

Pohjoismainen tietoturvatutkimus 2026

part of telenor

Tutkimuksen tiedot

Toteutustapa

Kuuden kysymyksen verkkokysely

Markkina-alueet

Suomi, Ruotsi, Norja, Tanska

Kohderyhmä

Yksityisen ja julkisen sektorin päättäjät pohjoismaisissa organisaatioissa

Tiedonkeruu

Elo–syyskuu 2026. Tutkimuksen on toteuttanut Opinion Telenorin toimeksiannosta.

Tavoite

Tutkimuksen tavoitteena oli selvittää yritys- ja organisaatiopäättäjien näkemyksiä digitaalisesta turvallisuudesta ja resilienssistä.

Otos

2 427 vastaajaa

Suomi: 610 vastaajaa

Ruotsi: 610 vastaajaa

Norja: 601 vastaajaa

Tanska: 606 vastaajaa

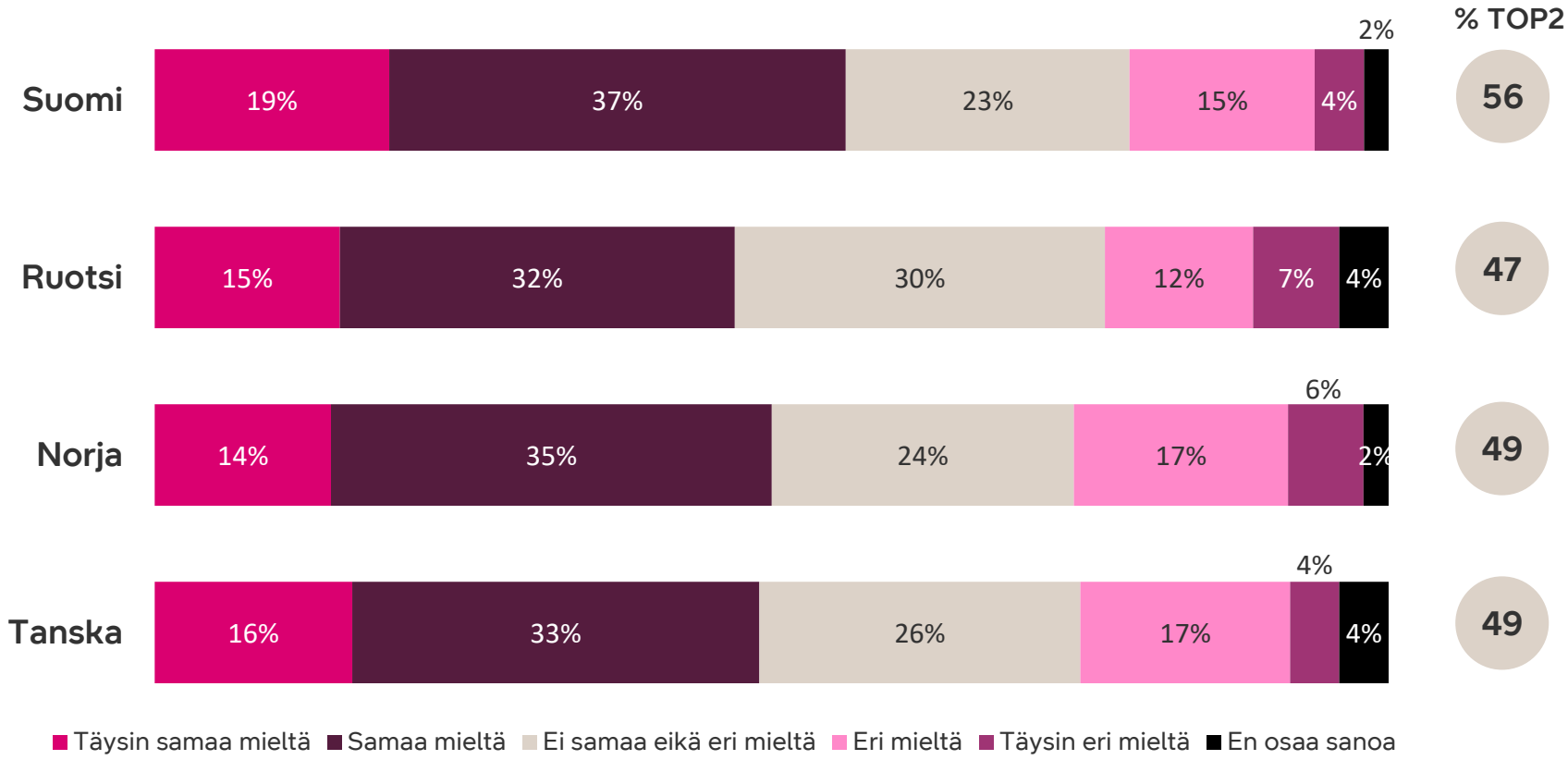
©DNA

Sensitivity: Open

Pohjoismainen tietoturvatutkimus 2026

Valmius ylläpitää kriittisiä toimintoja vakavan digitaalisen häiriön aikana

? Missä määrin olet samaa tai eri mieltä seuraavan väittämän kanssa?
Organisaationi on hyvin varautunut ylläpitämään kriittisiä toimintojaan vakavan digitaalisen häiriön, kuten yhteys- tai digitaalisten palveluiden häiriön, aikana.



Enemmistö päättäjistä arvioi, että heidän organisaatiollaan on hyvät valmiudet ylläpitää kriittisiä toimintojaan vakavan digitaalisen häiriön aikana.

Valmiudet arvioidaan parhaiksi Suomessa, jossa 56 prosenttia vastaajista on väittämän kanssa samaa mieltä. Ruotsissa vastaava osuus on 47 prosenttia, Norjassa ja Tanskassa 49 prosenttia.

Suomessa 19 prosenttia vastaajista on väittämän kanssa täysin samaa mieltä ja 37 prosenttia jokseenkin samaa mieltä. Neutraalisti suhtautuvien osuus on kaikissa maissa huomattava ja vaihtelee Suomen 23 prosentista Ruotsin 30 prosenttiin. Tulokset viittaavat siihen, että organisaatioiden resilienssiä ja varautumista on edelleen mahdollista vahvistaa.

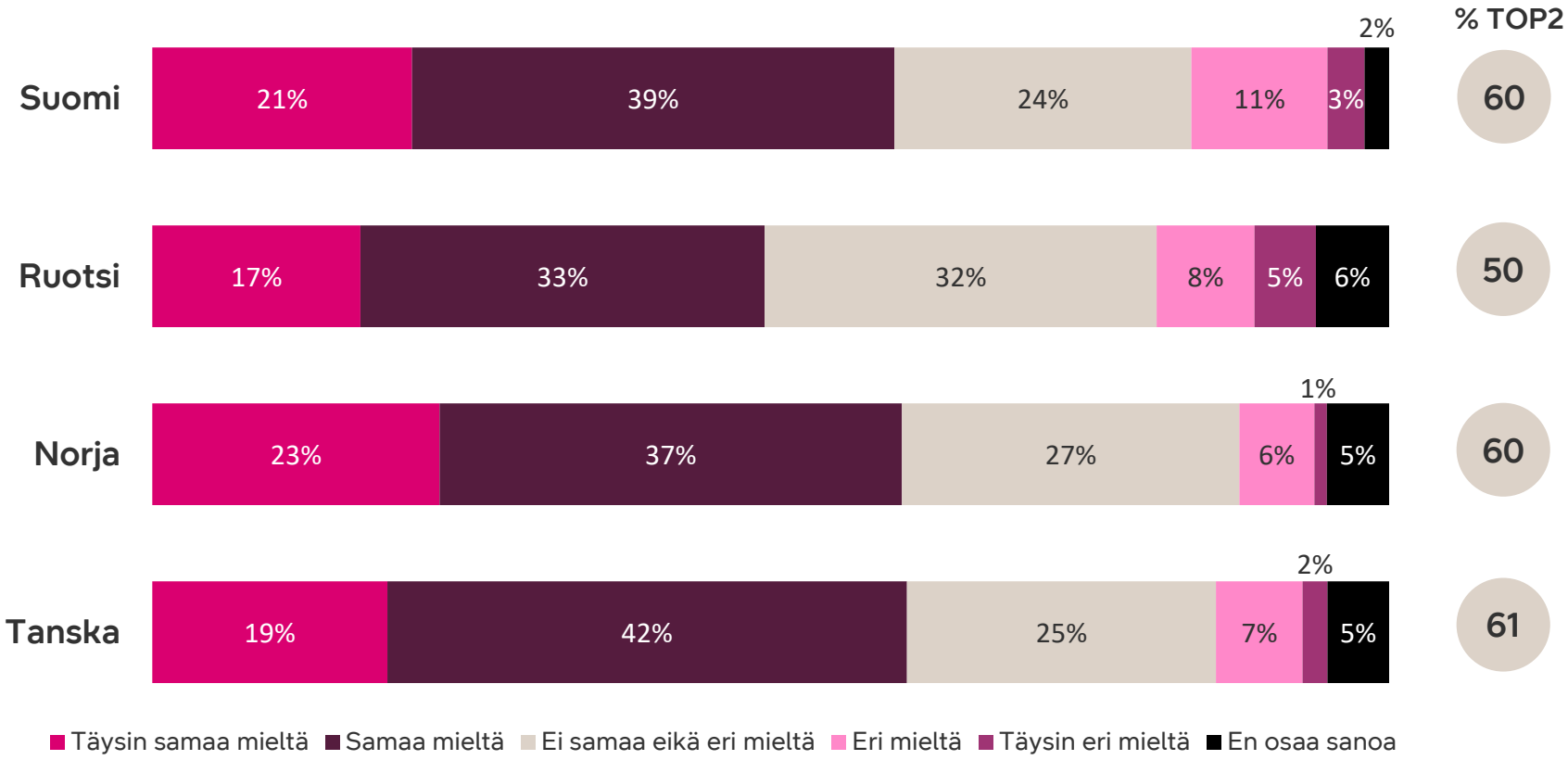
©DNA

Sensitivity: Open

Pohjoismainen tietoturvatutkimus 2026

Turvallisuuden ja resilienssin merkitys tietoliikenne-yhteyksien ja digitaalisten palveluiden hankinnassa

? Missä määrin olet samaa tai eri mieltä seuraavan väittämän kanssa?
Kuluneen 12 kuukauden aikana tietoturvasta ja liiketoiminnan jatkuvuuden turvaamisesta on tullut entistä tärkeämpiä tekijöitä organisaationi yhteys- ja digitaalisten palveluiden hankintapäätöksissä.



Kaikissa neljässä maassa enemmistö vastaajista arvioi, että turvallisuuden ja resilienssin merkitys tietoliikenneyhteyksien ja digitaalisten palveluiden hankintakriteereinä on kasvanut.

Samaa mieltä olevien osuus on suurin Tanskassa, 61 prosenttia. Norjassa ja Suomessa osuus on 60 prosenttia. Ruotsissa samaa mieltä olevien osuus on pienin, 50 prosenttia.

Neutraalien vastausten verrattain suuri osuus, Suomen 24 prosentista Ruotsin 32 prosenttiin, viittaa siihen, ettei turvallisuuden ja resilienssin kasvanut merkitys ole vielä vakiintunut yhtä vahvasti kaikissa organisaatioissa.

©DNA

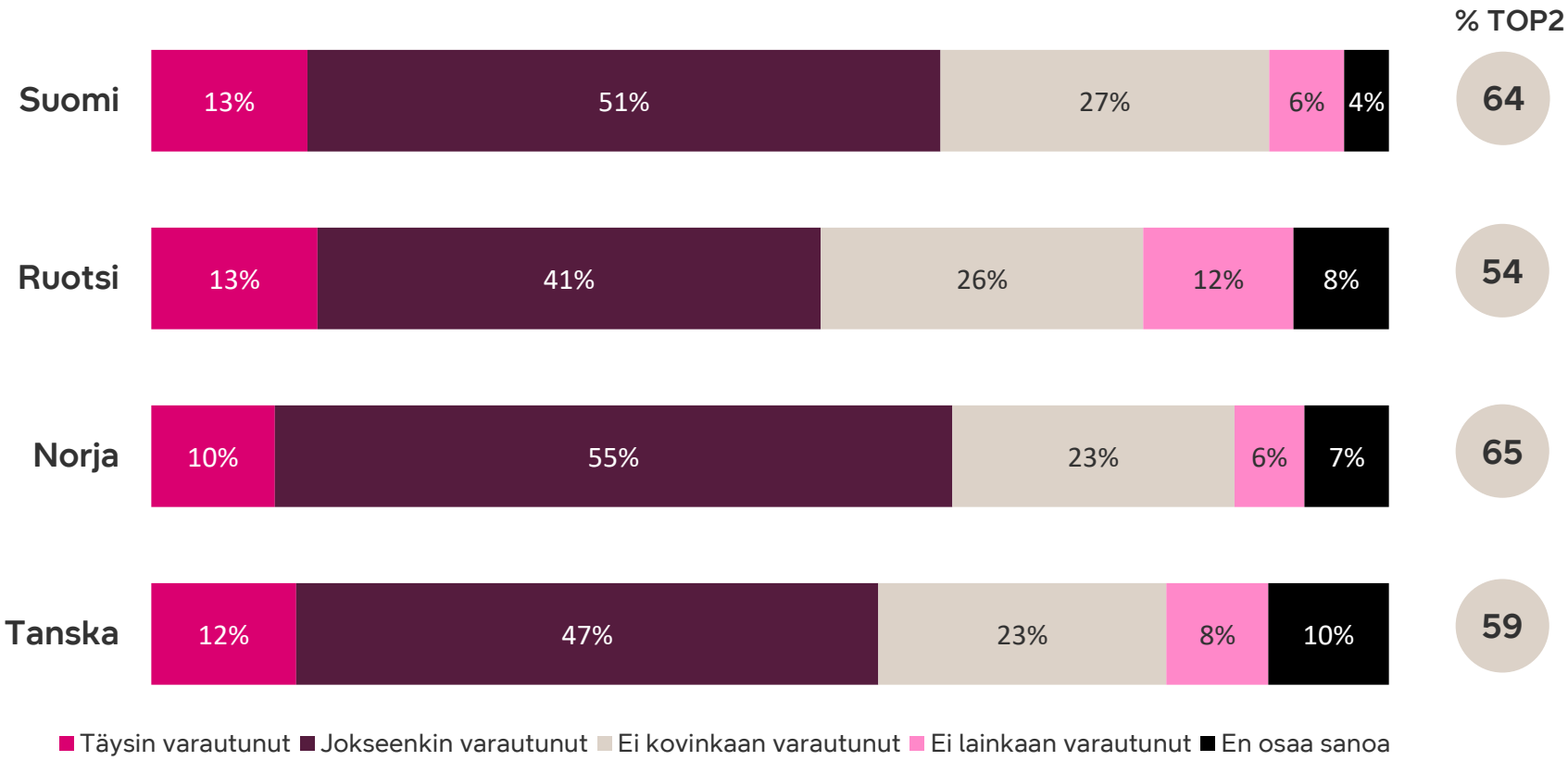
part of telenor

Sensitivity: Open

Pohjoismainen tietoturvatutkimus 2026

Organisaatioiden valmius havaita tekoäly-avusteisia kyberuhkia ja reagoida niihin

? Kuinka hyvin organisaatiosi on varautunut tunnistamaan tekoälyn mahdollistamia kyberuhkia ja reagoimaan niihin?



Useimmat organisaatiot arvioivat olevansa ainakin jossain määrin valmistautuneita havaitsemaan tekoälyavusteisia kyberuhkia ja reagoimaan niihin.

Koettu valmius on vahvin Norjassa, jossa 65 prosenttia vastaajista arvioi organisaationsa olevan valmistautunut. Suomessa vastaava osuus on 64 prosenttia, Tanskassa 59 prosenttia ja Ruotsissa 54 prosenttia.

Vain 10–13 prosenttia vastaajista arvioi organisaationsa olevan täysin valmistautunut. Ruotsissa yleinen valmiustaso arvioitiin maista matalimmaksi, ja 38 prosenttia vastaajista arvioi, ettei heidän organisaationsa ole valmistautunut tekoälyavusteisiin kyberuhkiin.

Tulokset osoittavat, että organisaatioilla on yleisesti jonkinasteisia valmiuksia, mutta vain harvat arvioivat olevansa täysin varautuneita tekoälyavusteisten kyberuhkien hallintaan.

©DNA

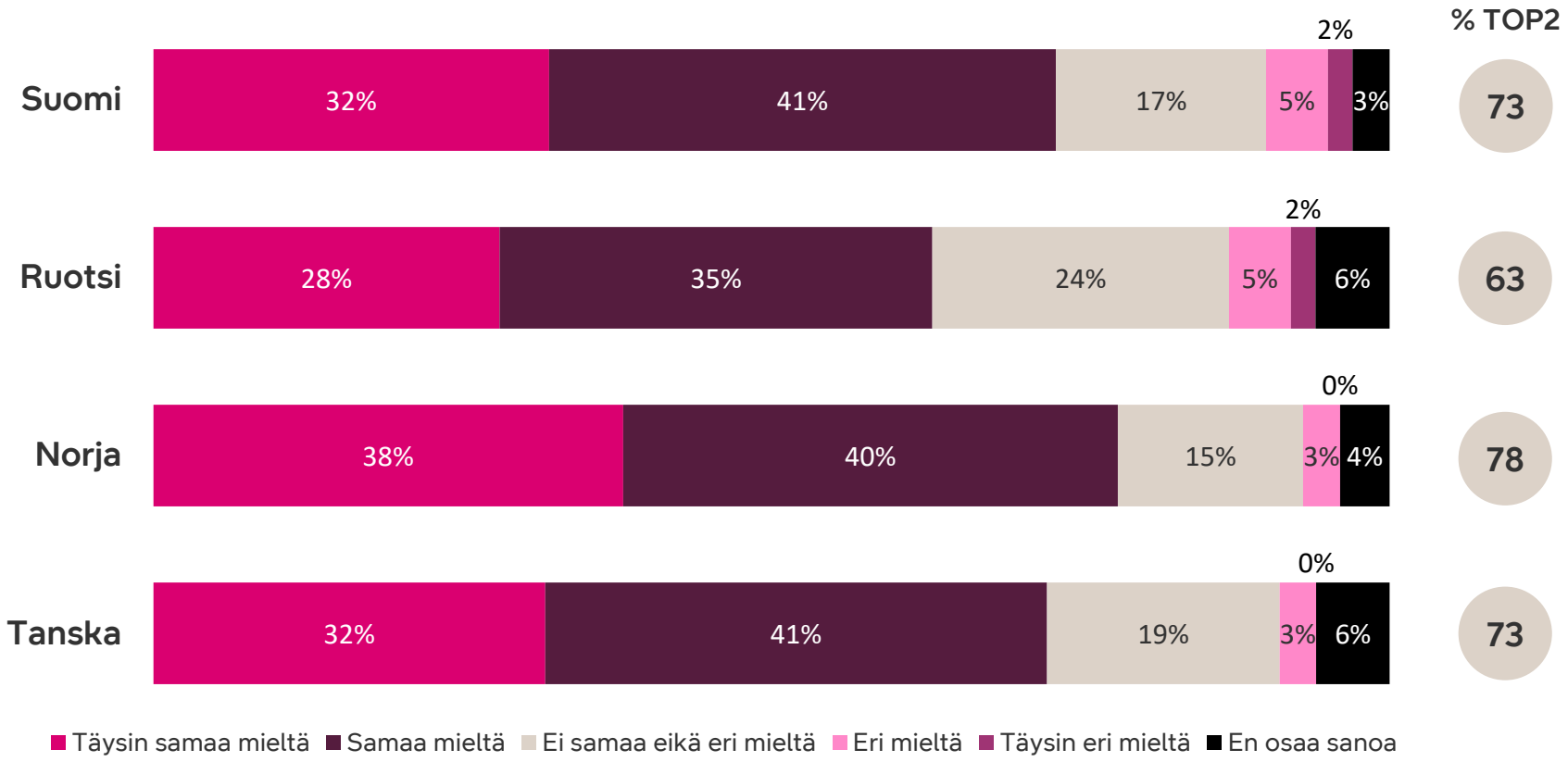
part of telenor

Sensitivity: Open

Pohjoismainen tietoturvatutkimus 2026

Digitaalisen suvereniteetin merkitys

? Missä määrin olet samaa tai eri mieltä seuraavan väittämän kanssa?
Digitaalinen suvereniteetti, mukaan lukien se, missä kriittistä dataa säilytetään, kenellä on pääsy siihen ja minkä lainsäädännön piirissä sitä suojataan, tulee olemaan yhä tärkeämpää organisaatiolleni.



Digitaalisen suvereniteetin merkityksen arvioidaan kasvavan kaikissa neljässä maassa.

Samaa mieltä olevien osuus on suurin Norjassa, 78 prosenttia. Tanskassa ja Suomessa osuus on 73 prosenttia ja Ruotsissa 63 prosenttia.

Norjassa täysin samaa mieltä olevien osuus on erityisen suuri, 38 prosenttia. Ruotsissa puolestaan neutraalisti suhtautuvien osuus on suurin, 24 prosenttia.

Kokonaisuutena tulokset osoittavat laajaa kannatusta sille, että organisaatiot voivat hallita kriittisten tietojen tallennuspaikkaa, käyttöoikeuksia ja tietojen suojaamiseen sovellettavaa lainkäyttöaluetta.

©DNA

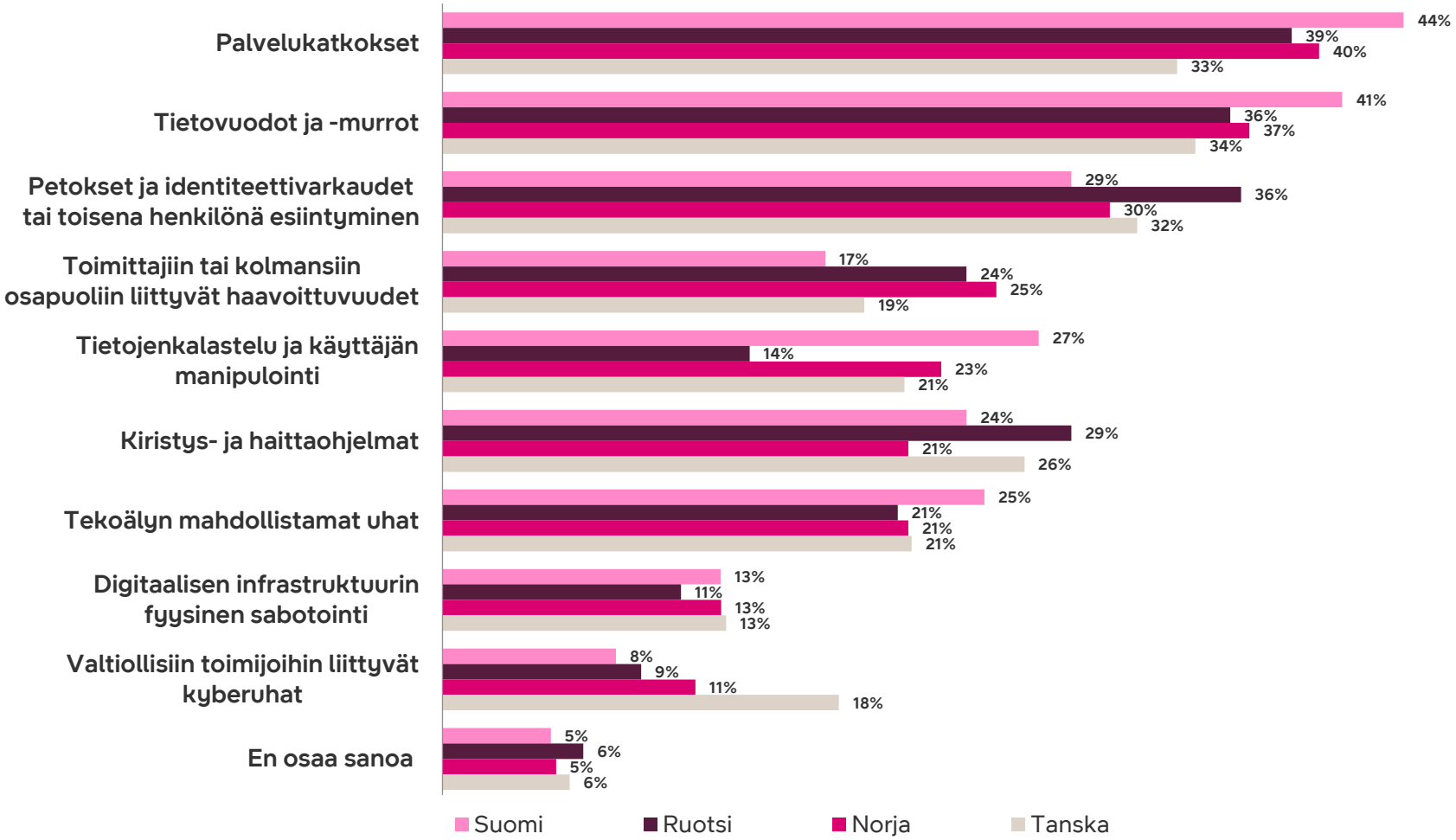
Sensitivity: Open

part of telenor

Pohjoismainen tietoturvatutkimus 2026

Organisaatioita eniten huolestuttavat digitaaliset uhat

? Mitkä seuraavista digitaalisista uhista ovat oman organisaatiosi kannalta suurimpia huolenaiheita? Valitse enintään kolme vastausvaihtoehtoa.



Palvelukatkokset ovat yleisin huolenaihe Suomessa, Norjassa ja Ruotsissa. Ne mainitsee 39–44 prosenttia vastaajista. Myös Tanskassa palvelukatkokset kuuluvat keskeisimpiin huolenaiheisiin, ne mainitsee 33 prosenttia vastaajista.

Tietomurrot nousevat johdonmukaisesti keskeisten huolenaiheiden joukkoon kaikissa neljässä maassa. Niistä huolestuneiden osuus vaihtelee Tanskan 34 prosentista Suomen 41 prosenttiin.

Huolenaiheissa on myös maakohtaisia eroja. Petokset ja toisena henkilönä esiintyminen korostuvat erityisesti Ruotsissa ja Tanskassa. Kiristyshaittaohjelmat ja muut haittaohjelmat mainitaan yleisimmin Ruotsissa.

Suomessa korostuvat muita maita enemmän tietojenkalastelu ja sosiaalinen manipulointi, jotka mainitsee 27 prosenttia vastaajista, sekä tekoälyavusteiset uhat, jotka mainitsee 25 prosenttia vastaajista.

Toimittajiin tai muihin kolmansiin osapuoliin liittyvät haavoittuvuudet sekä digitaaliseen infrastruktuuriin kohdistuva fyysinen sabotaasi mainitaan harvemmin. Valtiollisiin toimijoihin yhdistetty kybertoiminta herättää selvästi eniten huolta Tanskassa, jossa sen mainitsee 18 prosenttia vastaajista.

©DNA

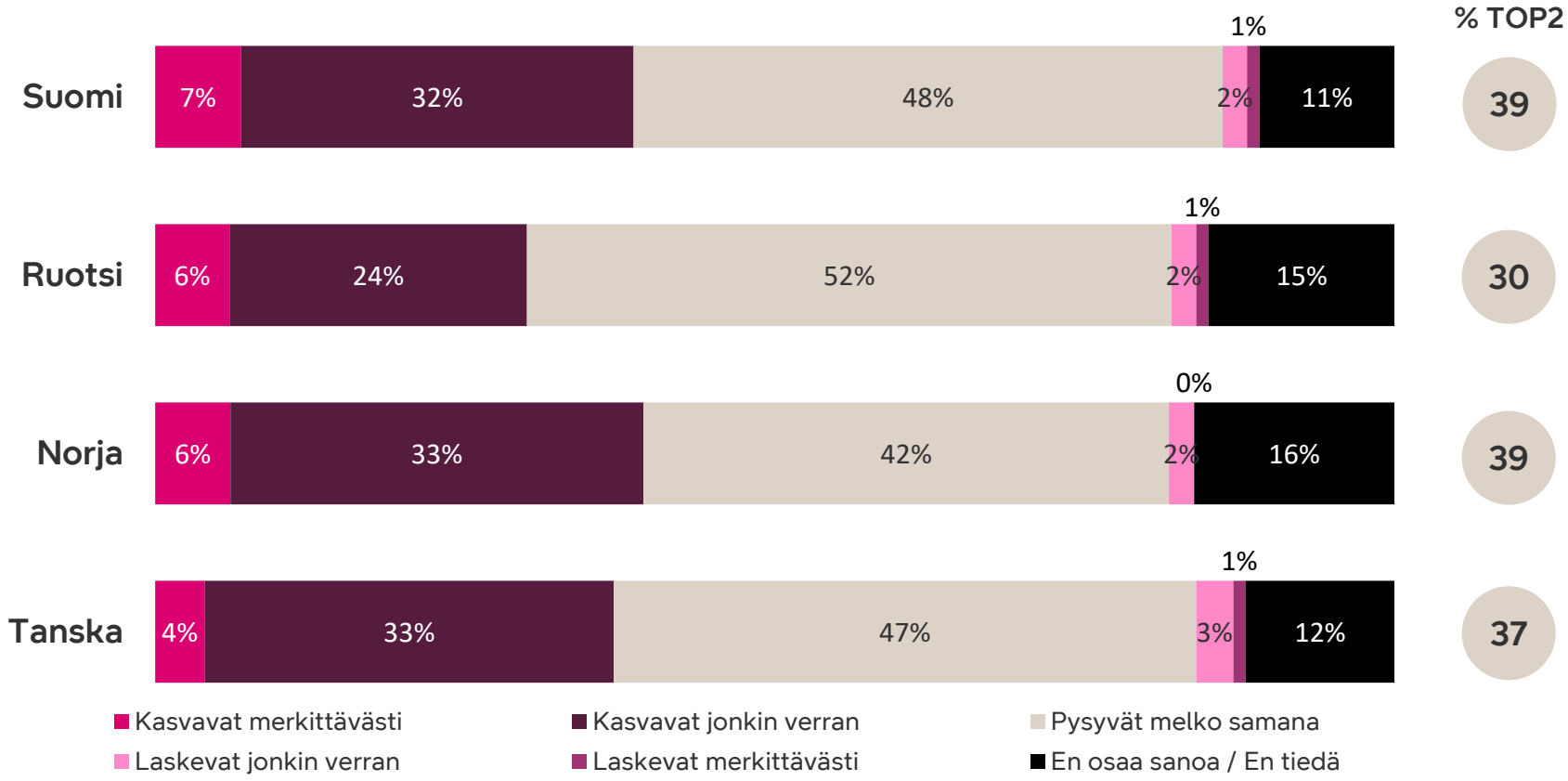
Sensitivity: Open

part of telenor

Pohjoismainen tietoturvatutkimus 2026

Muutokset kyberturvallisuuteen ja digitaaliseen resilienssiin tehtävissä investoinneissa

? Miten organisaatiosi investoinnit kyberturvallisuuteen ja digitaalisen toimintakyvyn takaamiseen tulevat kehittymään seuraavien 12 kuukauden aikana kuluneeseen 12 kuukauteen verrattuna?



Useimmat organisaatiot arvioivat kyberturvallisuuteen ja digitaaliseen resilienssiin tehtävien investointien säilyvän seuraavien 12 kuukauden aikana suunnilleen ennallaan.

Investointien ennallaan säilymistä odottaa Ruotsissa 52 prosenttia, Suomessa 48 prosenttia, Tanskassa 47 prosenttia ja Norjassa 42 prosenttia vastaajista.

Odotukset investointien kasvusta ovat vahvimmat Norjassa ja Suomessa. Molemmissa maissa 39 prosenttia vastaajista ennakoi investointien kasvavan. Tanskassa vastaava osuus on 37 prosenttia ja Ruotsissa 30 prosenttia.

Vain pieni osa vastaajista arvioi investointien vähenevän. Verrattain suuri osa ei kuitenkaan osaa ennakoida investointien kehitystä. Epävarmuus on suurinta Norjassa, jossa 16 prosenttia ei osaa vastata, sekä Ruotsissa, jossa vastaava osuus on 15 prosenttia.

©DNA

part of telenor

Sensitivity: Open

Yhteenveto

Kyberturvallisuuden merkitys kasvaa, mutta varautuminen ja investoinnit eivät kehity samaa tahtia.

- Kyberturvallisuus ja digitaalinen resilienssi ovat keskeisiä teemoja kaikkialla Pohjoismaissa. Turvallisuuden ja resilienssin merkitys hankintakriteereinä on kasvanut erityisesti Tanskassa (61 %), Norjassa (60 %) ja Suomessa (60 %).
- Digitaalisen suvereniteetin merkitys tunnistetaan kaikissa Pohjoismaissa. Samaa mieltä olevien osuus vaihtelee Ruotsin 63 prosentista Norjan 78 prosenttiin.
- Palvelukatkokset ja tietomurrot ovat keskeisimmät organisaatioita huolestuttavat digitaaliset uhat. Myös petokset, kiristyshaittaohjelmat ja tekoälyavusteiset uhat korostuvat tuloksissa, mutta niiden merkityksessä on maakohtaisia eroja.
- Organisaatiot arvioivat varautumisensa pikemminkin kohtalaiseksi kuin vahvaksi. Noin puolet kokee olevansa valmistautunut ylläpitämään kriittisiä toimintoja vakavan digitaalisen häiriön aikana. Vain 10–13 prosenttia arvioi organisaationsa olevan täysin valmistautunut vastaamaan tekoälyavusteisiin kyberuhkiin.
- Investointinäkymät ovat varovaisia. Vastaajista 30–39 prosenttia odottaa kyberturvallisuuteen ja digitaaliseen resilienssiin tehtävien investointien kasvavan, kun taas noin puolet arvioi niiden säilyvän ennallaan.



©DNA

part of telenor

Sensitivity: Open

Pohjoismainen tietoturvatutkimus 2026

DNA osana Telenor Groupia:

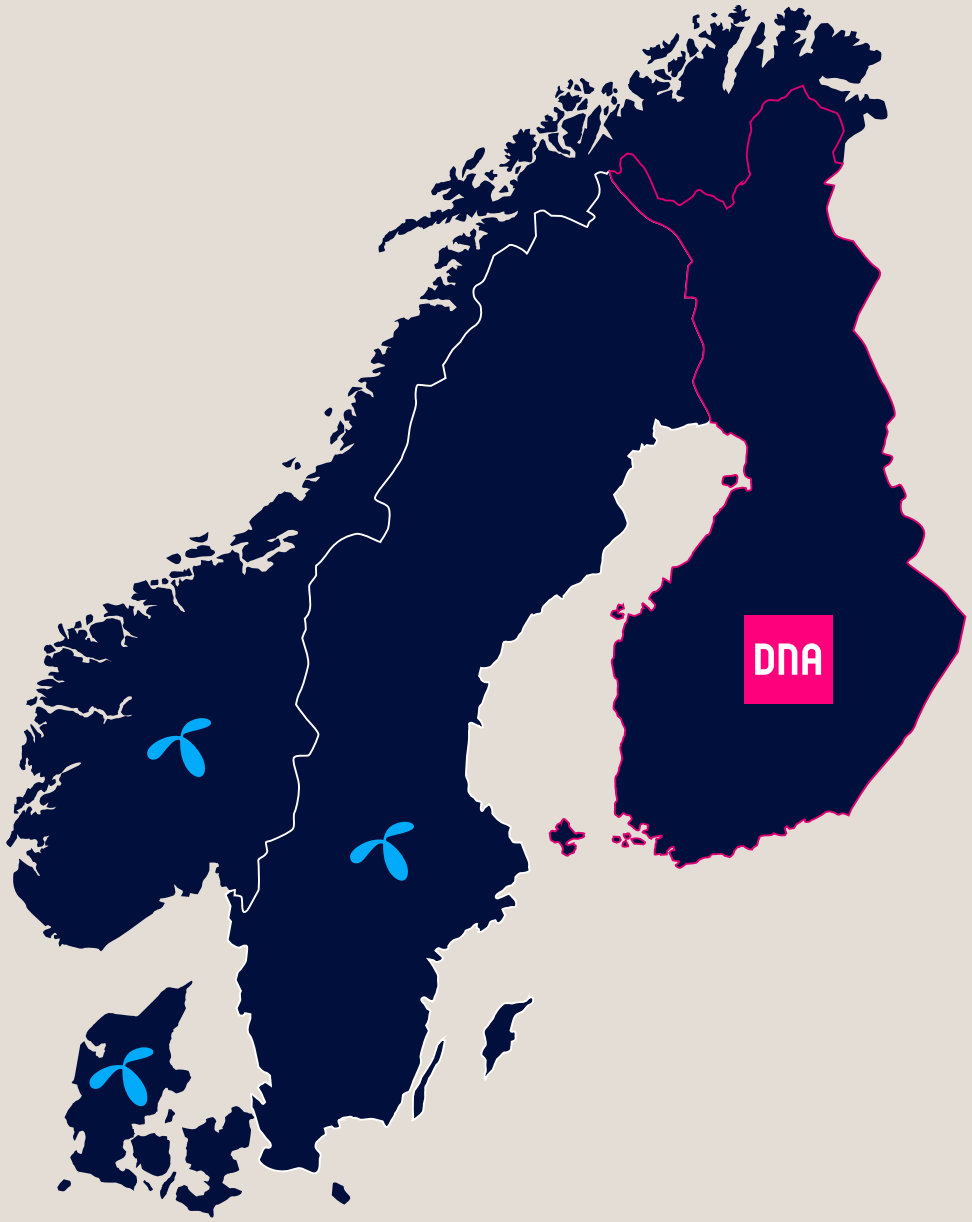
Pohjoismaiden suurin tietoliikennetoimija

DNA on osa pohjoismaalaista Telenor-konsernia, joka on yksi Pohjoismaiden suurimpia tietoliikenneyhtiöitä.

- 207 miljoonaa mobiiliasiakasta
- 250 miljoonaa estettyä huijauspuhelua vuosittain
- 200 kyberturvallisuuden asiantuntijaa
- 400 roaming-kumppania
- 10 miljoonaa mobiililiittymää Pohjoismaissa
- 2,3 miljoonaa laajakaista- ja kituliittymää Pohjoismaissa

Investoimme jatkuvasti pohjoismaisen mobiili- ja kiinteän verkkoinfrastruktuurin sekä kyvykkyyksien kehittämiseen.

Laajan yhteistyön ansiosta voimme tarjota asiakkaillemme kaikkialla Pohjoismaissa kestäviä, turvallisia ja innovatiivisia ratkaisuja, jotka perustuvat vankkaan asiantuntemukseemme.



part of telenor

©DNA

Sensitivity: Open

Kiitos.

dna.fi/pohjoismainen-tietoturvatutkimus-2026

part of telenor