mikä näkyy vahvasti myös turvallisuustutkimuksemme tuloksissa. Ja nimenomaan kyberhyökkäyksillä tätä kriittistä, digitaalista infrastruktuuria yritetään horjuttaa.

Mikä sitten avuksi?

Yrityspäättäjien mielestä tietoliikenneverkkojen kotimaisuuden merkitys on noussut keskeiseen asemaan digitaalisen turvallisuuden kivijalkana. Jopa puolet

suomalaisyrityksistä sanoo, että kotimaisten tietoliikenneverkkojen merkitys on nyt tärkeämpää kuin vuosi sitten.

Samaan aikaan on huolestuttavaa, että yrityspäättäjistä 40 prosenttia ajattelee, ettei yhteiskunta ole varautunut kyberhyökkäyksiin riittävästi. Siinä on työsarjaa meille digitaalisesta huoltovarmuudesta vastaaville yrityksille.

Me teimme oman ratkaisumme jo vuosia sitten, kun päätimme, että paras tapa pitää huolta mobiiliverkkojen turvallisuudesta on rakentaa ne yhdessä Nokian kanssa. Sitä päätöstä ei ole tarvinnut katua, päinvastoin.

Tämä opas kertoo yksityiskohtaisesti, miten suomalaisyritykset ja julkishallinto kokevat turvallisuutensa tällä hetkellä ja miten ne aikovat selviytyä vanhoista ja uusista haasteista.

Digiturvallisia lukuhetkiä!

Heli Partanen
toimitusjohtaja
Telia Finland





Tutkimusraportti: Yritykset ja julkishallinto

1. Tutkimuksen tavoite ja toteutus

Tietoturva ja turvallisuus ovat nousseet yleisiksi puheenaiheiksi, sillä tietoturvallisuuteen liittyvät asiat herättävät paljon kiinnostusta, huolta, pelkoa sekä kysymyksiä.

Tämän tutkimuksen tavoitteena on tuottaa ymmärrystä, mitä ajatuksia tietoturva ja turvallisuus herättävät yritysten ja julkishallinnon taholla.

Tarkoituksena on valottaa, miten eri tahot suhtautuvat tietoturvaan sekä millaisia ratkaisuja alan toimijoilta odotetaan.

Tutkimusmetodina oli kvantitatiivinen tutkimus yritysten ja julkishallinnon keskuudessa, ja kyselyn on toteuttanut Kantar.

	Osio 1: Yritykset 	Osio 2 : Julkishallinto 
Kohderyhmä	Suomalaisten väh. 5 hlön yritysten liiketoimintajohto, toimitusjohtaja, yrittäjä.	IT- ja liiketoimintajohtoa valtion-, alue- ja paikallishallinnossa.
Vastaajamäärä	N=253	N=82
Tiedonkeruu	Puhelinhaastattelu Kantarin BtoB-haastattelijoiden toimesta 2.11-14.12.2023	Puhelinhaastattelu Kantarin BtoB-haastattelijoiden toimesta 3.11-12.12.2023
Datakäsittely	Painotettu vastaamaan yrityskoko-jakaumaa yksityisellä sektorilla.	Ei painotusta.



Yhteenveto

	Yritykset 	Julkishallinto 
Millainen on kohderyhmän suhde tietoturvaan?	Digitaalinen turvallisuus on tärkeä aihe suomalaisille yrityksille. Mitä suurempi yritys on, sitä tärkeämpänä digitaalisen turvallisuuden merkitystä painotetaan. Vaikka yritykset ovat varmoja kyvykkyydestään tunnistaa digiturvallisuuteen liittyviä uhkia, viidennes suurista yrityksistä epäilee valmiuksiaan tunnistaa uhkia. Suurin osa yrityksistä on varautunut jollain keinoin tietojen kalasteluun ja henkilötietovarkauksiin kohdistuviin uhkiin, mutta pienimmät yritykset ovat muita harvemmin ryhtyneet toimiin tai hankkineet palveluita suojautuakseen uhkilta.	Digitaalinen turvallisuus on ainakin melko tärkeä asia käytännössä kaikille julkishallinnon aloille. Hyvin harva epäilee organisaation valmiuksia tunnistaa digiturvallisuuteen liittyviä uhkia ja oman organisaationsa kyvykkyydestä ollaan varmoja eri hallinnon tasoilla ja tehtävissä. Enemmistö kokee oman organisaation digitaalisen turvallisuuden olevan jopa paremmalla tasolla kuin aiemmin ja juuri kukaan ei koe tilanteen heikentyneen. Operaattoreiden katsotaan yleisesti hoitavan hyvin yhteysien digiturvallisuushkien ennaltaehkäisyn – tosin moni ei osaa sanoa miten asianlaita on.
Mitkä asiat liitetään tietoturvaan?	Tietoliikenneverkot ovat erittäin tärkeä osa digiturvallista yhteiskuntaa ja verkkoteknologian kotimaisuudella on suuri merkitys yrityksille. Verkon kotimaisuutta arvostetaan, mutta vielä tärkeämpää on verkon infrastruktuurin sijaitseminen Suomessa. Digitaalisen turvallisuuden ratkaisut ovat yleisimmin budjetoitu osaksi IT-budjettia, ja suuryrityksillä on usein oma budjettinsa tähän. Suurimmat yhteiskunnalliset uhkakuvat liittyvät talousnäkyymiin, kyberhyökkäyksiin ja pakolaistulvaan – eikä näihin olla varauduttu riittävästi, toisin kuin esimerkiksi sotaan tai epidemioihin. Sota koetaan myös merkittävänä uhkana, tosin osan mielestä siihen on jo osattu varautua kylliksi.	Tietoliikennetyhteyksien verkkoteknologian kotimaisuudella on vahva merkitys julkishallinnolle. Myös kotimaista verkkoa arvostetaan, mutta erityisen tärkeää on verkkoinfrastruktuurin sijaitseminen Suomessa – yhdessä näiden katsotaan olevan erittäin tärkeä osa digiturvallista yhteiskuntaa. Varautuminen on tärkeää ylläpidettäessä tietoturvallista ympäristöä. Lähes kaikki organisaatiot ovat varautuneet joillakin keinoin uhkiin, kuitenkin palveluratkaisujen ostaminen on vähemmän yleistä kuin muu varautuminen. Digitaalisen turvallisuuden ratkaisut ovat yleisimmin budjetoitu osaksi IT-budjettia. Näin on tilanne etenkin paikallishallinnon osalta.
Mitä ovat konkreettiset tietoturvaan liittyvät huolet ja ratkaisut?	Digitaalisen turvallisuuden suurin uhkakuva liittyy tietomurtoihin. Kyberuhat ja muut haittaohjelmiin ja huijauksiin liittyvät riskit mietittyvät laajasti. Huolet palvelunestohyökkäyksistä ovat hälventyneet. Lähes joka kolmas yrityksistä on kohdannut tietojen kalasteluun tai henkilötietovarkauksiin kohdistuvia uhkia – suurempien yritysten kohdalla todennäköisemmin tapauksia on ollut. Digitaalisen turvallisuuden tason katsotaan olevan ennallaan tai jopa paremmalla tasolla kuin aiemmin. Kaikki yritykset sanovat kuitenkin panostavansa tietoturva-asioihin vähintään saman verran kuin viime vuonna. Myös henkilöstön osaamiseen panostaminen on tärkeää, mutta pääsääntöisesti lisäpanostusten ei katsota olevan tarpeellisia.	Uhkakuvia tunnistetaan aktiivisesti. Kasvanut ja suurin uhkakuva liittyy tällä hetkellä kyberuhkiin, joihin riittävä varautumisen taso jakaa edustajia. Myös huolet yksilöihin ja organisaatioon liittyvien tietojen varastointiin, huijauksiin ja vakoiluun ovat kasvaneet, kun taas huolet viestintäverkkojen häiriöihin hälventyneet. Yli puolet julkishallinnon edustajista kertoo organisaation joutuneen tietojen kalastelun tai niiden yritysten kohteeksi. Yleisesti lähes kaikki organisaatiot panostavat tietoturva-asioihin enemmän kuin vuosi sitten tai vähintään saman verran kuin aikaisemmin.

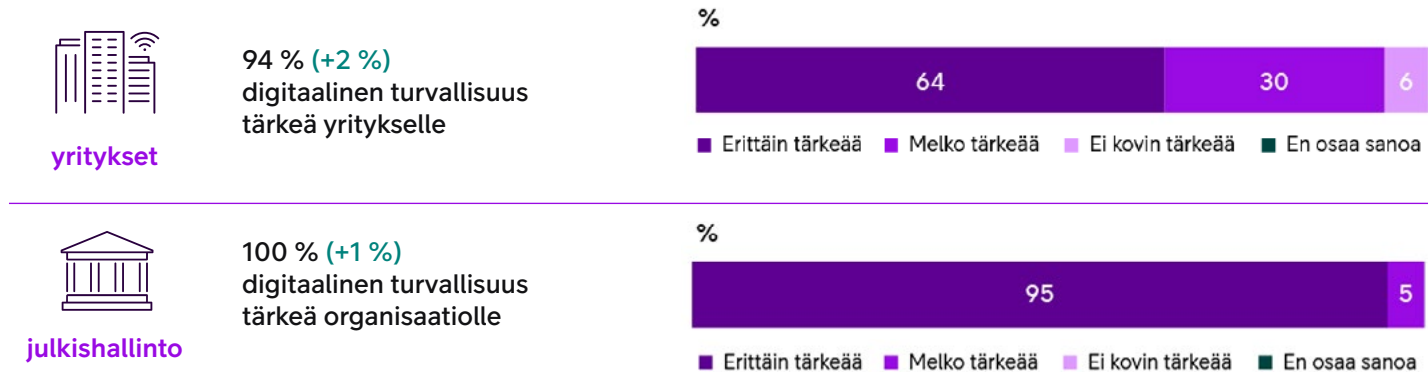
Kooste tuloksista: Oma suhde tietoturvaan

Digitaalisen turvallisuuden tärkeys:

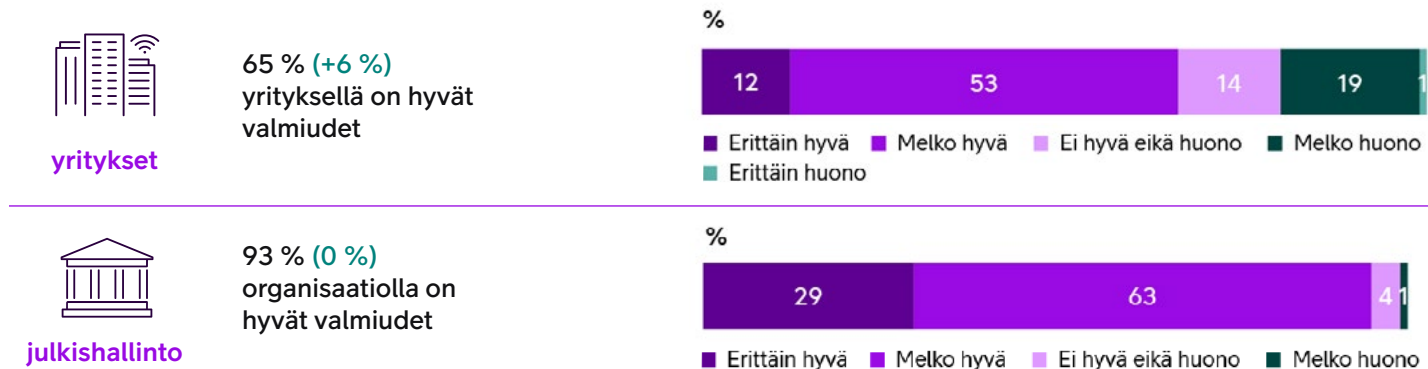
Etenkin suuret yritykset ovat varmoja kyvykkyydestään tunnistaa uhkia, kun taas pienimmät yritykset ovat muita harvemmin ryhtyneet toimiin varautuakseen tietojen kalastelun tai identiteettivarkauksien uhkaan.

Enemmistö julkishallinnon edustajista sanoo organisaation digitaalisen turvallisuuden olevan jopa paremmalla tasolla kuin aiemmin, ja hyvin harva kokee tilanteen heikentyneen.

Suluissa muutos viime vuoteen.



Valmius tunnistaa digiturvallisuusuhkia:





Kooste tuloksista: Tietoturvaan liittyvät merkittävimmät uhkakuvat

Merkittävimmät Suomeen kohdistuvat uhkat tällä hetkellä

Yritykset 	Julkishallinto 
1. Pitkittynyt taloudellinen taantuma	1. Kyberhyökkäykset
2. Kyberhyökkäykset	2. Pitkittynyt taloudellinen taantuma
3. Pakolaistulva	3. Pakolaistulva
4. Sota	4. Energian saannin ongelmat

Merkittävimmät digiturvallisuuteen liittyvät huolet

Yritykset 	Julkishallinto 
1. Tietomurrot, pankkitilin hakkerointi, maksukorttitiedot vääriin käsiin	1. Kyberuhat
2. Kyberuhat	2. Henkilö- ja yritystietoihin kohdistuvat uhat
3. Virukset ja haittaohjelmat	3. Huijausviestit / -soitot, tietojenkalastelu ja huijaukset
4. Huijausviestit / -soitot, tietojenkalastelu ja huijaukset	4. Palvelunestohyökkäykset
5. Henkilö- ja yritystietoihin kohdistuvat uhat	5. Tietomurrot, Pankkitilin hakkerointi, maksukorttitiedot vääriin käsiin

Yritykset: Yrityspuolella mitä suuremmasta yrityksestä on kyse, sitä todennäköisemmin on jo jouduttu tietojen kalastelun tai identiteettivarkauksien kohteeksi.

Julkishallinto: Lähes kaksi kolmesta julkishallinnon edustajasta kertoo organisaation joutuneen tietojen kalastelun tai niiden yritysten kohteeksi.

Kooste tuloksista: Tietoturvaan liittyvät ratkaisut

Verkkoteknologian kotimaisuuden merkitys:

Niin julkishallinnolle kuin yrityksillekin erityisen tärkeää on verkon infrastruktuurin sijaitseminen Suomessa. Suluissa muutos viime vuoteen.



yritykset

70 % (+1 %) verkkoteknologian kotimaisuudella merkitystä yritykselle



julkishallinto

67 % (+10 %) verkkoteknologian kotimaisuudella merkitystä organisaatiolle



Miksi suomalainen 5G-verkko?

Yhteiskunnan digitalisoituessa tietoturvan merkitys nousee uudelle tasolle. 5G:ssä verkon reunalle rakentuu aiempia sukupolvia enemmän dataa ja älyä, mikä luo haasteen tietoturvalle. Ratkaisevaa on tällöin ydinverkon turvallisuus, verkon ohjausjärjestelmät ja operaattorin toiminta. Verkkojen turvallisuus on operaattorin vastuulla, mutta yksi tärkeä tekijä turvallisuuden varmistamisessa on luotettavien kumppaneiden valinta.

Yksi seuraus turvallisuuden painottamisesta on se, että Telia on valinnut kotimaisen Nokian mobiiliverkkojen toimittajaksi Suomessa. Nokia toimii myös Telialle ja DNA:lle mobiiliverkkoja Pohjois- ja Itä-Suomessa rakentavan Suomen Yhteisverkon kumppanina, eli Telian asiakkaat surffaavat jatkossa aina Nokian tekniikalla rakennetuissa verkoissa.



2. Tämänhetkinen turvallisuuden tunne

Oma turvallisuuden tunne

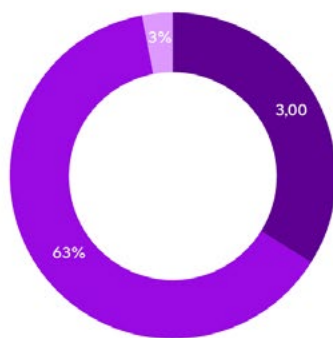
Yksityisellä sektorilla lähes jokainen tuntee olonsa turvalliseksi. Pohjois- ja Itä-Suomessa luku on hieman matalampi: noin yhdeksän kymmenestä tuntee olonsa turvalliseksi. Julkishallinnossa olo tunnetaan turvalliseksi

– joko erittäin tai melko turvalliseksi. Aluehallinnossa ja hyvinvointialueilla turvallisuudentunne on hieman jakaantuneempaa, kuin muilla hallinnon tasoilla.

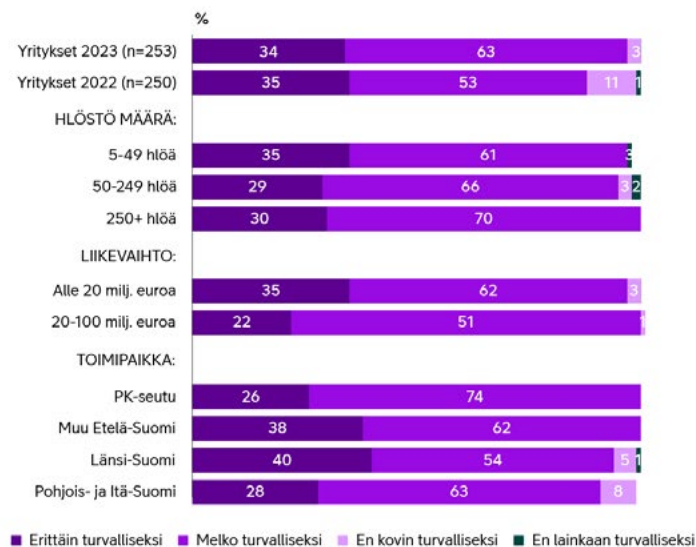
Yritykset



Kun ajattelette yritystänne juuri nyt, niin kuinka turvalliseksi tunnette olonne tällä hetkellä? (n=253)



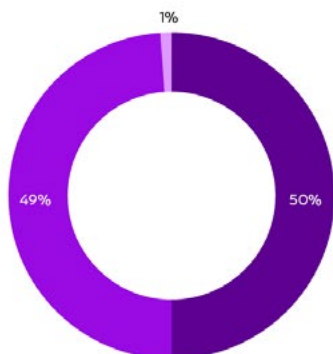
■ Erittäin turvalliseksi
■ Melko turvalliseksi
■ En kovin turvalliseksi
■ En lainkaan turvalliseksi
■ En osaa sanoa



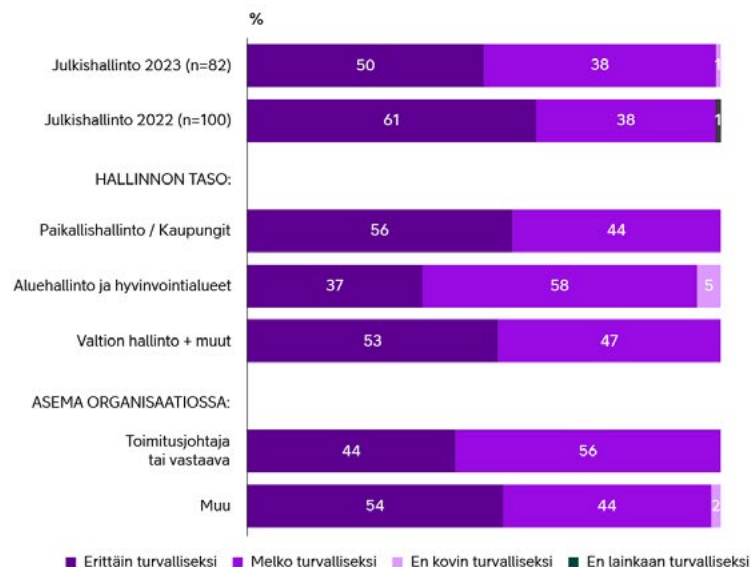
Julkishallinto



Kun ajattelette organisaatiotanne juuri nyt, niin kuinka turvalliseksi tunnette olonne tällä hetkellä? (n=82)



■ Erittäin turvalliseksi
■ Melko turvalliseksi
■ En kovin turvalliseksi
■ En lainkaan turvalliseksi
■ En osaa sanoa



Monen yrityksen tulevaisuudenusko horjuu markkinoiden epävakauden ja arvaamattoman maailmantilanteen vuoksi.

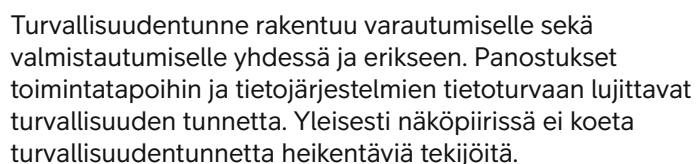
Turvallisuudentunteeseen vaikuttavat tekijät

Turvallisuudentunnetta on rakennettu varautumalla uhkiin, kuten panostamalla ajantasaisiin järjestelmiin ja prosesseihin, sekä solmimalla kumppanuuksia tietoturvan osalta. Osaava ja tiedostava henkilöstö lujittaa luottamusta turvalliseen päivittäiseen toimintaan. Turvallisuudentunnetta lujittaa myös

kuuluminen isompaan konserniin, ja luottamus yhteiskuntaan. Vaikka toiminta koetaan turvalliseksi, ymmärretään, että tilanteet voivat muuttua ja heiketä nykyisestä. Luottamusta tulevaan nakertaa arvaamaton maailmantilanne (kyberhyökkäykset, geopolitiikan muutokset).

Yritykset





Yhteiskunnalliset uhkat ja niihin varautuminen

Yritysten suurimmat uhkakuvat liittyvät talousnäkyymiin, kyberhyökkäyksiin ja pakolaistulvaan, eikä näihin olla varauduttu riittävästi, toisin kuin esimerkiksi sotaan tai epidemioihin. Sota koetaan myös merkittävänä uhkana, tosin osan

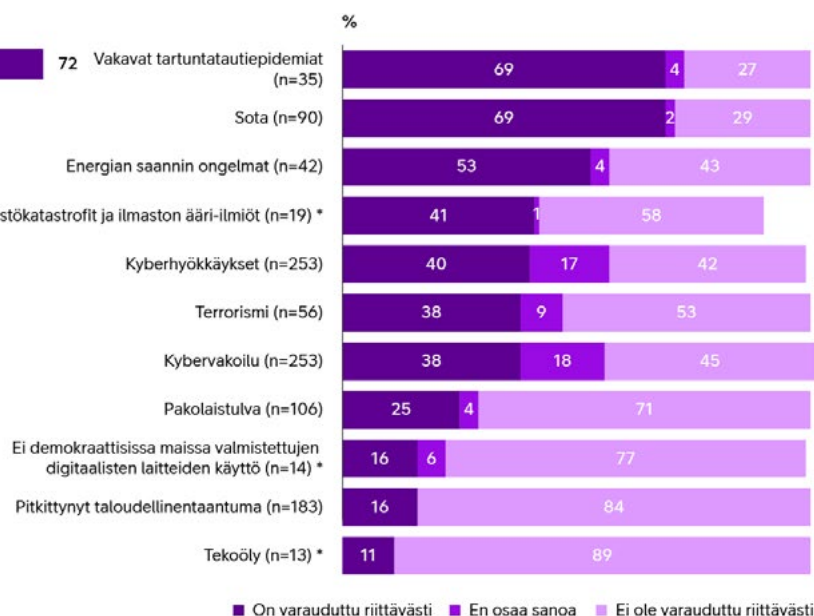
mielestä siihen on osattu jo varautua kylliksi. Julkishallinnossa selvästi suurimmat uhkakuvat liittyvät kyberhyökkäyksiin ja talousnäkyymiin, joihin ei olla suurimman osan mielestä varauduttu riittävästi – toisin kuin sotaan tai terrorismiin.

Yritykset

Mitkä ovat mielestänne kolme suurinta Suomeen kohdistuvaa uhkaa tällä hetkellä? (n=253)



Mihin seuraavista on suomalaisessa yhteiskunnassa varauduttu riittävästi?



■ On varauduttu riittävästi ■ En osaa sanoa ■ Ei ole varauduttu riittävästi

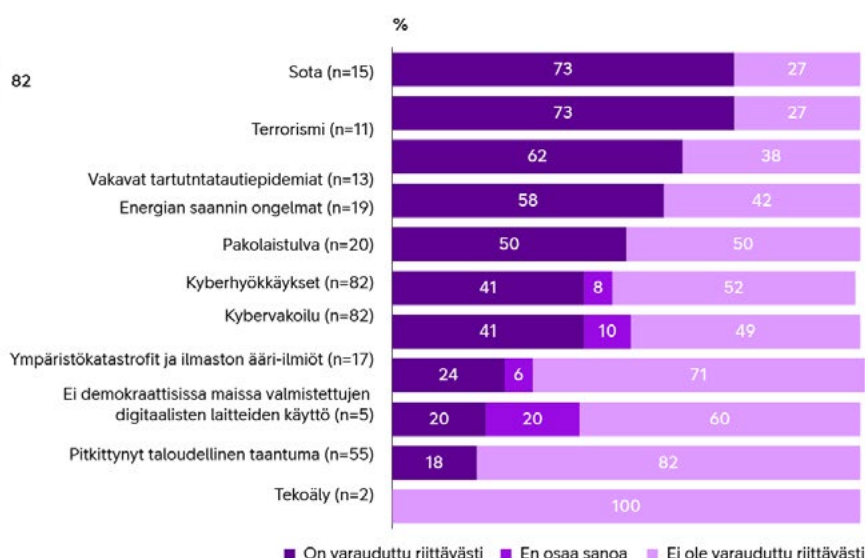
* Huom! Pieni vastaajamäärä

Julkishallinto

Mitkä ovat mielestänne kolme suurinta Suomeen kohdistuvaa uhkaa tällä hetkellä? (n=100)



Mihin seuraavista on suomalaisessa yhteiskunnassa varauduttu riittävästi?



■ On varauduttu riittävästi ■ En osaa sanoa ■ Ei ole varauduttu riittävästi

*Kysytty, mikäli mainitsi uhaksi. Poikkeuksena kyberhyökkäys, joka kysytty kaikilta.



3. Digiturvallisuuden tärkeys ja siihen liittyvät uhkat

Tietoliikenneverkon merkitys digiturvalliselle yhteiskunnalle

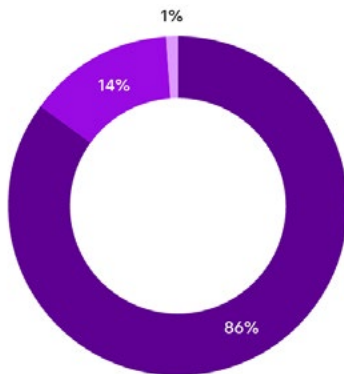
Käytännössä kaikki yritysten johtohenkilöt ovat vakuuttuneita, että tietoliikenneverkot ovat tärkeä osa digiturvallista

yhteiskuntaa. Maan pohjois- ja itäosissa sijaitsevista yrityksistä seistään väitteen takana vielä vahvemmin kuin muualla. Käytännössä kaikki julkishallinnon johtohenkilöt kokevat, että tietoliikenneverkot ovat erittäin tärkeä osa digiturvallista yhteiskuntaa.

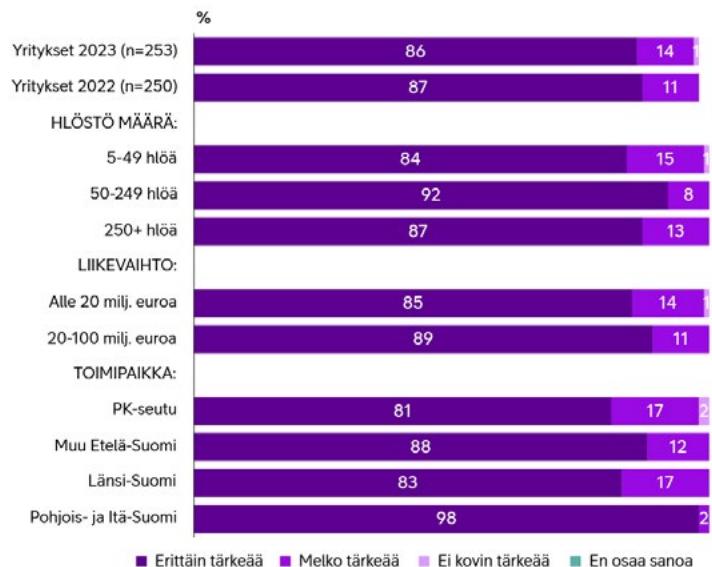
Yritykset



Kuinka tärkeä osa digiturvallista yhteiskuntaa tietoliikenneverkko on? (n=253)



■ Erittäin tärkeä
■ Melko tärkeä
■ Ei kovin tärkeä
■ Ei lainkaan tärkeä
■ En osaa sanoa

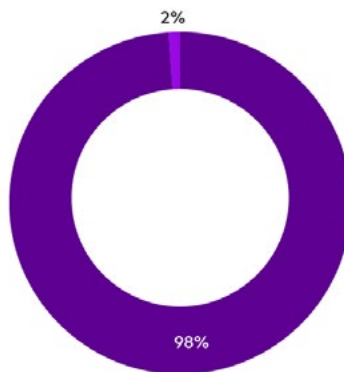


■ Erittäin tärkeä ■ Melko tärkeä ■ Ei kovin tärkeä ■ Ei lainkaan tärkeä ■ En osaa sanoa

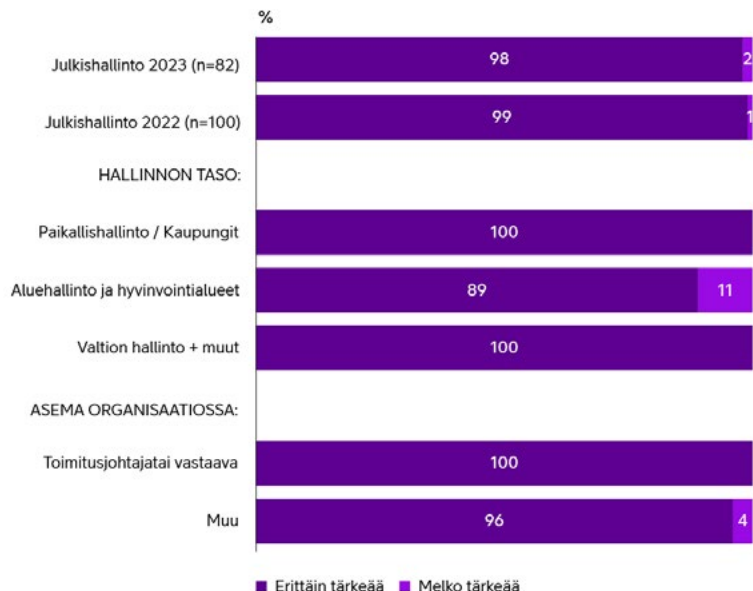
Julkishallinto



Kuinka tärkeä osa digiturvallista yhteiskuntaa tietoliikenneverkko on? (n=82)



■ Erittäin tärkeä
■ Melko tärkeä
■ Ei kovin tärkeä
■ Ei lainkaan tärkeä
■ En osaa sanoa



■ Erittäin tärkeä ■ Melko tärkeä



"Toimivat tietoverkot koetaan erittäin tärkeinä, koska ne luovat pohjan digitaaliselle yhteiskunnallemme. Digitalisaation kasvaessa voimakkaasti, onkin kriittistä varmistaa toiminnan jatkuvuus kaikissa tilanteissa.

Viimeaikaiset poliittiset tapahtumat korostavat tiedon varastoinnin, suojaamisen ja saavutettavuuden merkitystä yritysten ja organisaatioiden toiminnan jatkuvuuden takaamiseksi. Tutkimuksen mukaan julkishallinnossa huoli näistä asioista on kasvanut.

Suomen julkishallinnossa digiturvallisuuden taso koetaan korkeaksi ja jopa paremmaksi kuin aiemmin. Ote ei kuitenkaan saa herpaantua, vaan tietoturvan jatkuva kehittäminen ja kriittinen tarkastelu on tärkeää. Onneksi julkishallinnossa tietoturva nähdään asiana, johon halutaan panostaa merkittävästi enemmän kuin aiemmin. Tämä on oikea valinta."

Samu Viisteensaari

Myyntijohtaja, Government & Security asiakkaat
Telia Finland



Digitaalisen turvallisuuden tärkeys itselle

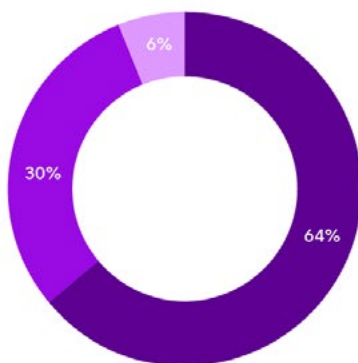
Digitaalinen turvallisuus on ainakin melko tärkeää lähes kaikille suomalaisille yrityksille. Mitä suurempi yritys, sitä voimakkaammin digitaalisen turvallisuuden tärkeyttä painotetaan. Myös julkishallinnon aloille digitaalinen

turvallisuus on vähintään melko tärkeää. Etenkin paikallishallinto sekä valtion hallinto painottavat asian olevan erittäin tärkeää.

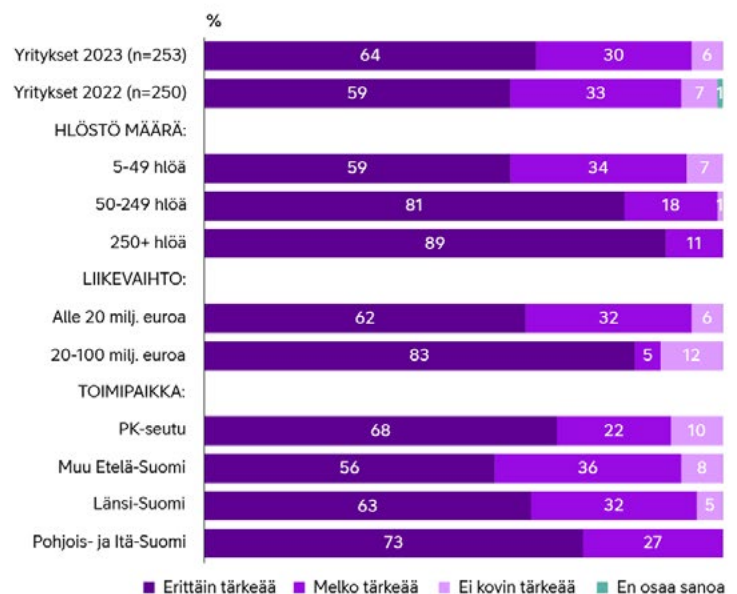
Yritykset



Kuinka tärkeää digitaalinen turvallisuus on yrityksellenne? (n=253)



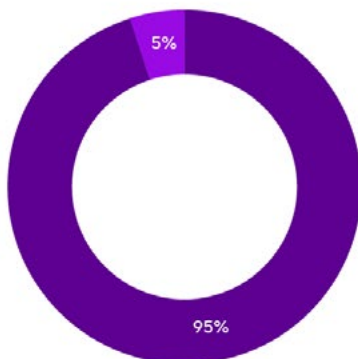
■ Erittäin tärkeää
■ Melko tärkeää
■ Ei kovin tärkeää
■ Ei lainkaan tärkeää
■ En osaa sanoa



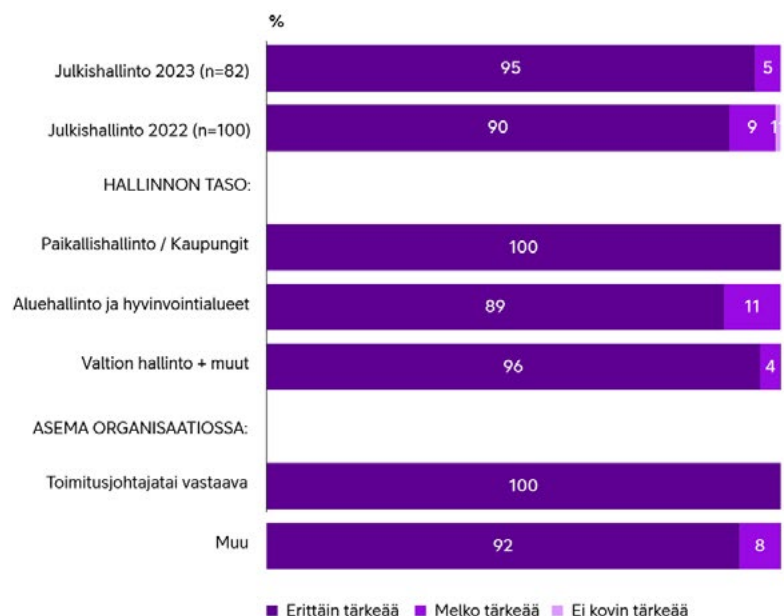
Julkishallinto



Kuinka tärkeää digitaalinen turvallisuus on organisaatiollenne? (n=82)



■ Erittäin tärkeää
■ Melko tärkeää
■ Ei kovin tärkeää
■ Ei lainkaan tärkeää
■ En osaa sanoa



Digiturvallisuuden kohdistuvat uhkakuvat

Suurin uhkakuva liittyy tietomurtoihin, joista ovat huolissaan etenkin yritysten johtohenkilöt. Kyberuhat ja muut haittaohjelmiin ja huijauksiin liittyvät riskit mietityttävät myös laajasti. Julkishallinnossa suurin uhkakuva liittyy

kyberuhkiin. Myös yksilöihin ja organisaatioon liittyvien tietojen varastointiin, huijauksiin, palvelunestohyökkäyksiin ja tietojärjestelmiin murtautumiseen liittyvät asiat huolestuttavat julkisella puolella.

Yritykset



Mitkä digitaaliseen turvallisuuteen liittyvät asiat huolestuttavat yritystänne? (spontaani maininta, n=253)



Julkishallinto



Mitkä digitaaliseen turvallisuuteen liittyvät asiat huolestuttavat organisaatiotanne? (spontaani maininta, n=82)





Oma valmius tunnistaa digiturvallisuushkia

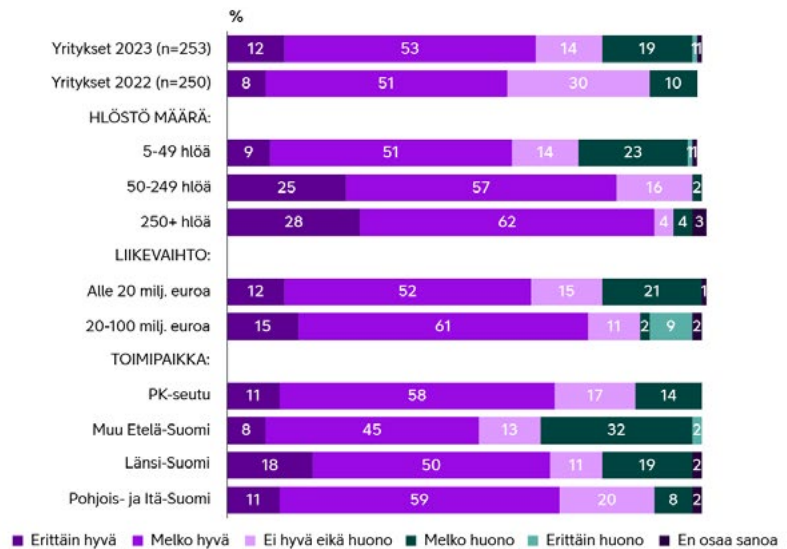
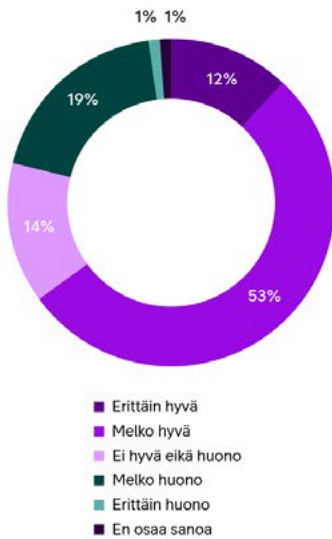
Yrityksissä ollaan vakuuttuneita kyvykkyydestä tunnistaa digiturvallisuuteen liittyviä uhkia, erityisesti suurissa yrityksissä. Viidennes epäilee yrityksen valmiuksia. Julkishallinnossa hyvin harva epäilee organisaation

valmiuksia tunnistaa digiturvallisuuteen liittyviä uhkia. Oman organisaationsa kyvykkyydestä ollaan varmoja eri hallinnon tasoilla ja tehtävissä.

Yritykset



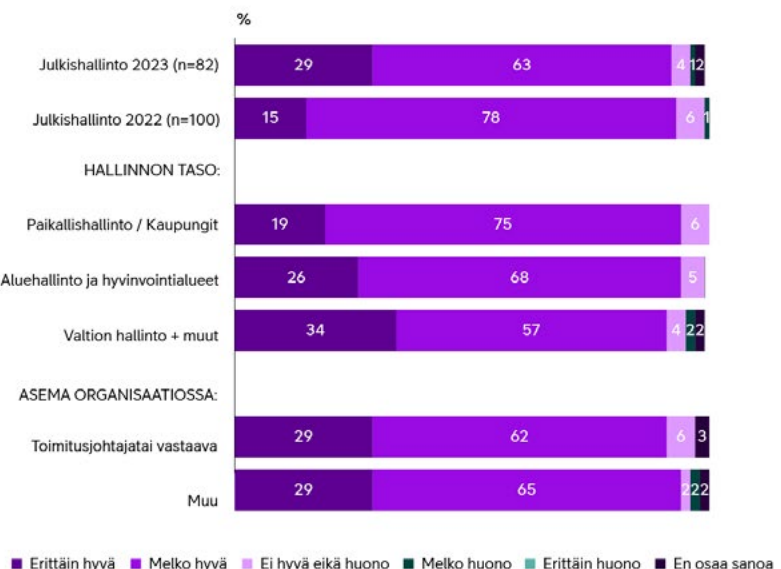
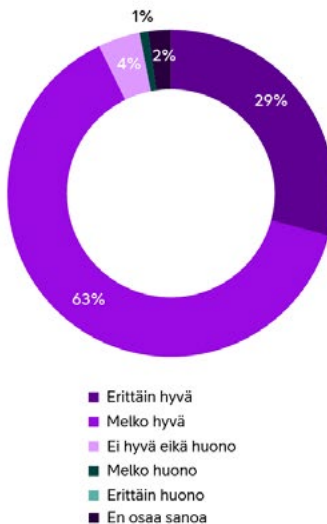
Millaiseksi koette yrityksenne valmiuden tunnistaa digiturvallisuushkia? (n=253)



Julkishallinto



Millaiseksi koette organisaationne valmiuden tunnistaa digiturvallisuushkia? (n=82)



Identiteettivarkauksien kohteeksi joutuminen

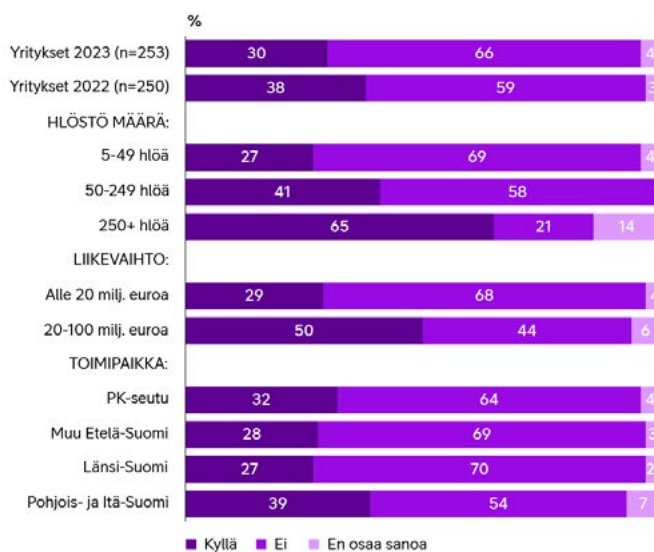
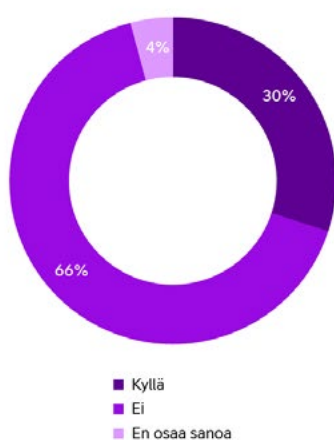
Lähes joka kolmas yritysjohtajista kertoo yrityksen kohdanneen tietojen kalasteluun tai henkilötietovarkauksiin kohdistuvia uhkia. Mitä suuremmasta yrityksestä on

kyse, sitä todennäköisemmin joitain tapauksia on ollut. Julkishallinnon edustajista yli puolet kertoo organisaation joutuneen tietojen kalastelun tai niiden yritysten kohteeksi.

Yritykset



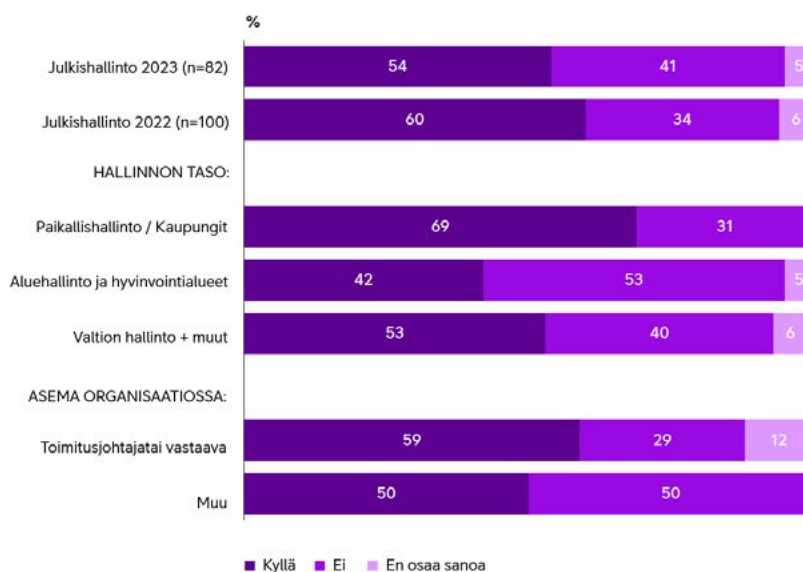
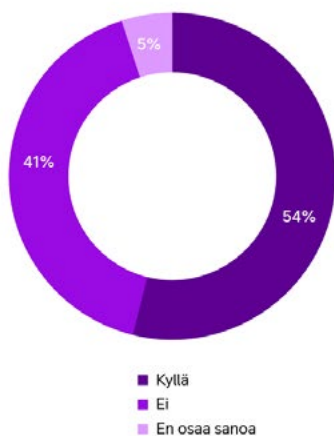
Onko yrityksenne joutunut tietojen kalastelun (PHISHING) tai identiteettivarkauksien kohteeksi? (n=253)



Julkishallinto



Onko organisaationne joutunut tietojen kalastelun (PHISHING) tai identiteettivarkauksien kohteeksi? (n=82)





”Identiteettivarkauksia voidaan estää tehokkaasti käyttämällä vahvaa tunnistusta, eli yleisimmin pankkitunnistusta tai mobiilivarmennetta. Vahvan tunnistautumisen avulla on mahdollista päästä eroon käyttäjätunnus-salasanapariin liittyvistä riskeistä. Vahva tunnistus on aina kaksivaiheinen: tunnistettavalla henkilöllä on salasanan tai PIN-koodin lisäksi hallussaan myös

yksilöity fyysinen laite kuten puhelin. Näin identiteetin kaappaaminen tai luottamuksellisen tiedon leviäminen ei onnistu, vaikka käyttäjän salasana tai PIN-koodi varastettaisiin.”

Mika Loukola
Telia Tunnistus -palvelun
liiketoimintapäällikkö
Telia Finland

Yritysten digiturvallisuudesta huolehtiminen

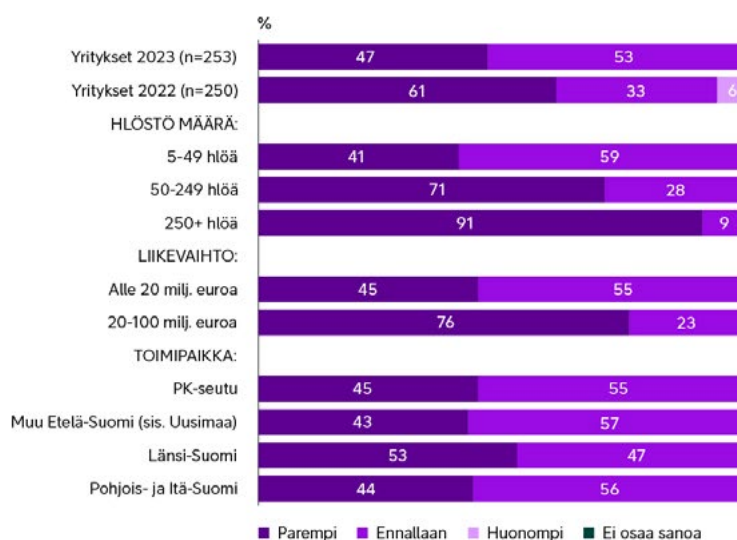
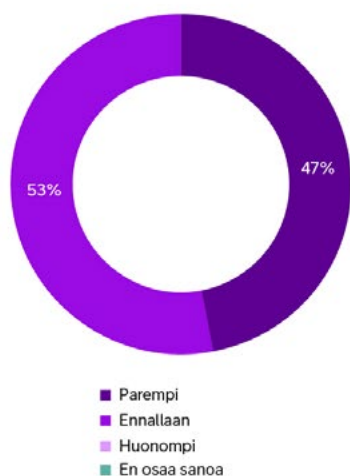
Puolet yritysten johtohenkilöistä sanoo yrityksen digitaalisen turvallisuuden tason olevan ennallaan ja toiset ilmoittavat sen olevan jopa paremmalla tasolla kuin aiemmin. Mitä suurempi yritys, sitä todennäköisemmin on tehty parannuksia digiturvallisuuteen.

Enemmistö julkishallinnon edustajista sanoo organisaation digitaalisen turvallisuuden olevan jopa paremmalla tasolla kuin aiemmin. Moni kokee tason pysyneen ennallaan ja juuri kukaan ei koe tilanteen heikentyneen.

Yritykset



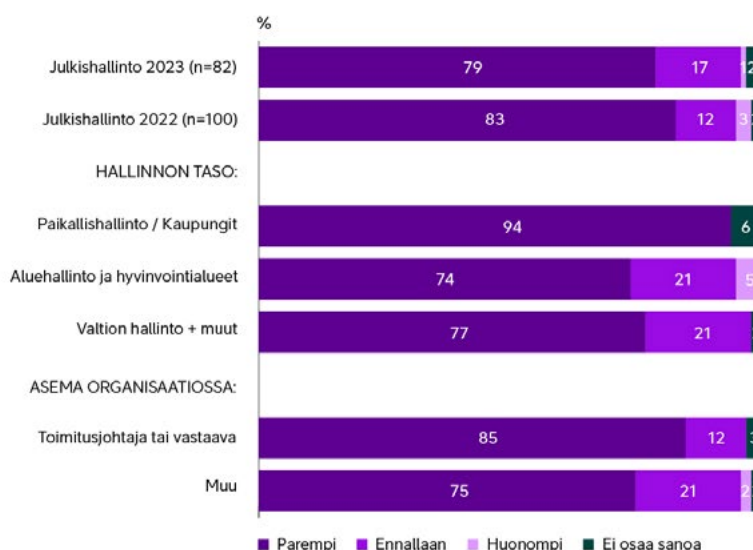
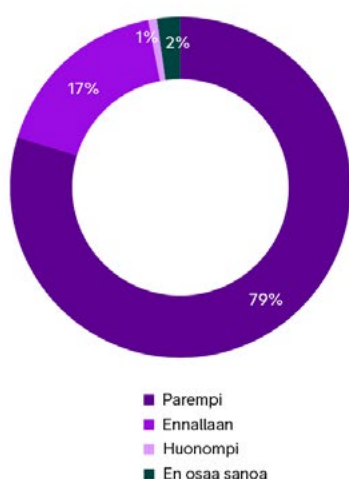
Onko yrityksenne digitaalisen turvallisuuden taso nyt parempi vai huonompi kuin vuosi sitten? (n=253)



Julkishallinto



Onko organisaationne digitaalisen turvallisuuden taso nyt parempi vai huonompi kuin vuosi sitten? (n=82)





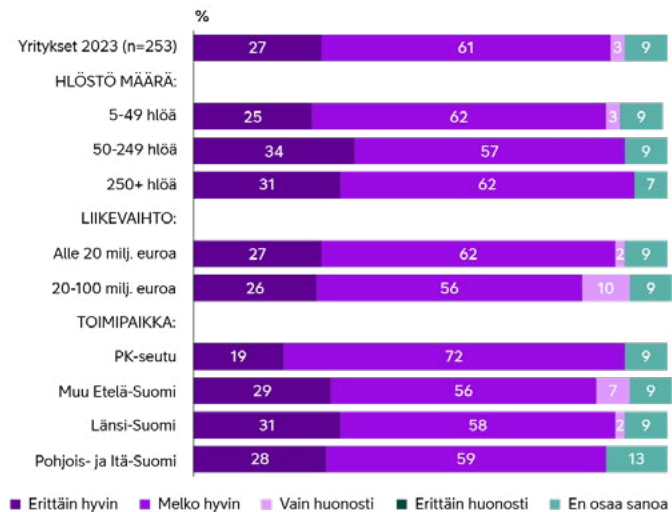
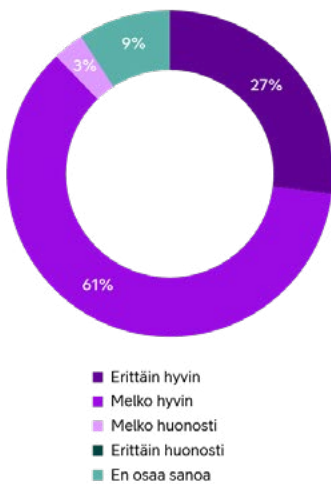
Operaattoreiden huolehtiminen digiturvallisuudesta

Operaattoreiden katsotaan yleisesti hoitavan hyvin digiturvallisuuksien ennaltaehkäisyä niin yrityksissä kuin julkishallinnon organisaatioissakin – tosin osa ei ole varma mielipiteestään.

Yritykset



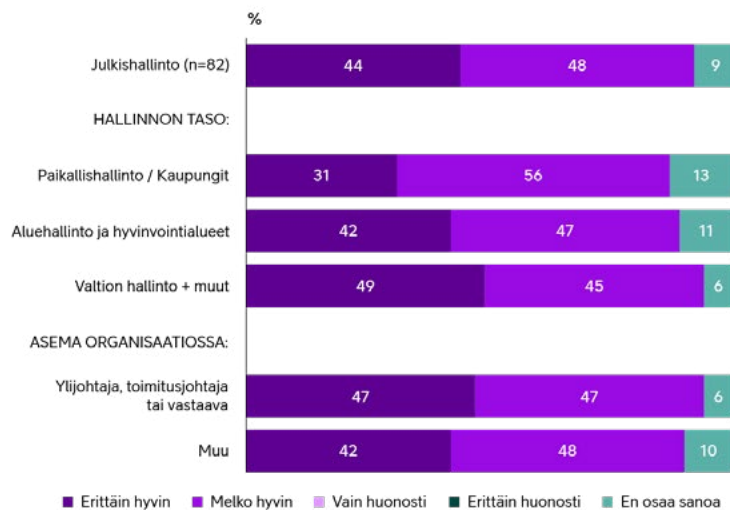
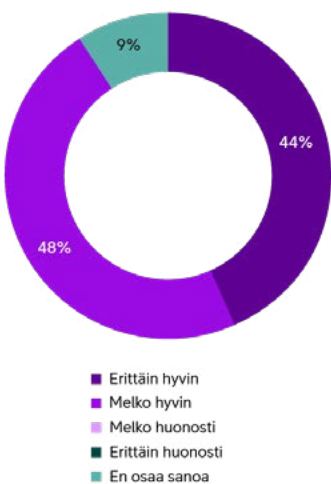
Kuinka hyvin koette yrityksenne operaattorin huolehtivan puhelin- ja nettiyhteyksien turvallisuudesta? (n=253)



Julkishallinto



Kuinka hyvin koette organisaationne operaattorin huolehtivan puhelin- ja nettiyhteyksien turvallisuudesta? (n=82)







4. Digitaaliseen turvallisuuteen liittyvät ratkaisut

Varautuminen tietoturvauxhiin

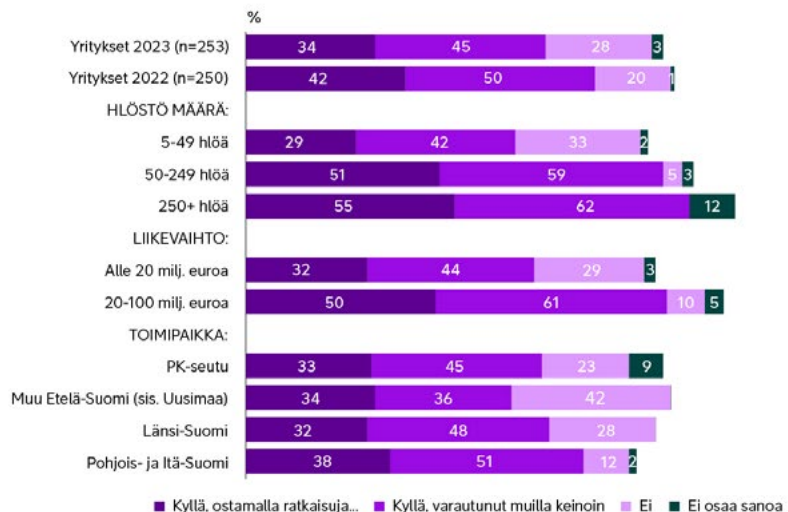
Suurin osa yrityksistä on varautunut jollakin keinolla tietojen kalasteluun ja henkilötietovarkauksiin kohdistuviin uhiin. Pienimmät yritykset ovat ryhtyneet muita harvemmin toimiin

tai hankkineet palveluita suojaukseen. Julkishallinnossa lähes kaikki organisaatiot ovat varautuneet jollakin keinoin henkilö- ja yritystietoihin kohdistuviin uhiin. Palveluratkaisujen ostaminen on kuitenkin vähemmän yleistä kuin muu varautuminen.

Yritykset



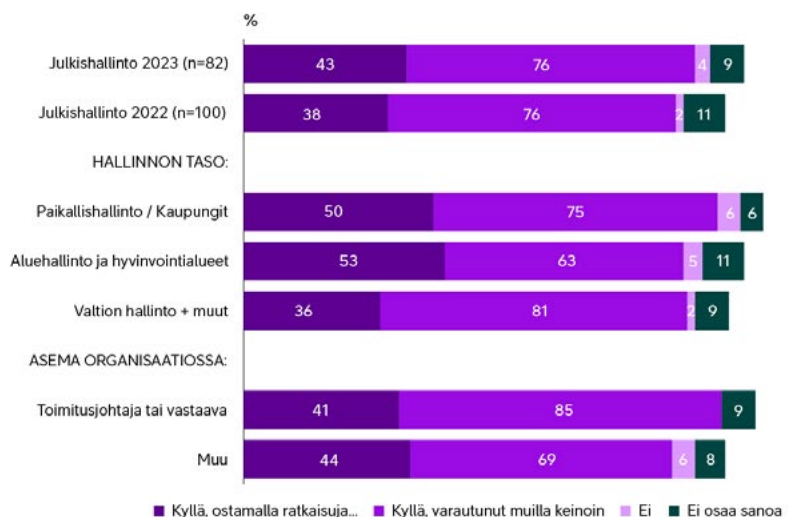
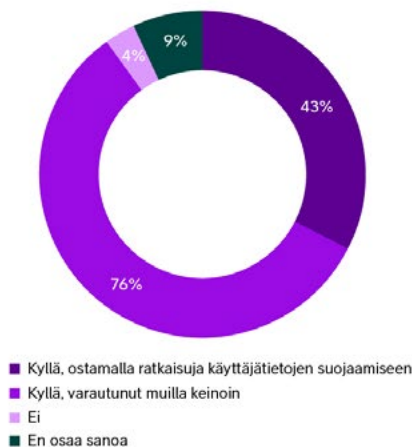
Onko yrityksenne varautunut tietojen kalastelun (PHISHING) tai identiteettivarkauksien uhkaan? Jos kyllä, miten? (n=253)



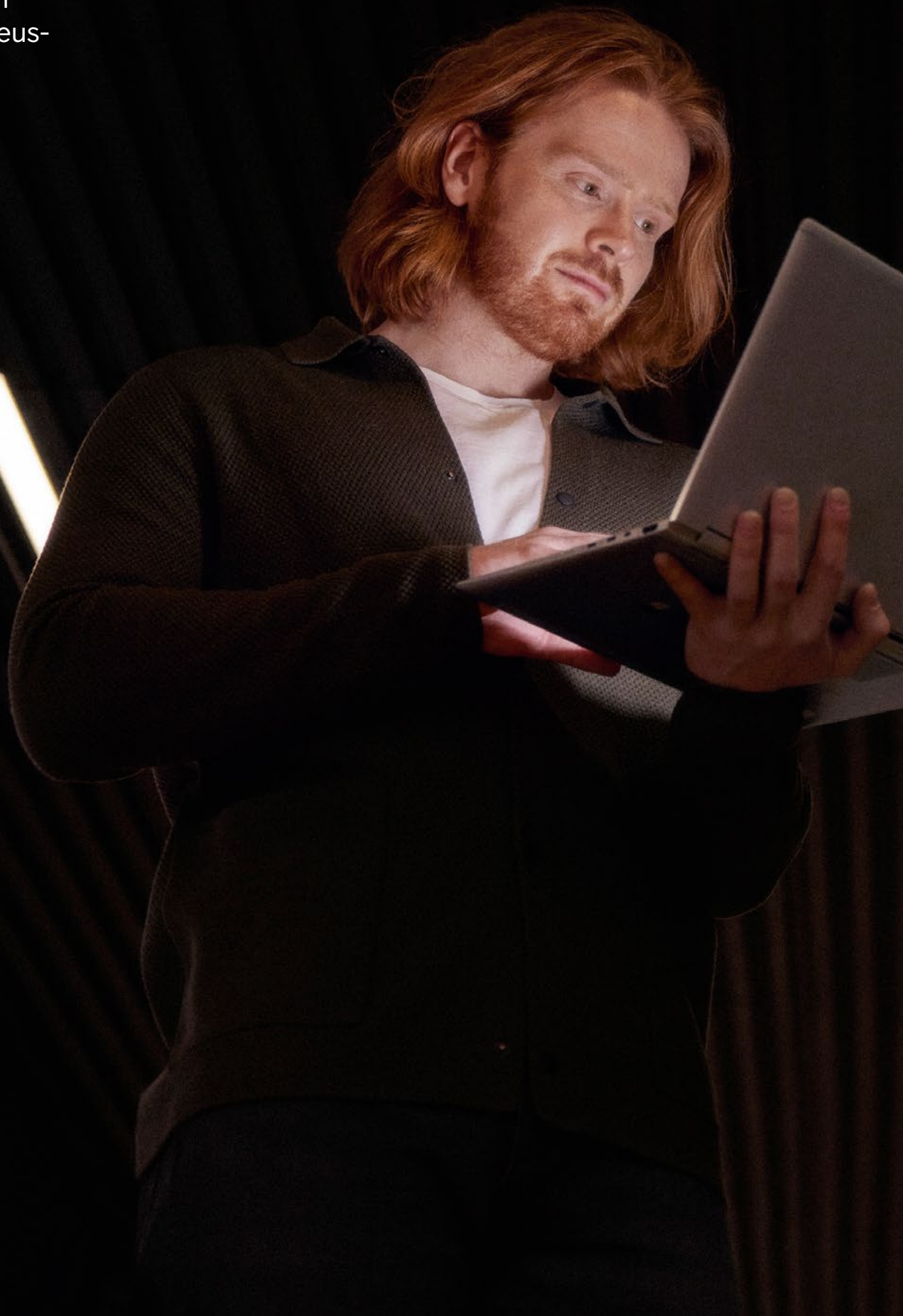
Julkishallinto



Onko organisaationne varautunut tietojen kalastelun (PHISHING) tai identiteettivarkauksien uhkaan? Jos kyllä, miten? (n=82)



Tietoturvan tulisi olla yritysjohdon prioriteetti, sillä se turvaa liiketoiminnan jatkuvuuden myös poikkeus-tilanteissa.





”Tietoturvan merkitys on kasvanut huomattavasti viimeisen parinkymmenen vuoden aikana. Perinteiset virustorjunta- ja palomuuritoiminnot ovat nykyisin vain osa kokonaisuutta, sillä nykyään yritysten on otettava tietoturva huomioon kattavasti liiketoiminnan jatkuvuuden turvaamiseksi. Yksi tärkeimmistä keinoista torjua kyberuhkia on ennaltaehkäisevä toiminta. Tietoturvan tilaa on tärkeä seurata ja pitää ajan tasalla, sillä jopa yksi saastunut laite tai järjestelmä voi muodostaa potentiaalisen hyökkäyspinnan kyberhyökkäyksille. Henkilöstön säännöllinen koulutus on myös olennainen osa tätä kokonaisuutta. Tietoturvan tulisi olla yritysjohdon prioriteettilistalla, sillä se varmistaa liiketoiminnan jatkuvuuden myös poikkeustilanteissa.”

Tommi Vänninen

Senior product manager

Tietoturva ry:n hallituksen puheenjohtaja

Telia Finland

Panostus tietoturvaan

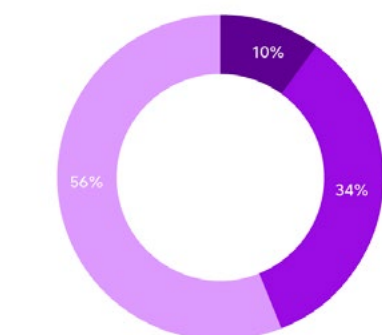
Kaikki yritykset panostavat tietoturva-asioihin vähintään saman verran kuin viime vuonna. Panostukset henkilöstön osaamiseen ovat myös selviä, mutta pääsääntöisesti tässä pärjätään ilman lisäpanostuksia. Julkishallinnon puolella

lähes kaikki organisaatiot panostavat tietoturva-asioihin enemmän kuin vuosi sitten tai vähintään saman verran kuin aikaisemmin. Myös panostukset henkilöstön osaamiseen ovat pääsääntöisesti kasvussa.

Yritykset

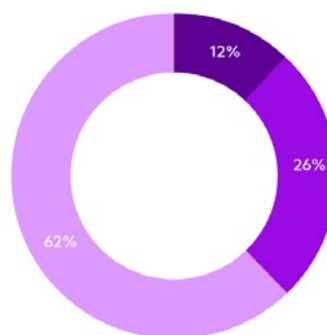


Panostaako yrityksenne nykyään enemmän tietoturva-asioihin kuin vuosi sitten? (n=253)



- Merkittävästi enemmän
- Jossain määrin enemmän
- Saman verran kuin aikaisemminkin
- Jossain määrin vähemmän
- Merkittävästi vähemmän
- En osaa sanoa

Panostaako yrityksenne enemmän työntekijöiden tietoturva-koulutukseen ja/-tai ohjeistuksiin kuin vuosi sitten? (n=253)

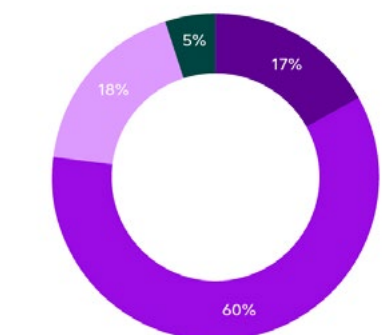


- Merkittävästi enemmän
- Jossain määrin enemmän
- Saman verran kuin aikaisemminkin
- Jossain määrin vähemmän
- Merkittävästi vähemmän
- En osaa sanoa

Julkishallinto

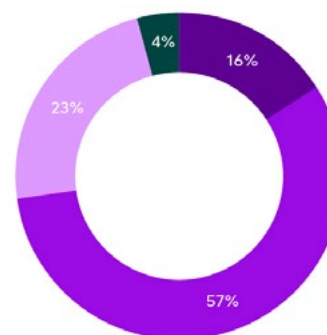


Panostaako organisaationne nykyään enemmän tietoturva-asioihin kuin vuosi sitten? (n=82)



- Merkittävästi enemmän
- Jossain määrin enemmän
- Saman verran kuin aikaisemminkin
- Jossain määrin vähemmän
- Merkittävästi vähemmän
- En osaa sanoa

Panostaako organisaationne enemmän työntekijöiden tietoturva-koulutukseen ja/-tai ohjeistuksiin kuin vuosi sitten? (n=82)



- Merkittävästi enemmän
- Jossain määrin enemmän
- Saman verran kuin aikaisemminkin
- Jossain määrin vähemmän
- Merkittävästi vähemmän
- En osaa sanoa



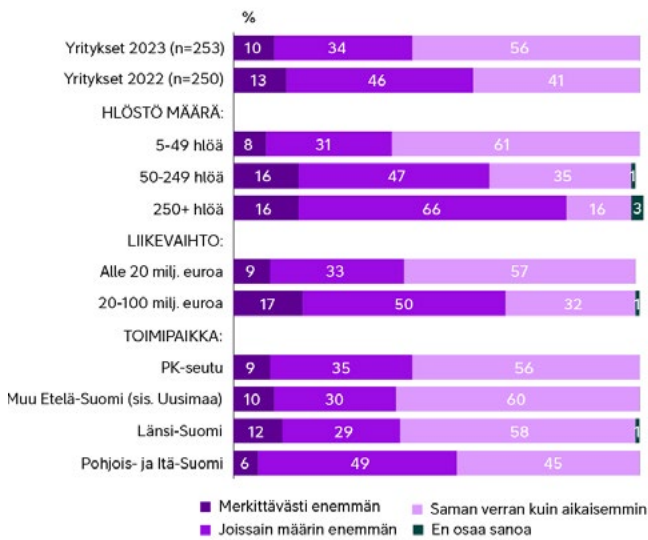
Panostus tietoturvaan nyt ja ennen

Panostukset organisaation tietoturvaan ja henkilöstön osaamiseen ovat lisääntyneet kautta linjan niin yrityksillä kuin julkishallinnollakin.

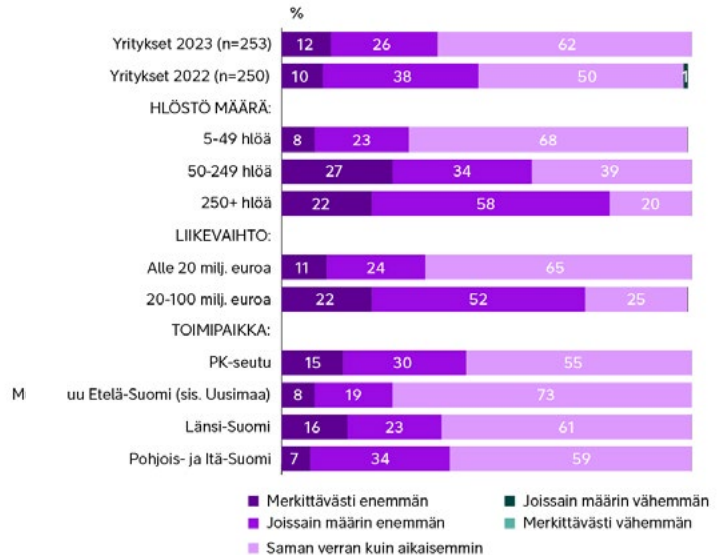
Yritykset



Panostaako yrityksenne nykyään enemmän tietoturva-asioihin kuin vuosi sitten?



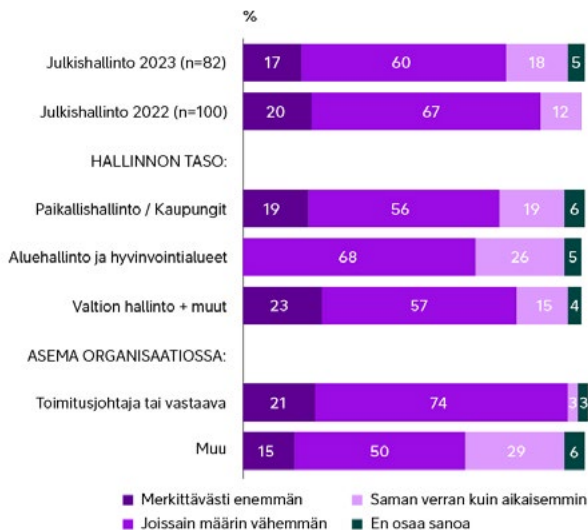
Panostaako yrityksenne enemmän työntekijöiden tietoturva-koulutukseen ja/-tai ohjeistuksiin kuin vuosi sitten?



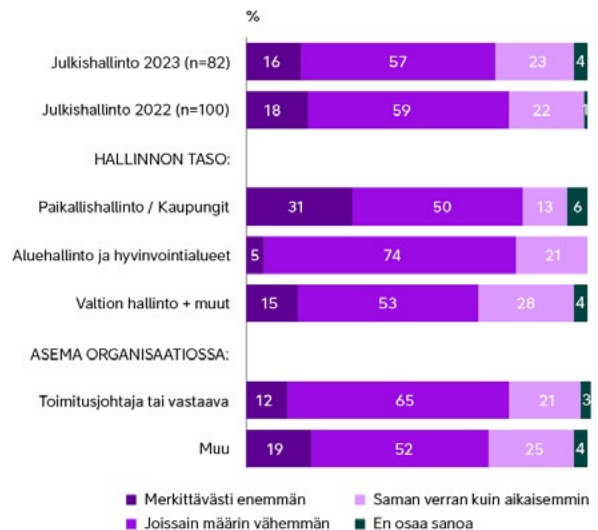
Julkishallinto



Panostaako organisaationne nykyään enemmän tietoturva-asioihin kuin vuosi sitten?



Panostaako organisaationne enemmän työntekijöiden tietoturva-koulutukseen ja/-tai ohjeistuksiin kuin vuosi sitten?





"Kyberrikollisuuden torjuminen vaatii järeitä toimia, etenkin nyt kun globaalien konfliktien kiihtyminen on tehnyt tietoturvauhista entistä merkittävämpiä. Tietoturvatietoisuus on kaikille tärkeä taito. Kun varaudumme riskeihin ennakolta, meillä on parempi palautumiskyky hyökkäyksistä.

Kyberturvallisuuteen liittyy myös uusia lainsäädännöllisiä velvoitteita. Tämän vuoden lokakuussa astuu voimaan EU:n NIS2-direktiivi, joka vaatii yhä suurempaa osaa yrityksistä kantamaan vastuuta tietoturvastaan."

Pirkko Filtress
Myyntijohtaja
Telia Cygate Oy



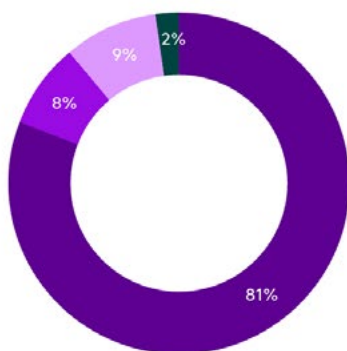
Tietoturvaratkaisujen budjetointi

Digitaalisen turvallisuuden ratkaisut on yleisimmin budjetoitu osaksi IT-budjettia sekä yrityksissä että julkishallinnossa. Suuryrityksillä on muita useammin oma budjettinsa tietoturvaratkaisuille.

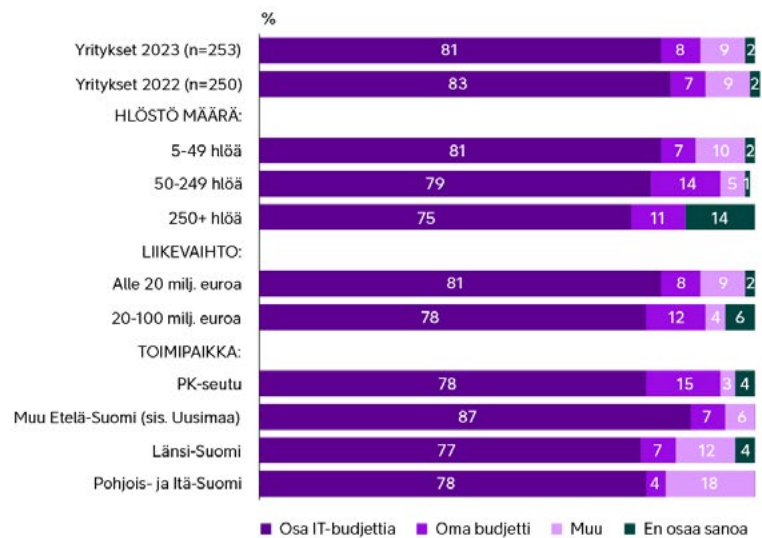
Yritykset



Ovatko digi- ja tietoturvaratkaisut osa IT-budjettianne, vai onko sille oma budjetti? (n=253)



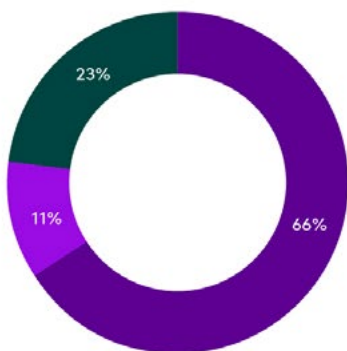
■ Osa IT-budjettia
■ Oma budjetti
■ Muu
■ En osaa sanoa



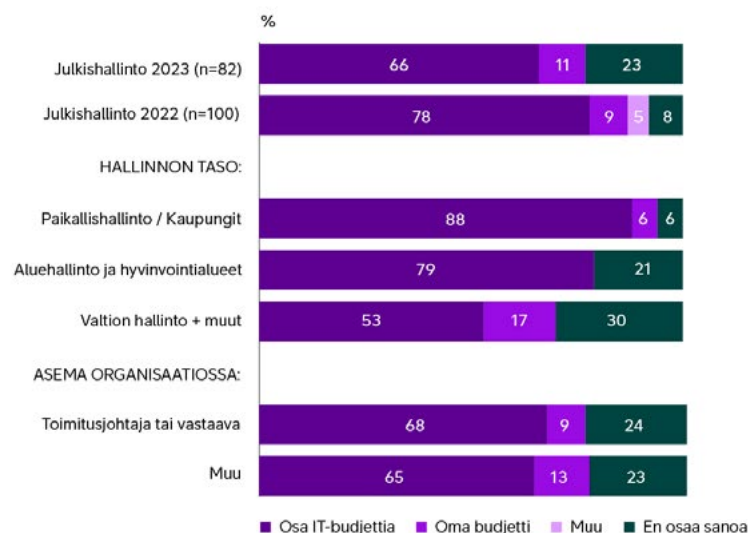
Julkishallinto



Ovatko digi- ja tietoturvaratkaisut osa IT-budjettianne, vai onko sille oma budjetti? (n=82)



■ Osa IT-budjettia
■ Oma budjetti
■ Muu
■ En osaa sanoa



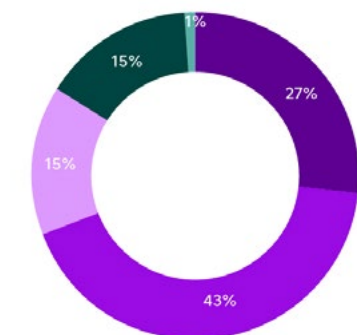
Verkkoteknologian kotimaisuuden merkitys

Verkkoteknologian kotimaisuudella on suuri merkitys yrityksille ja julkishallinnolle, mutta vielä tärkeämpää on verkon infrastruktuurin sijaitseminen Suomessa.

Yritykset

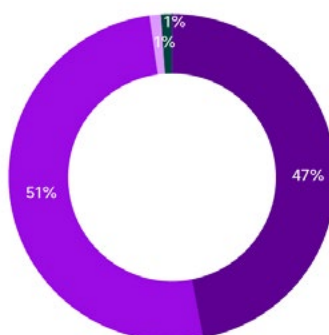


Onko käytetyn verkkoteknologian kotimaisuudella merkitystä yrityksellenne? (n=250)



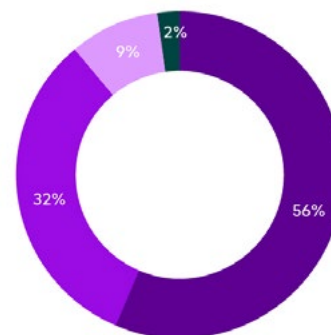
■ Erittäin suuri merkitys
■ Melko suuri merkitys
■ Jonkin verran merkitystä
■ Ei lainkaan merkitystä
■ En osaa sanoa

Onko tietoliikenneverkon kotimaisuus tärkeämpää vai vähemmän tärkeää nyt kuin vuosi sitten? (n=250)



■ Tärkeämpää
■ Yhtä tärkeää
■ Vähemmän tärkeää
■ En osaa sanoa

Kuinka tärkeänä pidätte sitä, että verkon infrastruktuuri (eli laitteet ja datavarastot) sijaitsevat Suomessa? (n=250)

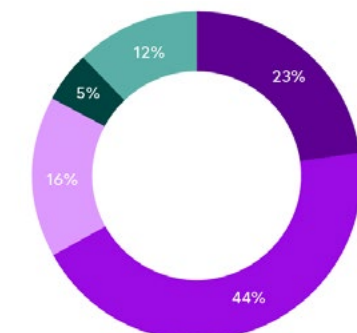


■ Erittäin tärkeää
■ Melko tärkeää
■ Ei kovin tärkeää
■ Ei lainkaan tärkeää
■ En osaa sanoa

Julkishallinto

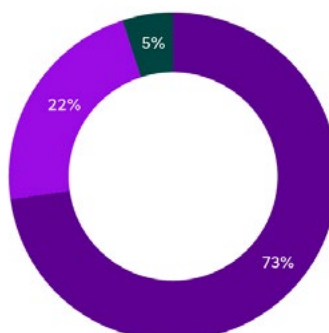


Onko käytetyn verkkoteknologian kotimaisuudella merkitystä organisaatiollenne? (n=100)



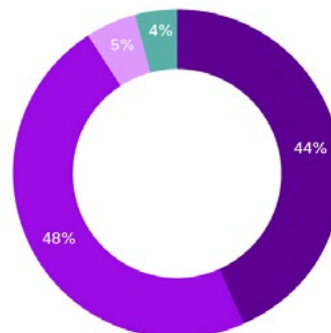
■ Erittäin suuri merkitys
■ Melko suuri merkitys
■ Jonkin verran merkitystä
■ Ei lainkaan merkitystä
■ En osaa sanoa

Onko tietoliikenneverkon kotimaisuus tärkeämpää vai vähemmän tärkeää nyt kuin vuosi sitten? (n=100)



■ Tärkeämpää
■ Yhtä tärkeää
■ Vähemmän tärkeää
■ En osaa sanoa

Kuinka tärkeänä pidätte sitä, että verkon infrastruktuuri (eli laitteet ja datavarastot) sijaitsevat Suomessa? (n=100)



■ Erittäin tärkeää
■ Melko tärkeää
■ Ei kovin tärkeää
■ Ei lainkaan tärkeää
■ En osaa sanoa



Verkkoteknologian kotimaisuuden merkitys itselle

Yrityksissä, jotka sijaitsevat ruuhka-Suomen ulkopuolella, kotimaisuuden merkitys korostuu. Kotimaisuus korostuu myös paikallishallinnon ja kaupunkien edustajien vastauksissa.

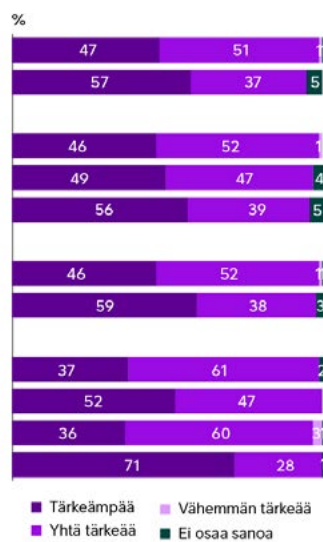
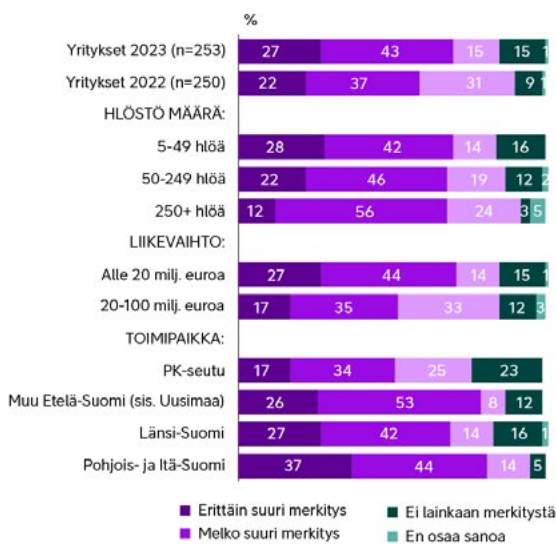
Yritykset



Onko käytetyn verkkoteknologian kotimaisuudella merkitystä yrityksellenne?

Onko tietoliikenneverkon kotimaisuus tärkeämpää vai vähemmän tärkeää nyt kuin vuosi sitten?

Kuinka tärkeänä pidätte sitä, että verkon infrastruktuuri (eli laitteet ja datavarastot) sijaitsevat Suomessa?



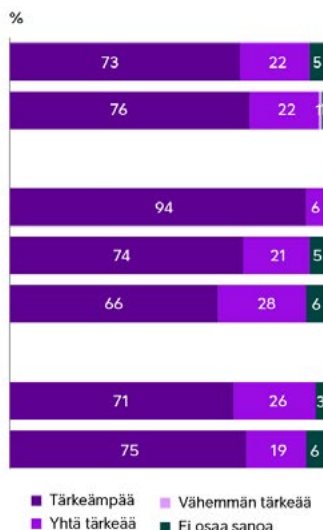
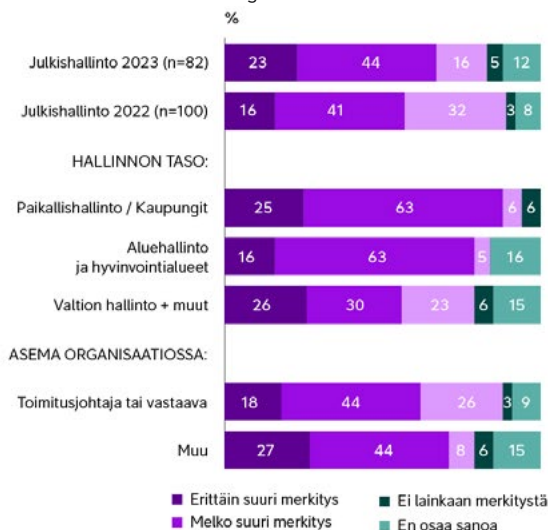
Julkishallinto



Onko käytetyn verkkoteknologian kotimaisuudella merkitystä organisaatiollenne?

Onko tietoliikenneverkon kotimaisuus tärkeämpää vai vähemmän tärkeää nyt kuin vuosi sitten?

Kuinka tärkeänä pidätte sitä, että verkon infrastruktuuri (eli laitteet ja datavarastot) sijaitsevat Suomessa?





Telia

Telia on viime vuosina kasvanut perinteisestä teleoperaattorista nykyaikaiseksi teknologia- ja mediatyhtiöksi, joka tarjoaa laajan kirjon tietoliikenne-, it- ja digipalveluita miljoonille kuluttaja- ja yritysasiakkailleen. Telialla on Suomessa 4 100 työntekijää ja yli neljä miljoonaa liittymäasiakasta. Tietoliikenneverkkoja Telia rakentaa Suomeen joka vuosi noin 200 miljoonalla eurolla.

Telia Finland on osa Telia Companya, joka toimii Pohjoismaissa ja Baltiassa. Telia Companyn liikevaihto vuonna 2021 oli 8,7 miljardia euroa. Yhtiö on sitoutunut olemaan päästötön ja jätteetön koko arvoketjussaan tavarantoimittajista asiakkaisiin vuoteen 2030 mennessä.

Ota yhteyttä

Herättikö tämä tutkimus ajatuksia?
[Jätä meille yhteystietosi](#), niin asiantuntijamme ottaa sinuun yhteyttä.

