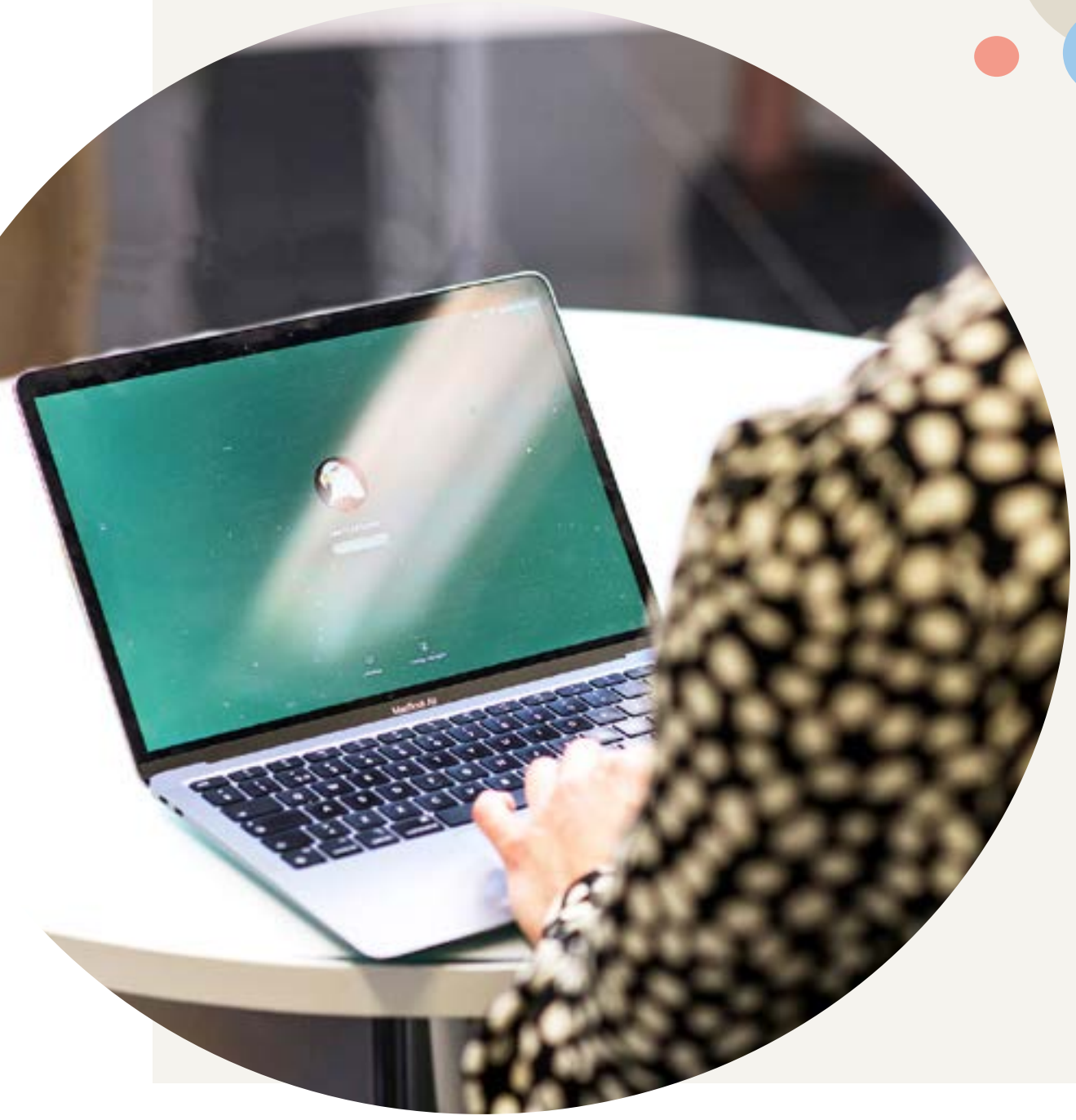
Selvitys 2022

Yrityksiin kohdistuvat kyberuhat



HELSINGIN SEUDUN
KAUPPAKAMARI

JOHDANTO

Selvityksessä tutkitaan suomalaisten yritysten käsityksiä niihin kohdistuvista kyberuhista ja niihin varautumisesta.

Yritykset vastasivat kyselyyn syyskuussa 2022. Tulokset on esitetty taulukkoina ja kuvioina, joista yksittäisen vastaajan mielipide ei käy ilmi. Selvitys perustuu 258 suomalaisen yrityksen antamiin vastauksiin.

Selvityksen ovat laatineet asiantuntija **Panu Vesterinen** Helsingin seudun kauppakamarista ja kehityspäällikkö **Petteri Korsow** Avarn Security Oy:stä.

Selvitys on osa Helsingin seudun kauppakamarin yritysturvallisuustoimintaa.

Kyselyyn vastanneista yrityksistä 50 prosenttia edustaa palveluita, 14 prosenttia kauppaa, 10 prosenttia teollisuutta ja rakennusalaa 6 prosenttia.

Vastanneista yrityksistä 75 prosenttia oli henkilömäärältään pieniä yrityksiä, jotka työllistävät alle 50 henkilöä. Vastaajista 10 prosenttia oli keskisuuria yrityksiä, joiden palveluksessa on 50–200 työntekijää. Suuria yli 200 henkilöä työllistäviä vastaajia oli 15 prosenttia.

Tässä selvityksessä ei jaeta tuloksia kokoluokan mukaan, koska jokainen yritys kokoon tai toimialaan katsomatta on potentiaalinen kyberrikoksen kohde tai saattaa olla reitti toiseen yritykseen. Yritykset muodostavat suuren hyökkäyspinta-alan, josta kyberrikolliset valitsevat omalta kannaltaan kulloisenkin tavoitteen mukaisen parhaan kohteen. Selvityksessä on paikka paikoin yleisluontoista vertailua vuosien 2015 ja 2019 ”Yrityksiin kohdistuvat kyberuhat” -selvitysten tuloksiin.

Vastaajat olivat yritysten toimitusjohtajia (25 %), yrittäjiä tai omistajia (39 %), muita johtajia (14 %). Päällikkötason tehtävissä vastaajista oli yhdeksän prosenttia. Selvityksessä on tavoitettu päätöksentekijät – turvallisuuden kehittämisen kannalta tärkeä resursseista päättävä ryhmä.

Selvityksessä on kursiivilla lainauksia yritysten vapaamuotoisista vastauksista.

Selvityksen tavoitteena on tukea ja kehittää yritysten omaa riskienhallintatyötä. Tuloksista yritykset saavat paremman kokonaiskuvan kyberuhista ja siitä, miten uhkiin on osattu varautua. Tämä puolestaan auttaa torjumaan yrityksiin kohdistuvia uhkia.

Helsingissä marraskuussa 2022

Sisällys

JOHDANTO 1

KYSELYN TULOKSET 4

Mitkä ovat suurimmat uhat yritysten kyberturvallisuudelle? 4

Mitkä ovat kolme suurinta estettä tehokkaan kyberturvallisuuden toteuttamisessa? 5

Mitkä seuraavista vaihtoehdoista ovat raskaimmat seuraukset kyberhyökkäyksistä? 6

Miten hyvin viranomaisten roolit tunnetaan? 7

Onko saanut käytännöllistä tietoa kyberuhkiin liittyen? 8

Miten organisaatio havaitsisi yrityksen tietoverkossa käynnissä olevan tunkeutumisen? 9

Minkälaista tietoa luulette tunkeutujien etsivän? 11

Minkä tyyppistä tietoa olette menettäneet tietoverkkotunkeutumisten vuoksi? 13

Miten organisaationne on järjestänyt tietoturvallisuusvastuut johtotasolla? 15

Tietääkö henkilökunta, miten toimia, jos he epäilevät tunkeutumista tietojärjestelmiinne? 16

Onko teillä käytössä käytännössä toimivia suunnitelmia tunkeutumisten varalle? 17

Mitä asioita suunnitelmiin on sisällytetty? 18

Oletteko koskaan harjoitelleet suunnitelmienne toimivuutta jollakin seuraavista tavoista? 19

Oletteko varautuneet kyberuhkiin seuraavin tavoin konkreettisesti tai suunnitelmilla? 20

Onko teillä vahvistettua koulutus- ja harjoitusohjelmaa kyberturvallisuuteen liittyen? 21

Ovatko kyberuhkiin liittyvät harjoitukset osa muihin liiketoimintaa uhkaaviin uhkiin liittyvää harjoittelua? 22

Oletteko viimeisen neljän vuoden aikana kohdistaneet kyberturvallisuuteenne jotain seuraavista toimenpiteistä? 23

UHKAHORISONTIN MUUTOS 24

COVID19 -pandemian aiheuttamat heijastevaikutukset 24

Venäjän hyökkäyssota Ukrainaa vastaan 25

Etätyöhön liittyvät tietoturvariskit 26

Hybridivaikuttamisen kohteeksi joutuminen suoraan tai välillisesti 27

Valtiollisten toimijoiden vihamielinen toiminta (vaikutus suora tai välillinen) 28

Kohdistettu tietojenkalastelu ja social engineering 29

IoT-laitteiden yleistymisen ja niihin liittyvät tietoturvariskit 30

Tietosuojaan ja yksityisyydensuojaan liittyvät uhat (ml. seuraamukset ja sanktiot) 31
Toimitusketjuihin liittyvät uhat 32
SOME:ssa kohdistetun vihamielisen kampanjan kohteeksi joutuminen 33
Henkilökunnan riittävä koulutus muuttuvien ja kehittyvien uhkien suhteen 34
Sisäpiiriuhat 35
Uhkahorisontin muutoksen vaikutus riskeihin kokonaisuudessaan 36
JOHTOPÄÄTÖKSET 37

KYSELYN TULOKSET

Mitkä ovat suurimmat uhat yritysten kyberturvallisuudelle?

Phishing- ja haittaohjelmahyökkäykset	77 %
Tunkeutumiset	37 %
Palvelunestohyökkäykset	32 %
Yhtiön sisäinen uhka (omat työntekijät)	29 %
Hyökkäykset, jotka kohdistuvat teollisiin tuotantoprosesseihin	8 %
Muu, mikä?	1 %

Yli kaksi kolmasosaa yrityksistä piti phishing- tai haittaohjelma-hyökkäyksiä suurimpana uhkana. Aiheina ne ovat olleet viime vuosina paljon julkisuudessa. Tiedottaminen ja keskustelun ylläpitäminen ovat olleet toimiva tapa jakaa tietoa yrityksille. Toiseksi suurimpana uhkana yli kolmasosa vastaajayrityksistä piti tietojärjestelmiin tunkeutumisten uhkaa. Kolmanneksi yleisimpänä uhkana palvelunestohyökkäykset voivat estää väliaikaisesti yrityksen digitaalisen liiketoiminnan.

Mikä yritys tahansa saattaa joutua kyberrikoksen kohteeksi ja uhka kohdistuu useimmin yritykseen sen ulkopuolelta. Mikäli yritys ei pidä uhkaa todellisena, on epätodennäköistä, että se kehittäisi kyberturvallisuuttaan. Yritys, joka ei ole kybervalveutunut, on helppo kohde rikollisille. Se ei edes aina huomaa tulleensa rikoksen kohteeksi.

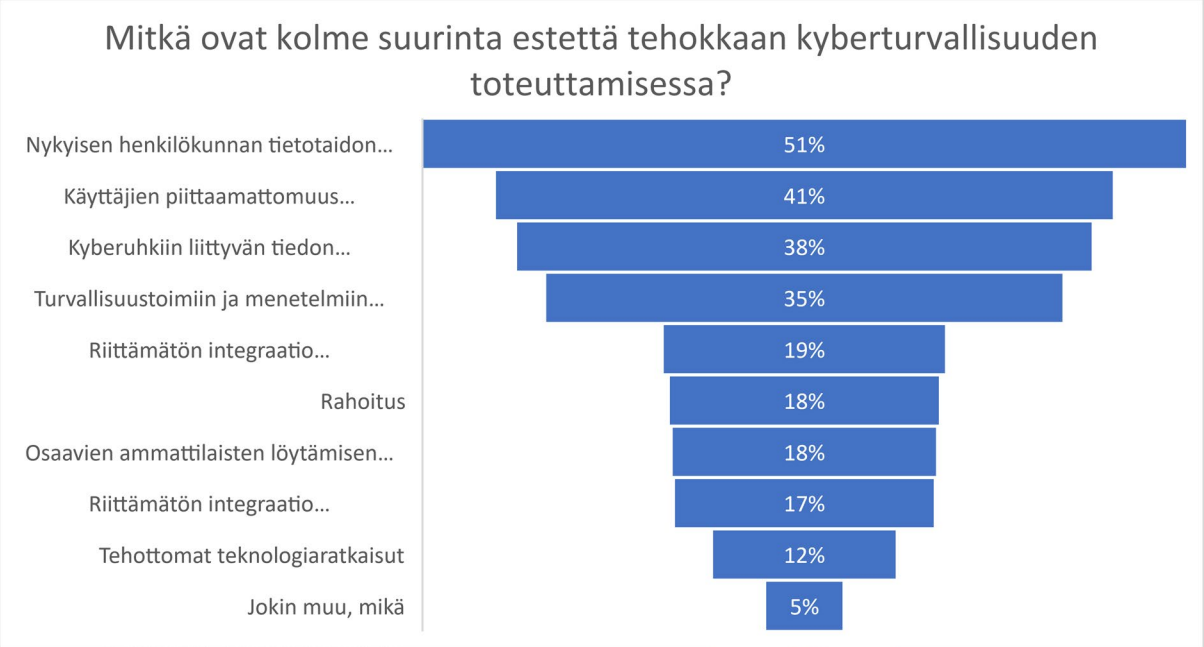
”Ratkaisujen kustannukset suhteessa yrityksen kokoon”

”Johdon tuki kyberturvallisuuden kehittämiselle”

”Liikaa asioita siirretty sähköiseen muotoon”

”Tietojen tuhoaminen”

Mitkä ovat kolme suurinta estettä tehokkaan kyberturvallisuuden toteuttamisessa?



Nykyisen henkilökunnan tietotaidon ylläpitäminen kyberuhkien suhteen	51 %
Käyttäjien piittaamattomuus tietoturvallisuudesta ja kyberuhista	41 %
Kyberuhkiin liittyvän tiedon riittämättömyys	38 %
Turvallisuustoimiin ja menetelmiin liittyvän tiedon riittämättömyys	35 %
Riittämätön integraatio kyberturvallisuuden ja liiketoiminnan välillä	19 %
Rahoitus	18 %
Osaavien ammattilaisten löytämisen vaikeus	18 %
Riittämätön integraatio kyberturvallisuuden ja muiden turvallisuuden osa-alueiden välillä (jatkuvuussuunnittelu, kriisienhallinta jne.)	17 %
Tehottomat teknologiaratkaisut	12 %
Jokin muu, mikä	5 %

Suurimmaksi esteeksi nousi henkilökunnan kyberuhkiin liittyvän tietotaidon ylläpito. Toiseksi yleisin este on käyttäjien piittaamattomuus tietoturvallisuudesta ja kyberuhista, jolla on yhteys tietotaidon ylläpitoon. Mikäli ihminen ei ymmärrä uhkaa eikä tiedä miten se ilmenee hänen arjessaan, on vaikea odottaa hänen osaavan toimia oikein ja tällöin voi helpommin olla piittaamaton kyberturvallisuudesta. Kolmanneksi ja neljänneksi suurimmat esteet liittyivät tiedon vähäisyyteen, kyberuhkiin ja turvallisuusmenetelmiin liittyvää tietoa ei vieläkään ole saatavissa yritysten tietoisuuteen.

Tiedon saatavuus on yhä este yritysten kyberturvallisuuden kehittämiselle. Yritysten on oltava aktiivisia tiedonhaussaan, mutta ymmärrettävää tietoa tulisi olla helpommin tarjolla ja sen olemassaolosta tulisi tiedottaa nykyistä enemmän. Kyberturvallisuuskeskus tekee paljon käyttökelpoista materiaalia, mutta jostain syystä yritykset eivät löydä sitä.

”Pienelle yritykselle suhteellisen kovat kustannukset”

”Kyberuhkiin liittyvän tiedon viestintä ymmärrettävässä muodossa ei-asiantuntijoille”

Mitkä seuraavista vaihtoehdoista ovat raskaimmat seuraukset kyberhyökkäyksistä?

Yksityisyyden (henkilökunnan tai asiakkaiden tiedot) loukkaus	59 %
Tuoton menetys – suora tai epäsuora	42 %
Aineettoman omaisuuden menetys	34 %
Negatiivinen julkisuus	29 %
Kansallisen turvallisuuden vaarantuminen	24 %
Markkinaosuuden menetys	5 %
Jokin muu, mikä	4 %

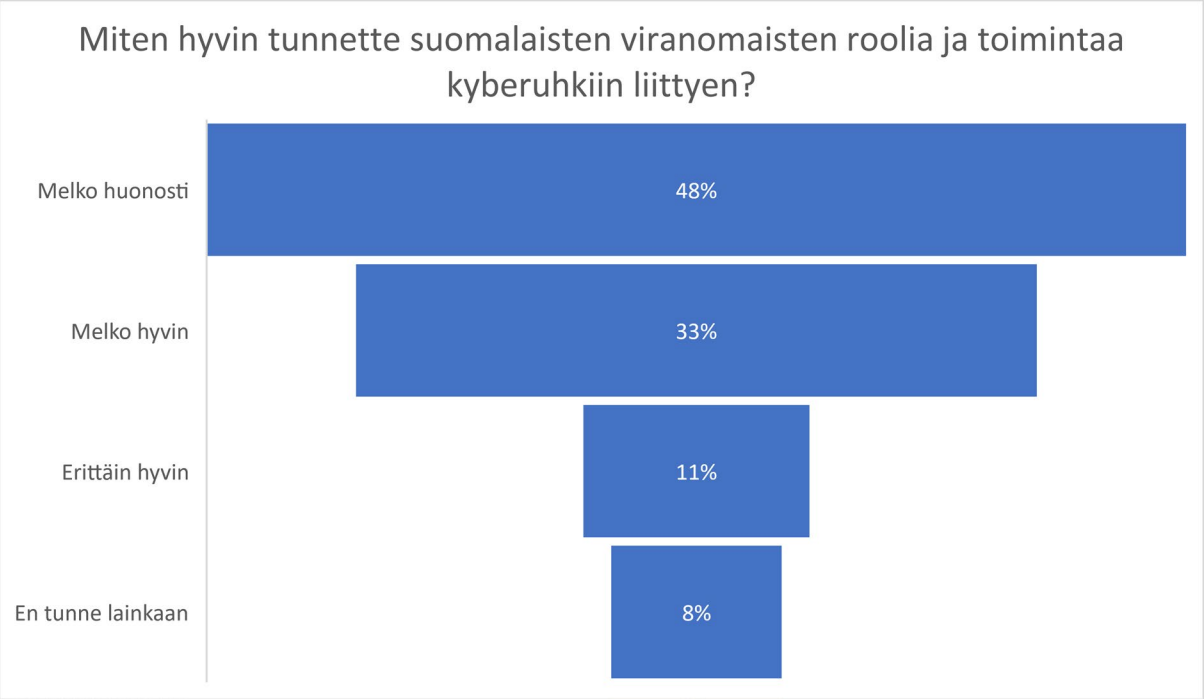
Raskaimpana seurauksena pidettiin henkilökunnan tai asiakkaiden yksityisyyden loukkausta. Julkisuudessa ollut Vastaamo-tapaus on nostanut loukkauksen seurauksia esille ja on hyvä, että yritykset tunnistavat sen merkityksen. Toiseksi raskain seuraus oli tuoton menetys. Aineettoman omaisuuden menetys ja negatiivinen julkisuus olivat kolmanneksi ja neljänneksi raskaimmat seuraukset. Kansallisen turvallisuuden vaarantumisesta pidettiin viidenneksi raskaimpana seurauksena.

Tällä kysymyksellä tavoiteltiin yritysten tietoisuutta siitä, mitä kaikkea kyberrikoksesta voi seurata ja mitä asioita kannattaa suojata. Kyberturvallisuudessa ei ole kyse vain liikesalaisuuksien suojaamisesta, vaan seuraukset voivat vaihdella aina kansallisen turvallisuuden vaarantumiseen saakka.

”Asiakasorganisaatioiden prosessien rampautuminen”

”Tuotannon keskeytyminen - ajan menetys, ei niinkään tuoton”

Miten hyvin viranomaisten roolit tunnetaan?

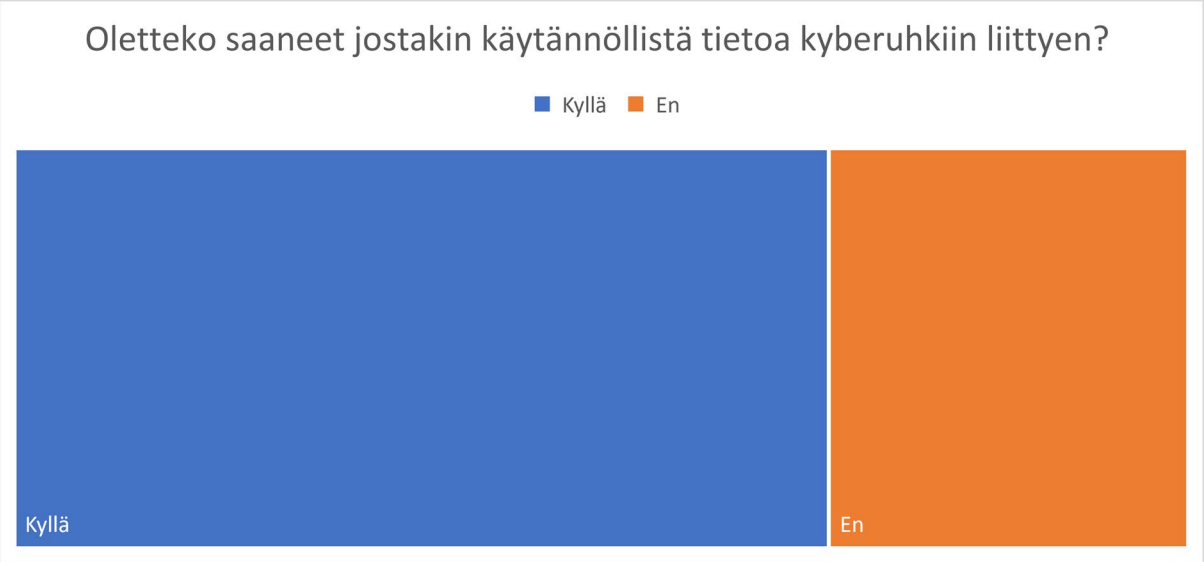


Melko huonosti	48 %
Melko hyvin	33 %
Erittäin hyvin	11 %
En tunne lainkaan	8 %

Kaikista vastaajista hieman yli puolet tunsi vähintään melko huonosti viranomaisten roolia ja toimintaa. Suuresta osuudesta huolimatta asiassa on seitsemän vuoden aikana tapahtunut myönteistä kehitystä. Niiden osuus, jotka eivät tunne lainkaan viranomaisten roolia, on puolittunut ja melko huonosti tuntevien osuus on vähentynyt melkein neljänneksen.

Vastaavasti toimintaa tuntevien määrä on noussut. Sekä erittäin hyvin että melko hyvin tuntevien osuus on kaksinkertaistunut. Tämä osoittaa viranomaistiedottamisen onnistuneen. Tietoisuus viranomaisten roolista helpottaa yritysten toimintaa kyberrikoksen tapahtuessa. Viranomaiset toivovat ilmoituksia yritysten kohtaamista tapauksista, mutta jolleivat yritykset tunne viranomaisten rooleja, ei ilmoitusaktiivisuus tule nousemaan suuressa määrin. Ilmoittaminen edellyttää tietynasteista luottamusta ja jos yritys ei tunne viranomaisia, ei riittävää luottamustakaan välttämättä ole.

Onko saanut käytännöllistä tietoa kyberuhkiin liittyen?



Kyllä	69 %
En	31 %

Yli kaksi kolmasosaa on saanut käytännöllistä tietoa kyberuhkiin liittyen. Tämä tarkoittaa kuitenkin sitä, että kolmasosaa yrityksistä ei ole saanut tai etsinyt tietoa kyberuhista. Seitsemän vuoden aikana tietoa saaneiden määrä on kuitenkin lähes kaksinkertaistunut. Tästäkin on syytä kiittää erityisesti viranomaisten tiedotustyötä ja ponnistelua tiedon jakamiseksi.

Yrityksillä on toisinaan vaikeuksia tunnistaa kyberuhkia ja sitä kautta varautua niihin. Kyse on kilpajuoksusta, jossa rikolliset kehittävät uusia keinoja aina kun vanhat tulevat tunnetuiksi ja käyttävät mielellään vanhoja toimivia konsteja, jos yritykset eivät saa tietoa niistä. Vastuu tiedon etsimisestä on kuitenkin yrityksillä itsellään. Yritykset eivät voi odottaa, että viranomaiset ja teleoperaattorit hoitavat kaiken asiaan liittyvän yrityksen odottaessa passiivisena.

”Yrityksen itsensä hankkimana (=kyvykkyys), HVO digipoolin tilaisuudet, globaalit kollegat, viranomaisten verkkosivuinformaatio”

”Konsulttiyritykseltä sekä suojelupoliisilta”

”Kyberturvallisuuskeskuksen tiedotteet”

”Huoltovarmuuskeskukselta”

Miten organisaatio havaitsisi yrityksen tietoverkossa käynnissä olevan tunkeutumisen?

Havaitsisimme sen itse käyttäen omia torjunta- ja hälytysjärjestelmiämme	34 %
Kolmas taho, kuten internet operaattori tai palveluntarjoaja, ilmoittaisi meille	28 %
Me emme todennäköisesti havaitsisi käynnissä olevaa tunkeutumista	21 %
Tunnistaisimme itse, koska tarkastamme ja analysoimme lokejamme ja arvioimme niistä ilmenevää uhkaan olemassaoloon liittyvää tietoa	8 %
Käyttäjämme tunnistaisivat sen ja ilmoittaisivat eteenpäin	8 %
Kotimaiset lainvalvontaviranomaiset tai tiedusteluorganisaatiot varoittaisivat meitä	2 %

Useimmin yritykset havaitsisivat hyökkäyksen itse käyttäen omia torjunta- ja hälytysjärjestelmiä. Toiseksi yleisin tapa olisi kolmannen tahon, operaattorin tai palveluntarjoajan ilmoitus kohteena olevalle yritykselle. Kolmanneksi yleisin vastausvaihtoehto on valitettavasti se, ettei yritys todennäköisesti havaitsisi käynnissä olevaa tunkeutumista. Viidesosalla vastaajayrityksistä ei ole valmiuksia tunnistaa kyberhyökkäystä.

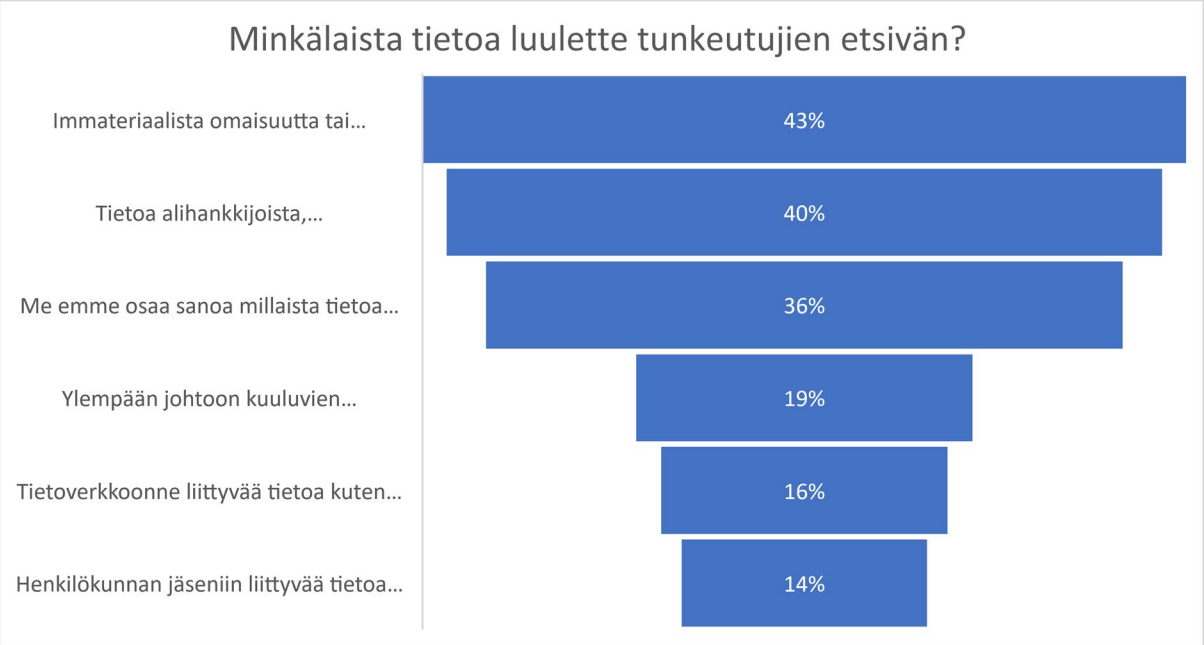
Tunnistaminen ei ole helppoa ja viime aikoina on arvioitu kohdeorganisaatiolla kestävän keskimäärin jopa 200 vuorokautta havaita tunkeutuminen, jos sitä edes havaitaan. Tunnistamiskyvyn kehittäminen on jatkuva haaste yrityksille. Jos ei kykene tunnistamaan tietoverkossaan tapahtunutta kyberrikosta, miten yrityksen johto voi vakuuttaa omistajat siitä, että yrityksen toimintaa on suojattu asianmukaisesti?

Moni yritys voi myös tietämättään olla reitti asiakkaan tai yhteistyökumppanin tietojärjestelmiin. Tai yrityksen hallussa ollut asiakkaan luottamuksellinen tieto on voitu viedä sen ja sen asiakkaan tietämättä. Tällaisen rikoksen paljastuminen jälkikäteen on merkittävä riski kohdeyrityksen asiakassuhteille. Myös yritysostotilanteissa tapahtuvat kyber due diligence -selvitykset ovat alkaneet yleistyä ja niiden tuloksilla on ollut alentava vaikutus kauppahintaan.

”Olemme onnistuneet tunnistamaan ja estämään useita hyökkäyksiä”

”Toistaiseksi olemme pystyneet tunnistamaan pfishing -yritykset, mutta uskon, että on vain ajan kysymys, kun jossain kohtaa inhimillisen erehdyksen kautta tietomurto pääsee tapahtumaan”

Minkälaista tietoa luulette tunkeutujien etsivän?



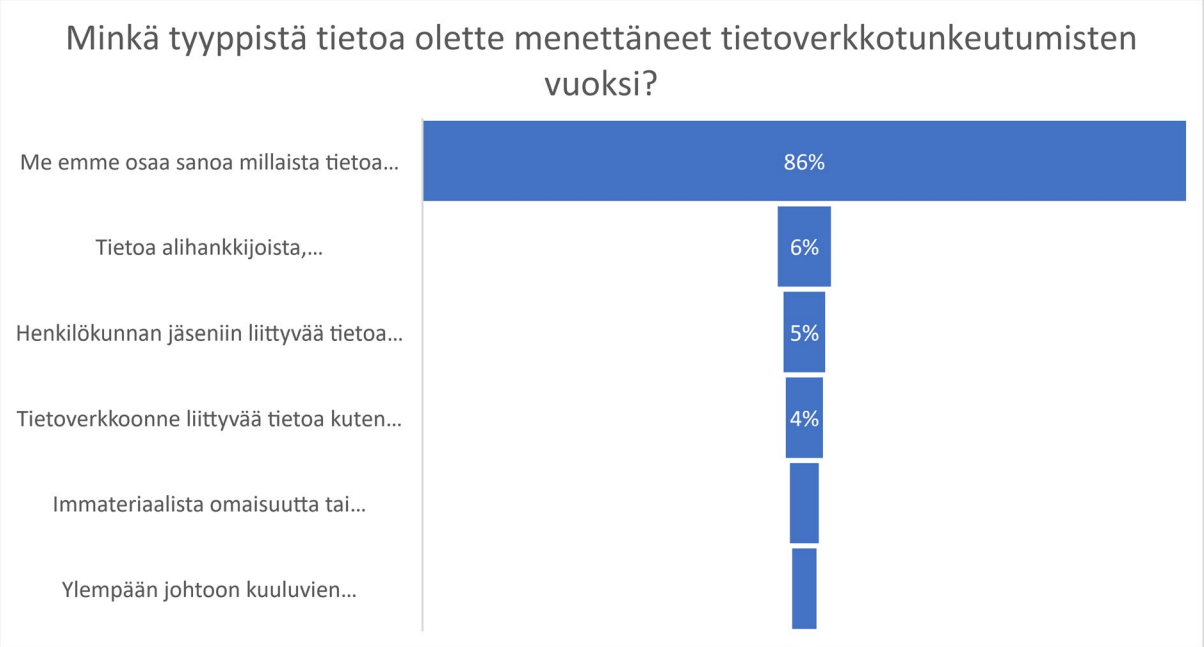
Immateriaalista omaisuutta tai luottamuksellista tietoa tuotteistamme tai palveluistamme	43 %
Tietoa alihankkijoista, yhteistyökumppaneista, tavarantoimittajista tai asiakkaista	40 %
Me emme osaa sanoa millaista tietoa vietäisiin tunkeutumisen yhteydessä	36 %
Ylempään johtoon kuuluvien henkilökohtaista tietoa	19 %
Tietoverkkoonne liittyvää tietoa kuten verkon arkkitehtuuri, asetukset tai tarkoitus	16 %
Henkilökunnan jäseniin liittyvää tietoa, kuten nimet, vastuualueet ja yksiköt	14 %

Suurin osa yrityksistä vastasi tunkeutujan etsivän tietoa immateriaalisesta omaisuudesta tai luottamuksellista tuotteisiin- tai palveluihin liittyvää tietoa. Toiseksi yleisin vaihtoehto oli se, että tunkeutujan etsii tietoa alihankkijoista, yhteistyökumppaneista, tavarantoimittajista tai asiakkaista. Kolmanneksi yleisintä oli se, että yritys ei tiedä millaista tietoa tunkeutuja etsisi.

On vaikea suojata yritystä, jos ei tiedä mitä joku haluaisi viedä siltä tai mitä toimintoja joku haluaisi haitata tai tuhota. Varauduttaessa yritykseen kohdistavaa uhkaa vastaan on ensin tunnistettava mitä halutaan suojata ja suhteuttaa toimenpiteet tunnistettuihin tai realistisiin riskeihin nähden. Jos tehdään suojaustoimenpiteitä vailla riskien arviointia, ei mikään takaa varautumisen suojaavan tehokkaasti yrityksen toiminnan kannalta tärkeitä asioita.

”Asiakkaiden tiedostot ja liiketoiminnan kannalta kriittinen info (laskutustiedot ja perusteet) säilytetään kryptatulla ulkoisella levyllä. Levyn pitäisi olla nykyteknologialla käytännössä mahdoton hakkeroida. Isompi uhka on levyn hukkaaminen ja sähköpostin (googlen verkkopalveluilta ostettu) tai kännykän hakkerointi. Levyllä säilytetään satojen ihmisten verokortteja ja työsopimuksia sekä kirjanpitoa tukevaa aineistoa”

Minkä tyyppistä tietoa olette menettäneet tietoverkkotunkeutumisten vuoksi?



Me emme osaa sanoa millaista tietoa on viety	86 %
Tietoa alihankkijoista, yhteistyökumppaneista, tavarantoimittajista tai asiakkaista	6 %
Henkilökunnan jäseniin liittyvää tietoa, kuten nimet, vastuualueet ja yksiköt	5 %
Tietoverkkoonne liittyvää tietoa kuten verkon arkkitehtuuri, asetukset tai tarkoitus	4 %
Immateriaalista omaisuutta tai luottamuksellista tietoa tuotteistamme tai palveluistamme	3 %
Ylempään johtoon kuuluvien henkilökohtaista tietoa	3 %

Vastaajista suurin osa ei osannut sanoa tai ei tiennyt mitä tietoa olisi viety. Tätä voidaan tätä pitää hyvänä herätteenä yrityksille. Jos tunkeutumista ja sitä mitä tietojärjestelmässä on tehty tunkeutujan toimesta ei kyetä huomaamaan, miten voidaan perustella suojaustoimien mielekkyyttä yrityksen johdolle. Kyse on kyvystä osoittaa kyberturvallisuuden kannattavuus ja perustelu resurssien sijoittamiselle siihen.

Havaitut menetykset jakaantuivat varsin tasaisesti eri vastausvaihtoehtojen kesken. Vastauksista käy hyvin ilmi, että tunkeutuja ei ole ensivaiheessa vain rahan perässä, vaikka julkisuudessa olevien tapausten nojalla voisi luulla niin. Tunkeutuja voi kerätä tietoa seuraavaa liikettään varten. Se voi olla tunkeutuminen toiseen organisaatioon tai tiedon kerääminen mahdollista kiristysyritystä varten. Yritys on osa digitaalista yhteiskuntaa ja jokaisella yrityksellä on oma digitaalinen vastuu asianmukaisesta varautumisesta uhkien varalle.

”Palvelimellemme onnistuttiin hyökkäämään automaattipäivityksessä olleen viiveen seurauksena. - kukaan ei varsinaisesti tehnyt mitään väärin ja vahinkoa ei lopulta päässyt syntymään, kiitos valppaan henkilökunnan ja hyvien varmuuskopioiden”

”Selvisimme Ramsonvare hyökkäyksestä "kuivin jaloin". Mitään tietoa ei lopulta menetetty, vain toimiston työt olivat osin seis pari päivää”

”Sisäverkkoomme on viimeisen kymmenen vuoden aikana päässyt kiristyshaittaohjelma, joka onnistuneesti saastutti kaksi työasemaa ja kolme levyjaollista palvelinta; dataa ei menetetty tehokkaan varmistusratkaisun ansiosta”

”Asiakasrekisterimme on päästy”

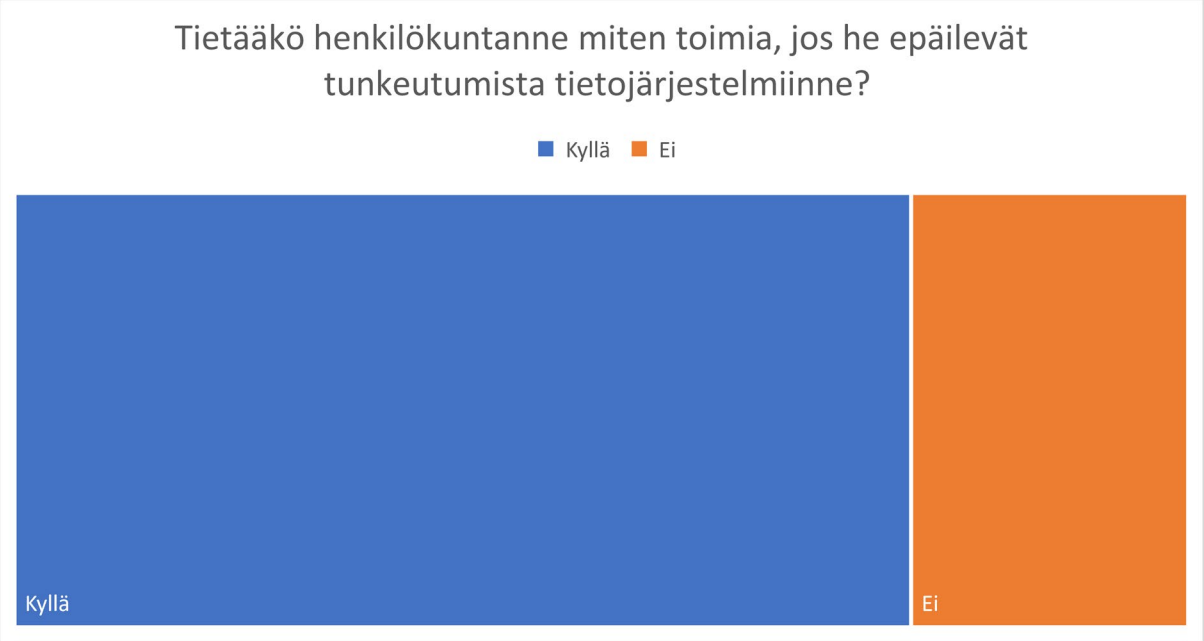
Miten organisaationne on järjestänyt tietoturvallisuusvastuut johtotasolla?

Meillä on kokoaikainen nimetty tietoturvallisuusjohtaja tai -päällikkö	12,2 %
Meillä on kokoaikainen IT-johtaja tai -päällikkö, joka vastaa tietoturvasta varsinaisen tehtävän ohella	9,4 %
Meillä on kokoaikainen johtaja tai päällikkö, joka vastaa tietoturvasta riskienhallinen tai yritysturvallisuuden osana	7,8 %
Meillä ei ole nimettyä tietoturvallisuusjohtajaa tai –päällikköä, vaan tietoturva on yleisesti IT-osaston vastuulla	4,7 %
Meillä ulkopuolinen palveluntarjoaja, joka tarjoaa tietoturvallisuusjohtajan tai -päällikön	11,8 %
Tietoturva on vastuutettu it-tuelle	12,2 %
Tietoturva on vastuutettu oman toimen ohella päällikkötason henkilölle tai toimitusjohtajalle	23,9 %
Meillä ei ole vastuutettu tietoturvallisuusasioita	18,0 %

Vastuiden selkeä jakaminen on myös kyberturvallisuuden johtamiseen kiinteästi liittyvä johdon tehtävä. Ilman selkeää vastuuttamista organisaation kyberturvallisuus ei ole kestävällä pohjalla. Kun kyberturvallisuuteen liittyvät tehtävät ovat vastuutettu, myös siihen panostetut resurssit ovat helpommin raportoitavissa johdon päätöksenteon tueksi. Selkeä, ja koko organisaation tiedossa oleva, vastuuttaminen on ensiarvoisen tärkeää myös poikkeamin hallinnoinnissa.

Positiivisena havaintona voidaan nostaa, että organisaatioiden osuus, joilla tietoturvaa ei ole vastuutettu kenellekään on vuodesta 2019 pienentynyt neljäsosasta (26 %) alle viidennekseen (18 %). Muutos on vielä suurempi, kun verrataan vuoden 2015 kyselyn tulokseen, jolloin kaikista vastanneista 35 % ilmoitti, että heillä ei ole vastuutettu tietoturvallisuusasioita.

Tietääkö henkilökunta, miten toimia, jos he epäilevät tunkeutumista tietojärjestelmiinne?



Kyllä	76 %
Ei	24 %

Organisaation jokaisen jäsenen kyky toimia oikein tietoturvapoikkeamassa tai sellaista epäiltäessä saattaa erottaa pienen vahingon isosta katastrofista. Vaikka *kyllä* vastausten osuus on jatkanut kasvuaan verrattuna edelliseen kyselyyn (2019 60 %) niin silti joka neljännen vastaajan mielestä henkilökunta ei tiedä miten toimia. Tätä voidaan pitää yhtenä tärkeimmistä kehityskohteista ja siihen voidaan kohtuullisen helposti vaikuttaa henkilökunnan kouluttamisella ja ohjeistuksella.

”Henkilöstö tunnistaa kalasteluyritykset todella hyvin. Ne ovat isoin uhka meille”

”Henkilökunta tunnistaa kalasteluyritykset ja osaa olla huolellinen netistä ladattavien ohjelmien suhteen”

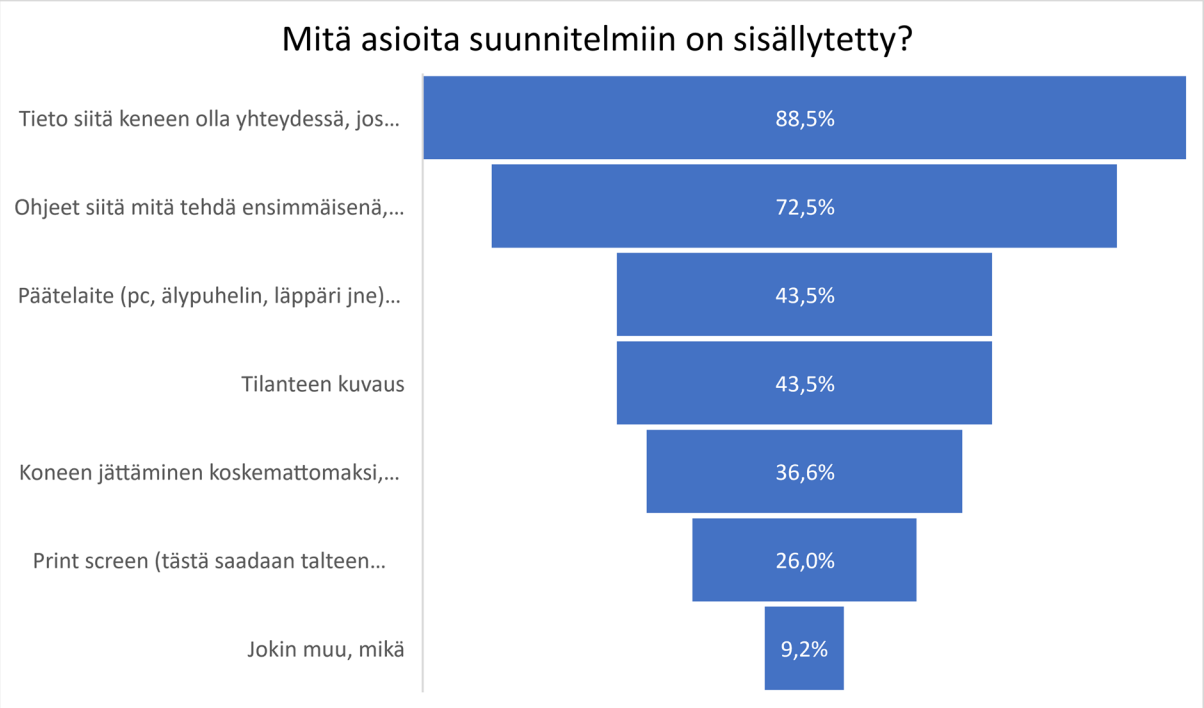
”Mahdollinen hyökkäys/tunkeutuminen on havaittu välittömästi ja tarvittaviin toimenpiteisiin on ryhdytty konsernin ohjeiden mukaan”

Onko teillä käytössä käytännössä toimivia suunnitelmia tunkeutumisten varalle?

Kyllä	52 %
Ei	48 %

Kyllä vastausten osuus (52 %) on noussut huomattavasti vuoden 2019 kyselystä (35 %) mutta silti *ei* vastausten osuus on lähes puolet. Vähäistä suuremmasta tietoturvapoikkeamasta selviäminen vaatii etukäteen laaditun suunnitelman, tai ainakin sen avulla vahinkoja saadaan todennäköisesti rajattua huomattavasti. Organisaation toiminnan luonteesta ja kyvykkyyksistä riippuen suunnitelma voi olla kohtuullisen kevyt tai hyvinkin kattava ja yksityiskohtainen. Suunnitelman laatiminen voisi olla yksi ensimmäisistä konkreettisista toimenpiteistä, kun organisaatio lähtee kohentamaan kybervalmiuksiaan.

Mitä asioita suunnitelmiin on sisällytetty?



Tieto siitä keneen olla yhteydessä, jos epäilee tunkeutumista	89 %
Ohjeet siitä mitä tehdä ensimmäisenä, jos epäilee tunkeutumista	73 %
Päätelaite (pc, älypuhelin, läppäri jne) irti verkosta (otetaan yhteyskaapeli irti tai katkaistaan langaton yhteys)	44 %
Tilanteen kuvaus	44 %
Koneen jättäminen koskemattomaksi, jotta sitä voidaan tutkia	37 %
Print screen (tästä saadaan talteen näytön näkymä myöhempää selvittelyä varten)	26 %
Jokin muu, mikä	9 %

Tämä oli jatkokysymys niille vastaajille, jotka vastasivat edelliseen kysymykseen *kyllä* (Onko teillä käytössä käytännössä toimiva suunnitelma tunkeutumisen varalle?).

Vastaukset olivat lähes identtiset vuoden 2019 kyselyn vastauksiin nähden. Tilanne tämän suhteen vaikuttaa hyvältä. Edelliseen *ei* vastanneille tämä tulos voisi toimia hyvänä kannustimena sen suhteen, että varautumissuunnitelman ei tarvitse aina ja varsinkaan heti olla kaiken kattava, vaan sen suhteen voi lähetä liikkeelle muutamasta perusasiasta ja laajentaa vähitellen.

”Suunnitelmassa korostetaan, ettei tietoturvapoikkeaman havainneen käyttäjän ole syytä hätääntyä tai panikoida tai pelätä joutuvansa syytetyn penkille. Jotta tietoturvapoikkeamista uskalletaan kertoa avoimesti, käyttäjiä ei saa moittia tai kurmoottaa”

”Päätelaitteen verkkoliikenteen sulkeminen ja koneen käyttäjätilin lukitseminen”

”Nopea toiminta ja välitön yhteys it-tukeen/talon omaan tietoturvahenkilöön”

”Security Incident prosessi ja sen eri variaatiot kriittisyyden mukaisesti”

”Pysyminen rauhallisena”

Oletteko koskaan harjoitelleet suunnitelmienne toimivuutta jollakin seuraavista tavoista?

Neuvotteluhuoneharjoitus (niin sanottu karttaharjoitus vailla käytännön toimia)	21,4 %
Käytännön harjoitus ulkopuolista tunkeutujaa vastaan	21,4 %
Emme ole harjoitelleet	61,8 %
Jokin muu, mikä	10,7 %

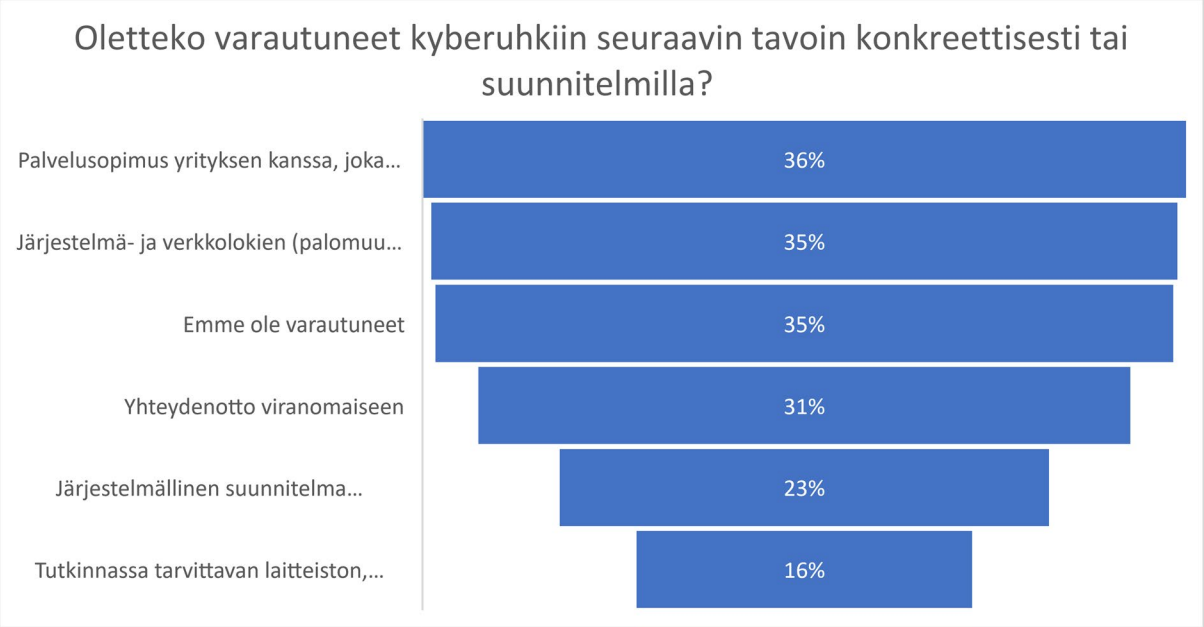
Niiden vastaajien osuus, jotka vastasivat *Emme ole harjoitelleen* on vähentynyt vuoden 2019 kyselyyn verrattuna huomattavasti (~90 % -> ~60 %). Viidennes vastaajista (21,4 %) on harjoitellut toimintaa osana oikean tunkeutujan torjuntaa.

Ohjeiden ja suunnitelmien toimivuutta on ehdottoman tärkeää testata ja harjoitella säännöllisesti. Organisaation koosta ja tarpeista riippuen harjoitteluun voi riittää jo vuosittainen muutaman tunnin neuvotteluhuoneharjoitus, jossa käydään läpi muun muassa ohjeistuksen löytyminen, niiden ajantasaisuus ja mahdolliset muutokset vastuisiin ja tehtäviin. Laajemmissa ja enemmän panostusta vaativissa harjoituksissa voidaan harjoitella esim. tietojen palauttamista varmuuskopioista tai varajärjestelmien käyttöönottoa ja toimivuutta.

”Emme vielä, mutta harjoituksen suunnittelu on seuraavana tietoturvatiimin pöydällä”

”Suunnitelmissa yhteistoimintaharjoitus”

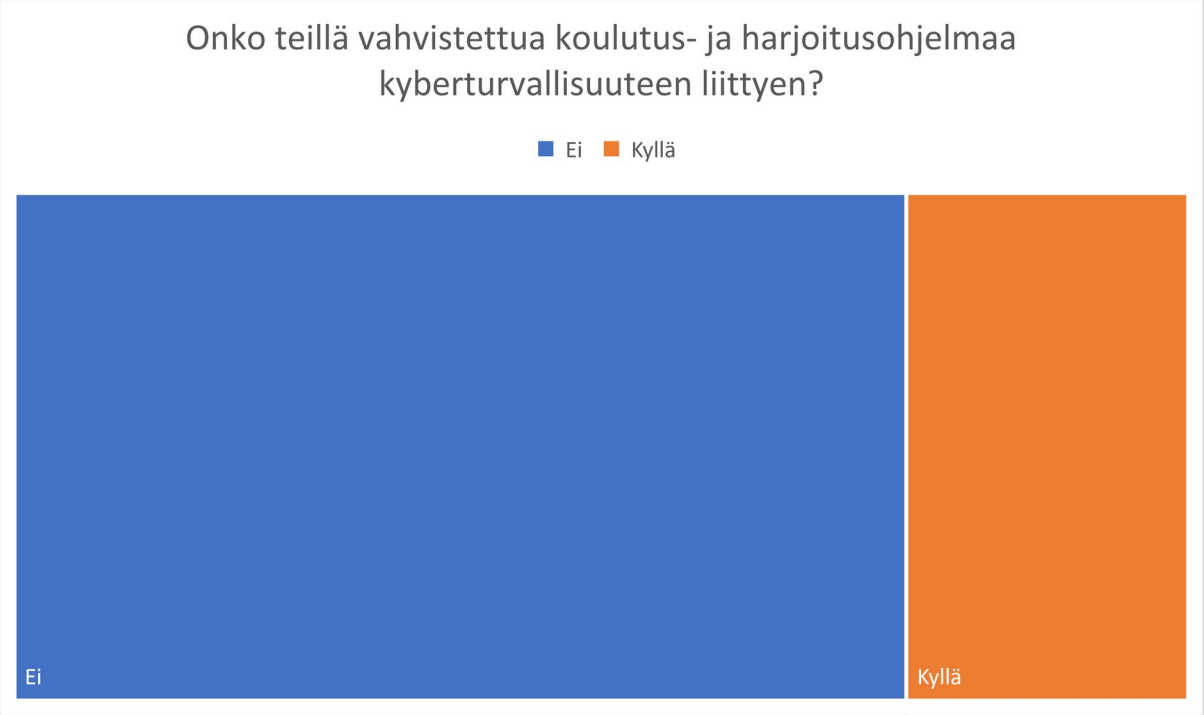
Oletteko varautuneet kyberuhkiin seuraavin tavoin konkreettisesti tai suunnitelmilla?



Järjestelmällinen suunnitelma tilannekuvan muodostamiseksi (datan kopiointi) tutkintaa ja puhdistustoimenpiteitä sekä loppuraportointia varten	22,9 %
Järjestelmä- ja verkkolokien (palomuuri, http, ad, dhcp, vpn) kerääminen kaikista järjestelmistä mahdollisimman pitkältä ajalta	34,9 %
Tutkinnassa tarvittavan laitteiston, ohjelmiston ja tutkintakyvyn ennakkoon hankinta	15,7 %
Yhteydenotto viranomaiseen	30,5 %
Palvelusopimus yrityksen kanssa, joka tarjoaa järjestelmiin tunkeutumisen ja haittaohjelmien tutkintaa	35,7 %
Emme ole varautuneet	34,5 %

Emme ole varautuneet vastaajien osuus on laskenut joitakin prosenttiyksiköitä vuoden 2019 kyselyyn verrattuna, jota voidaan pitää erittäin hyvänä kehityssuuntana. Varautumiskeinojen kesken jakautuminen on tasaista, isoin nousu on tapahtunut palvelusopimusten kautta tapahtuvan varautumisen noususssa. Lokien kerääminen hallintakeinona oli myös noussut huomattavasti vuoden 2019 tasosta (21 % -> 39 %). Riittävän pitkältä ajalta kerätyt lokit edesauttavat merkittävästi kyberrikosten selvittelyssä.

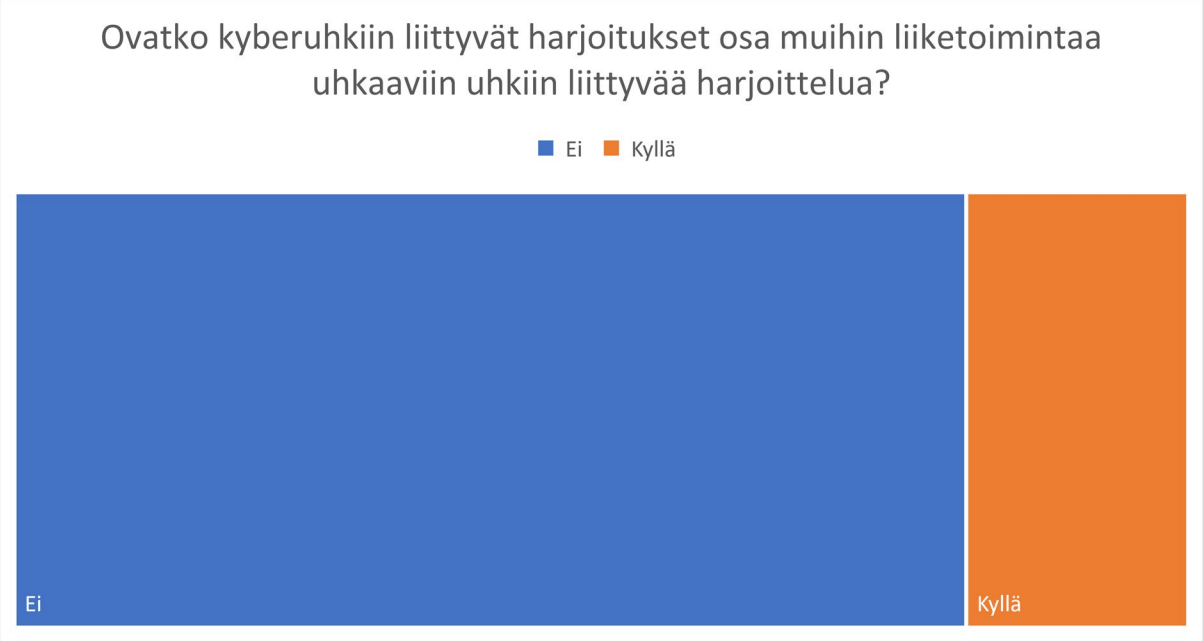
Onko teillä vahvistettua koulutus- ja harjoitusohjelmaa kyberturvallisuuteen liittyen?



Kyllä	24,0 %
Ei	76,0 %

Ei vastausten määrä on edelleen korkealla tasolla, mutta laskenut kymmenisen prosenttiyksikköä vuoden 2019 kyselystä (86 %->76 %). Kyberturvallisuuteen liittyvä koulutus ja harjoittelu tulee olla osana organisaation normaalia koulutustarjontaa samoin siihen liittyvä harjoittelu. Sen olemassaolo tai puuttuminen voi heijastaa johdon sitoutuneisuutta kyberturvallisuuden kehittämiseen. Vastaukset ovat linjassa ohjeistukseen ja harjoitteluun nähden.

Ovatko kyberuhkiin liittyvät harjoitukset osa muihin liiketoimintaa uhkaaviin uhkiin liittyvää harjoittelua?



Ei	81 %
Kyllä	19 %

Kyllä vastausten osuus on linjassa edellisten vastausten kanssa. Tässä varmasti heijastunee myös se, että harjoittelu ylipäätään näyttäisi keskittyvän suurempiin organisaatioihin ja näissä kyberturvallisuuteen liittyvät harjoituksen järjestetään osana muita varautumisharjoituksia.

Oletteko viimeisen neljän vuoden aikana kohdistaneet kyberturvallisuuteenne jotain seuraavista toimenpiteistä?

Kyberturvallisuuteen liittyvien ohjeiden laatiminen henkilökunnalle	53,6 %
Kyberturvallisuusammattilaisen palkkaaminen	15,0 %
Kyberturvallisuuspalvelujen hankkiminen alan palveluntarjoajalta	41,1 %
Kyberturvallisuusohjelmistojen ja -työkalujen hankkiminen	50,7 %
Kyberturvallisuuden budjetoiminen vuositasolla	15,9 %
Kyberturvallisuudesta vastaavan henkilön nimeäminen	32,4 %
Kyberturvallisuuspolitiikan laatiminen	25,1 %
Jokin muu, mikä	15,5 %

Kolmen kärki nousi vastauksista selkeästi esille, ohjeiden laatiminen (53,6 %), ohjelmistojen- ja työkalujen hankkiminen (50,7 %) sekä palvelujen hankkiminen palveluntarjoajilta (41,1 %). Näistä tuloksista ei kuitenkaan käy ilmi onko näillä toimenpiteillä vahvistettu olemassa olevaa kyvykkyyttä vai pyritty saavuttamaan hyväksyttävä taso.

”Kyberturvatiimin perustaminen. Tiimi vastaa ohjeista, henkilöstön jatkuvasta kouluttamisesta ja tiedottamisesta ja siitä, että kyberuhista pysytään ajan tasalla”

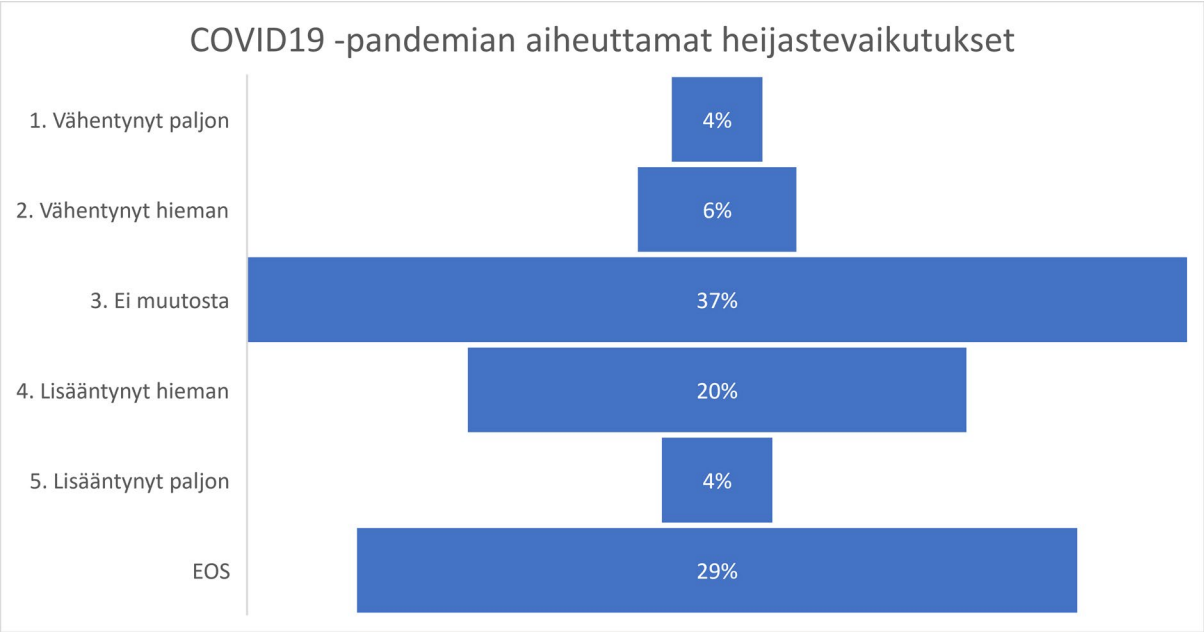
”Henkilökunnan koulutus ulkopuolisen asiantuntijan avulla”

”Ei mitään. Olen yksinyrittäjä ja pyrin kaikessa toiminnassani varovaisuuteen, myös kyberuhkiin liittyen, mutta mitään erillisiä toimenpiteitä en ole tehnyt toistaiseksi”

UHKAHORISONTIN MUUTOS

Kyselyyn otettiin uutena osuutena Uhkahorisointin muutos, jolla pyrittiin selvittämään viimeisen kahden vuoden aikana ilmenneiden kokonaan uusien uhkien tai vanhempien uudelleen pinnalle nousseiden uhkien vaikutusta.

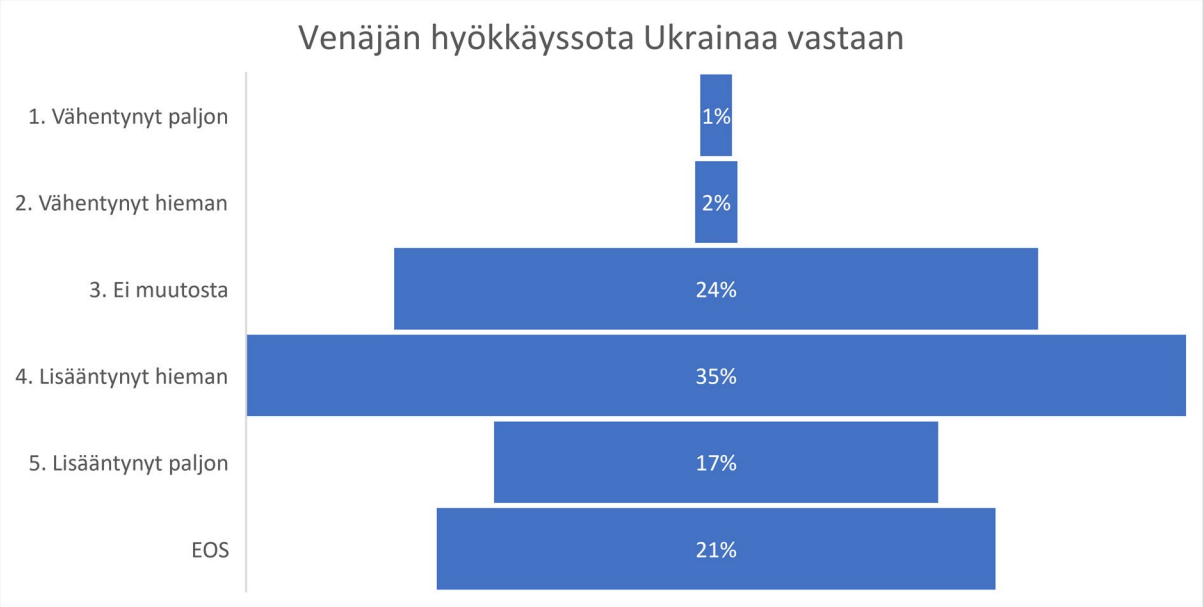
COVID19 -pandemian aiheuttamat heijastevaikutukset



1. Vähentynyt paljon	3,6 %
2. Vähentynyt hieman	6,3 %
3. Ei muutosta	37,3 %
4. Lisääntynyt hieman	19,8 %
5. Lisääntynyt paljon	4,4 %
EOS	28,6 %

COVID19 pandemia on varmasti heijastunut jokaiseen suomalaiseen yritykseen ja organisaatioon jollakin tavalla. Vastaajista kuitenkin valtaosa (37 %) katso, ettei vaikutus ole juurikaan lisääntynyt tai ei osannut arvioida vaikutuksen muutosta. Viidennes vastaajista (20 %) kuitenkin katsoi, että pandemian heijastevaikutukset ovat lisääntyneet jonkin verran.

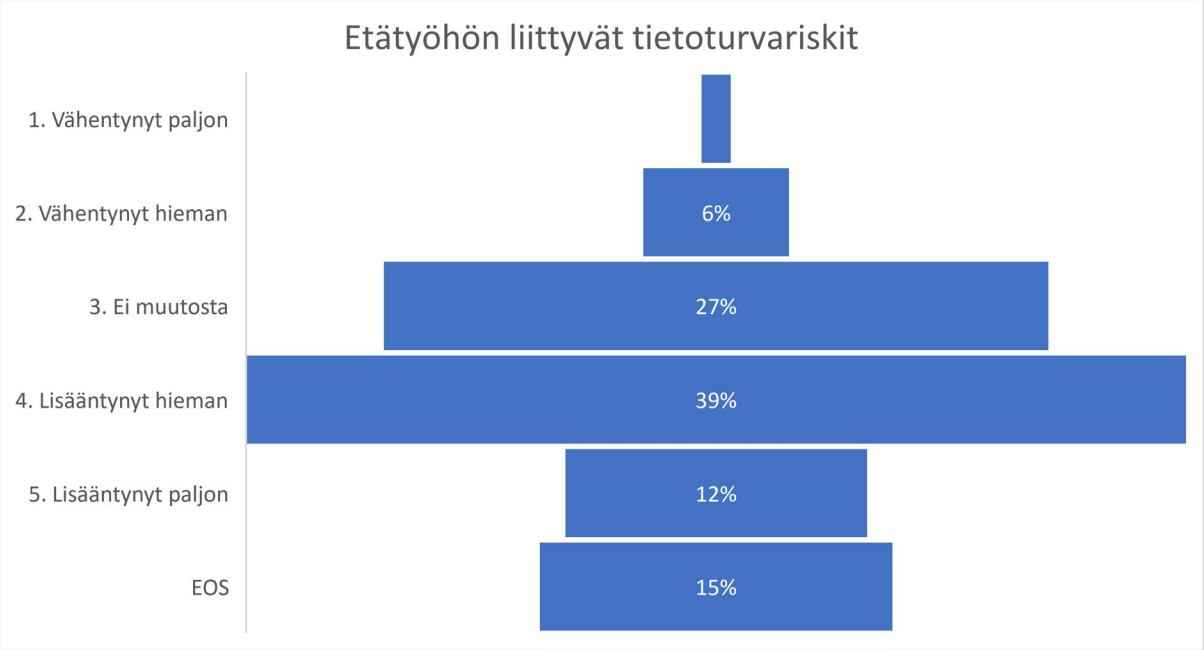
Venäjän hyökkäyssota Ukrainaa vastaan



1. Vähentynyt paljon	1,2 %
2. Vähentynyt hieman	1,6 %
3. Ei muutosta	24,2 %
4. Lisääntynyt hieman	35,3 %
5. Lisääntynyt paljon	16,7 %
EOS	21,0 %

Venäjän helmikuussa 2022 aloittama täysimittainen hyökkäyssota Ukrainaa vastaan on aiheuttanut selvästi huolta vastaajien keskuudessa. Yli puolet (52 %) katsoi, että Venäjän hyökkäyssota Ukrainaa vastaan on vaikuttanut uhkahorisonttiin joko jonkun verran tai paljon. Vain muutama prosentti vastaajista katsoi, että tällä ei ole ollut vaikutusta.

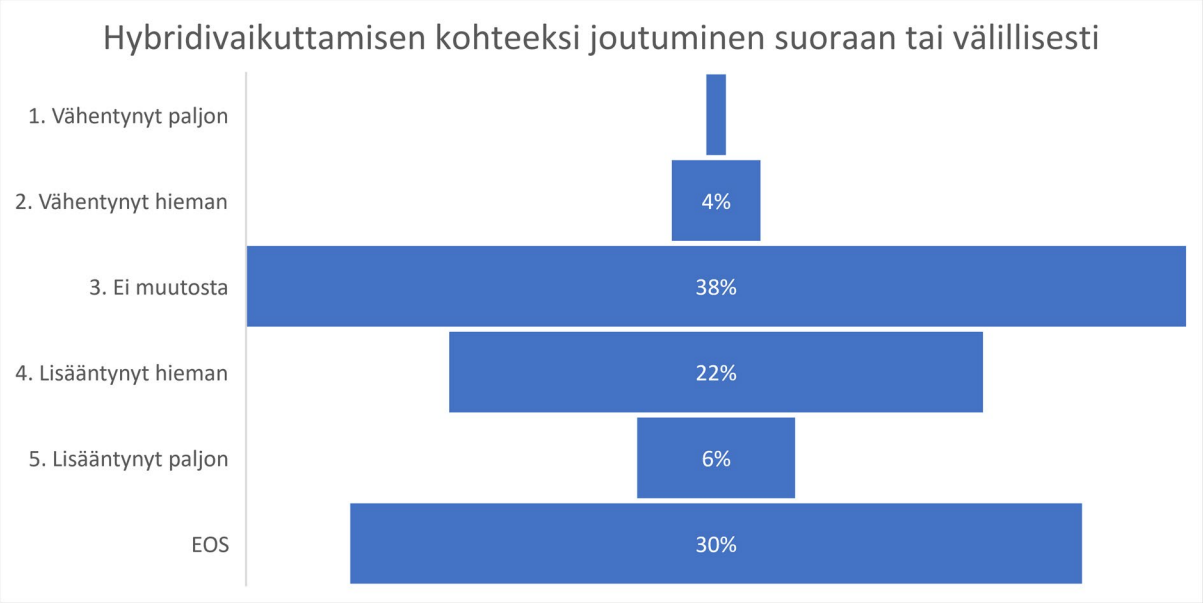
Etätyöhön liittyvät tietoturvariskit



1. Vähentynyt paljon	1,2 %
2. Vähentynyt hieman	6,0 %
3. Ei muutosta	27,3 %
4. Lisääntynyt hieman	38,6 %
5. Lisääntynyt paljon	12,4 %
EOS	14,5 %

Etätyöhön liittyvien tietoturvauhkien lisääntyminen huolestutti vastaajia eniten uhka-horisonttiosuudessa. Vastaajista yli puolet katsoi, että etätyöhän liittyvät riskit ovat kasvaneet jonkin verran tai paljon. Laajamittaiseen etätyöskentelyyn siirryttiin COVID19-pandemian pakottamana hyvin nopealla aikataululla eikä sen tietoturvallista toteuttamista pystytty pääsääntöisesti selvittämään ja toteuttamaan kunnolla. Etätyön muututtua uudeksi normaaliksi organisaatiot ovat ilmeisesti heränneet laajamittaiseen etätyöhön liittyviin tietoturvakysymyksiin.

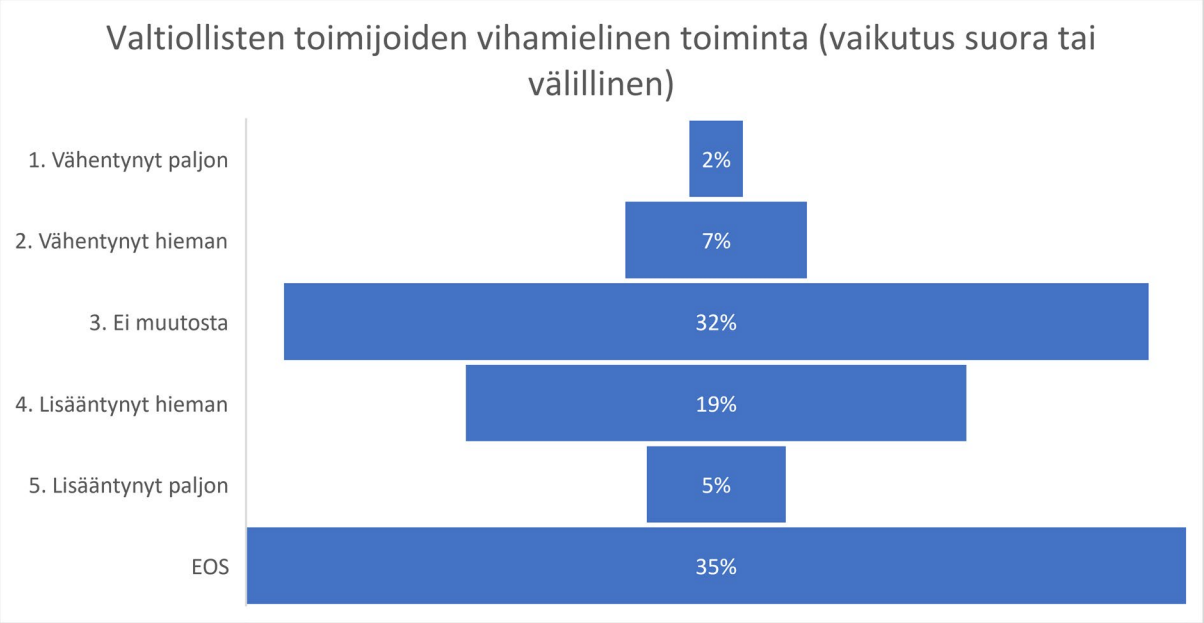
Hybridivaikuttamisen kohteeksi joutuminen suoraan tai välillisesti



1. Vähentynyt paljon	0,8 %
2. Vähentynyt hieman	3,6 %
3. Ei muutosta	38,0 %
4. Lisääntynyt hieman	21,6 %
5. Lisääntynyt paljon	6,4 %
EOS	29,6 %

Hybridivaikuttamisen kohteeksi joutuminen tai sen todellisen uhan kohteeksi joutuminen on todennäköisesti rajoittunut pieneen määrään yrityksiä ja organisaatioita. Vaikka kohdeorganisaatio ei kuuluisikaan varsinaisen hybridivaikuttamisen suoraan kohderyhmään, on yleisen resilienssin kannalta keskeistä, että tämäkin uhka tunnistetaan.

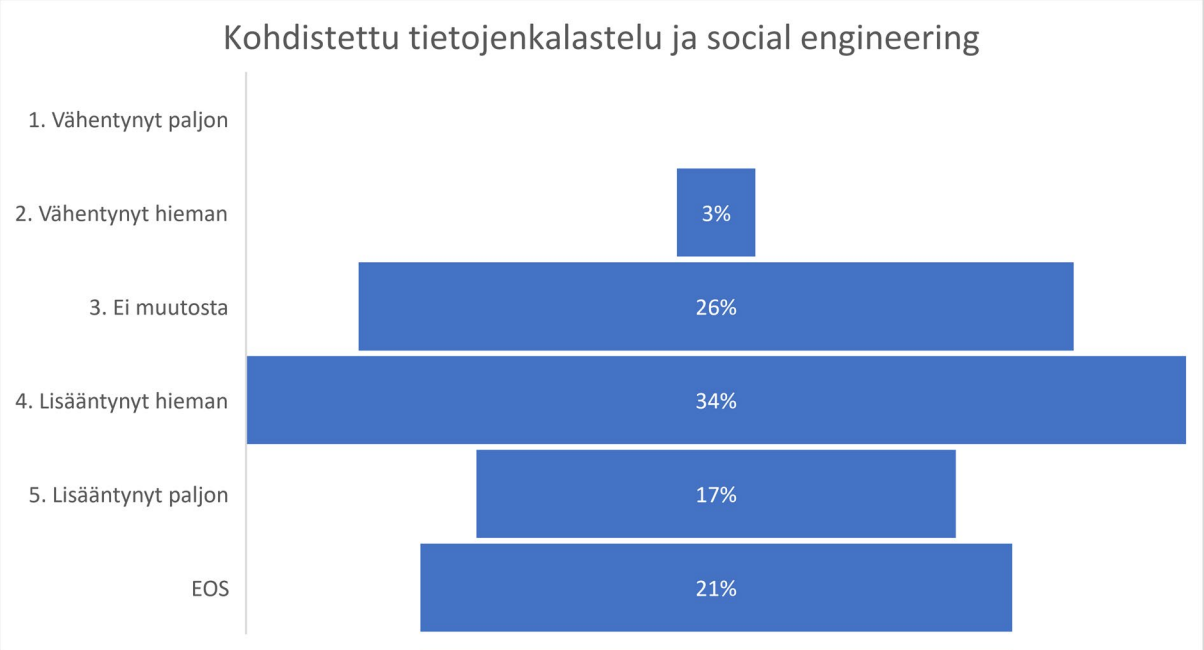
Valtiollisten toimijoiden vihamielinen toiminta (vaikutus suora tai välillinen)



1. Vähentynyt paljon	2,0 %
2. Vähentynyt hieman	6,8 %
3. Ei muutosta	32,3 %
4. Lisääntynyt hieman	18,7 %
5. Lisääntynyt paljon	5,2 %
EOS	35,1 %

Tätä kysymystä voidaan pitää hyvin samansuuntaisena kuin hybiridivaikuttamista koskeva kysymys. Vastaukset ovatkin linjassa hybridivaikuttamista koskevan kysymyksen kanssa. Suoraan valtiollisen toimijan vihamielisten toimenpiteiden kohteeksi joutuminen on varmasti myös rajatun yritys ja organisaationryhmän riski, mutta välillisesti sen vaikuttavuuden piiriin saattaa kuulua lähes mikä tahansa yritys tai organisaatio. Näiden heijastevaikutusten takia tämäkin uhka pitäisi pitää organisaation uhkarekisterissä ainakin jossakin määrin.

Kohdistettu tietojenkalastelu ja social engineering

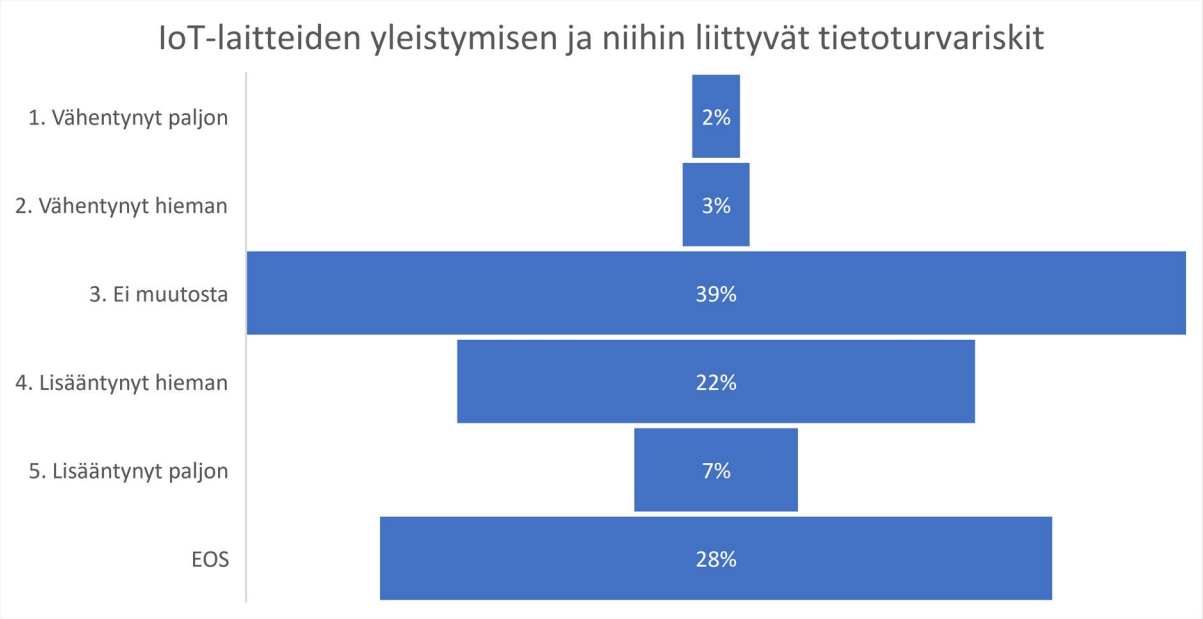


1. Vähentynyt paljon	0,0 %
2. Vähentynyt hieman	2,8 %
3. Ei muutosta	25,5 %
4. Lisääntynyt hieman	33,5 %
5. Lisääntynyt paljon	17,1 %
EOS	21,1 %

Vastaukset kertovat selvästi, että yli puolet vastaajista on selvästi huolissaan kohdistetun tietojenkalastelun ja social engineering hyökkäysten vaikutuksesta uhkahorisonttiin nimenomaan negatiivisessa mielessä. Vain muutama prosentti vastaajista katso, että nämä uhat ovat vähentyneet viimeisen parin vuoden aikana.

Viidennes vastaajista ei osannut arvioida onko tilanne näiden kohdalla muuttunut viimeisen vuosien aikana. Kyberuhkina nämä ovat kuitenkin osallisena valtaosaan poikkeamista ja erittäin käytetty ”taktiikka & tekniikka” -yhdistelmä verkossa toimivien vihamielisten toimijoiden keskuudessa.

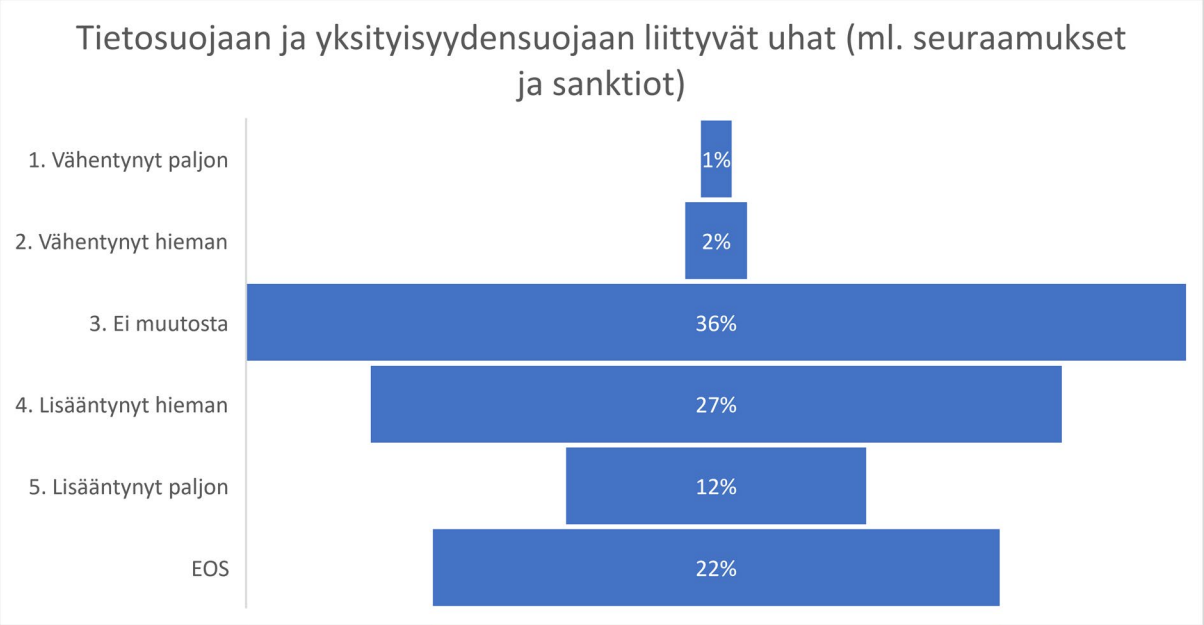
IoT-laitteiden yleistymisen ja niihin liittyvät tietoturvariskit



1. Vähentynyt paljon	2,0 %
2. Vähentynyt hieman	2,8 %
3. Ei muutosta	39,0 %
4. Lisääntynyt hieman	21,5 %
5. Lisääntynyt paljon	6,8 %
EOS	27,9 %

Neljännes vastaajista katsoi, että IoT-laitteisiin liittyvät uhat ovat nostaneet merkitystään kyberin yleisessä uhkahorisontissa. Valtaosa katsoi, että IoT-laitteisiin liittyvät uhat eivät ole muuttuneet tai eivät osanneet arvioida onko muutosta tapahtunut vai ei. Verkkoon liitettävien älykkäiden laitteiden määrä kasvaa jatkuvasti ja laitteisiin liittyvät turvallisuuskysymykset ovat vielä pitkälti vastaamatta ja saattavat aiheuttaa kyberturvallisuuden kannalta uhkia yllättävissäkin paikoissa ja tilanteissa.

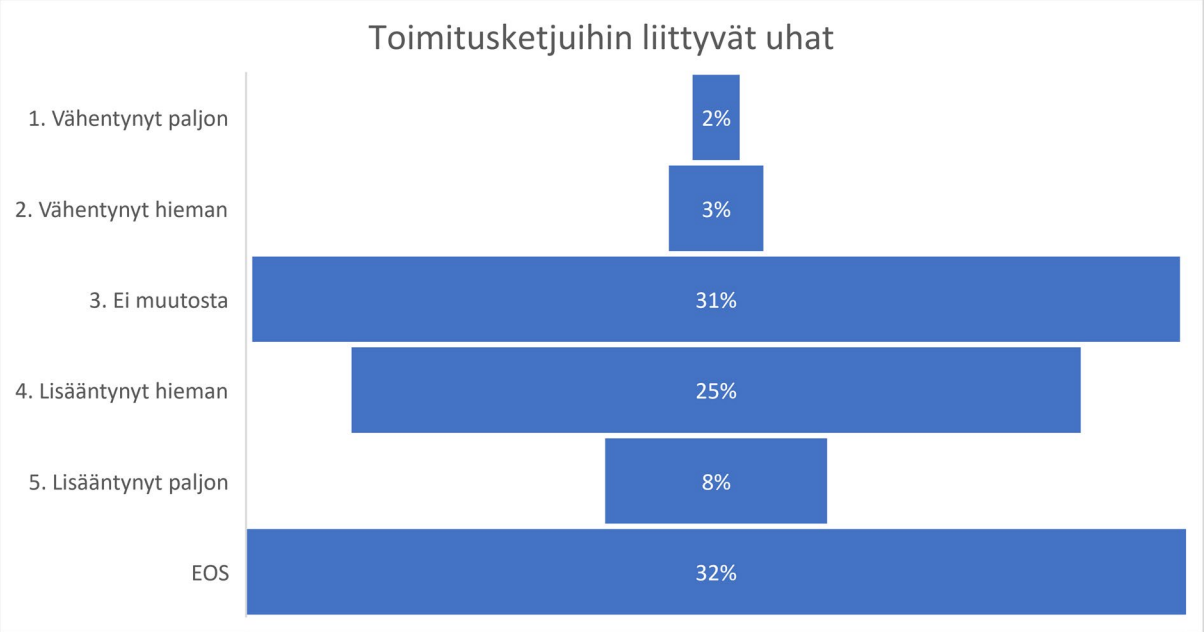
Tietosuojaan ja yksityisyydensuojaan liittyvät uhat (ml. seuraamukset ja sanktiot)



1. Vähentynyt paljon	1,2 %
2. Vähentynyt hieman	2,4 %
3. Ei muutosta	36,3 %
4. Lisääntynyt hieman	26,7 %
5. Lisääntynyt paljon	11,6 %
EOS	21,9 %

Kolmasosa (36 %) vastaajista katsoi, että tietosuojaan liittyvät uhat eivät ole oleellisesti muuttuneet viimeisen kahden vuoden aikana. Toisaalta lähes 40 % katsoi, että uhat ovat kasvaneet. Vain muutaman vastaajan mielestä nämä uhat ovat vähentyneet viimeisen kahden vuoden aikana. Mielenkiintoisena lisäpohdintana voisi olla onko uhan vähentymisen kokevien vastaajien kohdalla tehty selkeitä toimenpiteitä millä riskiä on saatu selvästi vähennettyä.

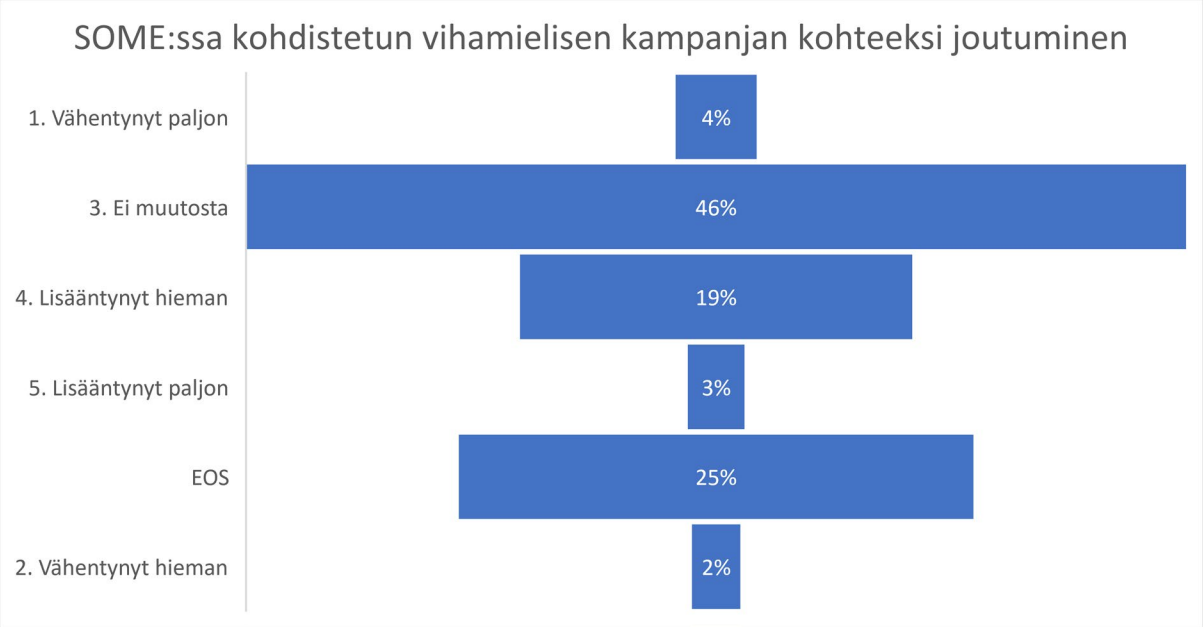
Toimitusketjuihin liittyvät uhat



1. Vähentynyt paljon	1,6 %
2. Vähentynyt hieman	3,2 %
3. Ei muutosta	31,3 %
4. Lisääntynyt hieman	24,6 %
5. Lisääntynyt paljon	7,5 %
EOS	31,7 %

Toimitusketjuihin liittyvistä uhista on puhuttu viimeisten vuosien aikana paljonkin ja uhkien toteutumisesta on myös merkittäviä esimerkkejä (esim. Solarwinds Orion 2020). Toimitusketjuihin liittyvät kyberuhat ovat yksi merkittävimmistä moderneista uhista kohdistettujen tietojenkalastelun ja social engineering hyökkäysten ohella. Kolmannes vastaajista näkikin tämän uhan kasvaneen jonkin verran tai huomattavasti.

SOME:ssa kohdistetun vihamielisen kampanjan kohteeksi joutuminen

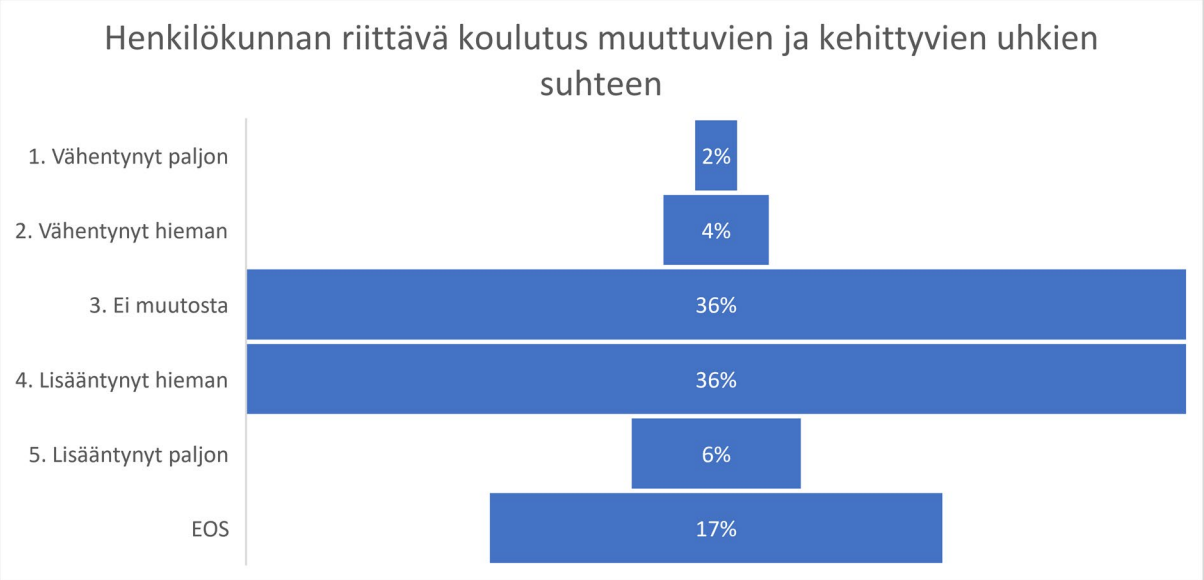


1. Vähentynyt paljon	4,0 %
2. Vähentynyt hieman	2,4 %
3. Ei muutosta	46,2 %
4. Lisääntynyt hieman	19,3 %
5. Lisääntynyt paljon	2,8 %
EOS	25,3 %

Lähes puolet vastaajista katsoi, että tämän kaltainen uhka ei ole merkittävästi muuttunut viimeisen parin vuoden aikana. Viidennes kuitenkin näki, että tähän liittyvä uhka olisi kohonnut jonkin verran viime aikoina.

Sosiaalisen median käyttö erilaisiin vihakampanjoihin on yleistynyt viimeisen vuosikymmenen aikana. Niitä on kohdistettu yrityksiin ja yksilöihin. Jotkin valtiot käyttävät aktiivisesti trollausta osana työkaluvalikoimaansa.

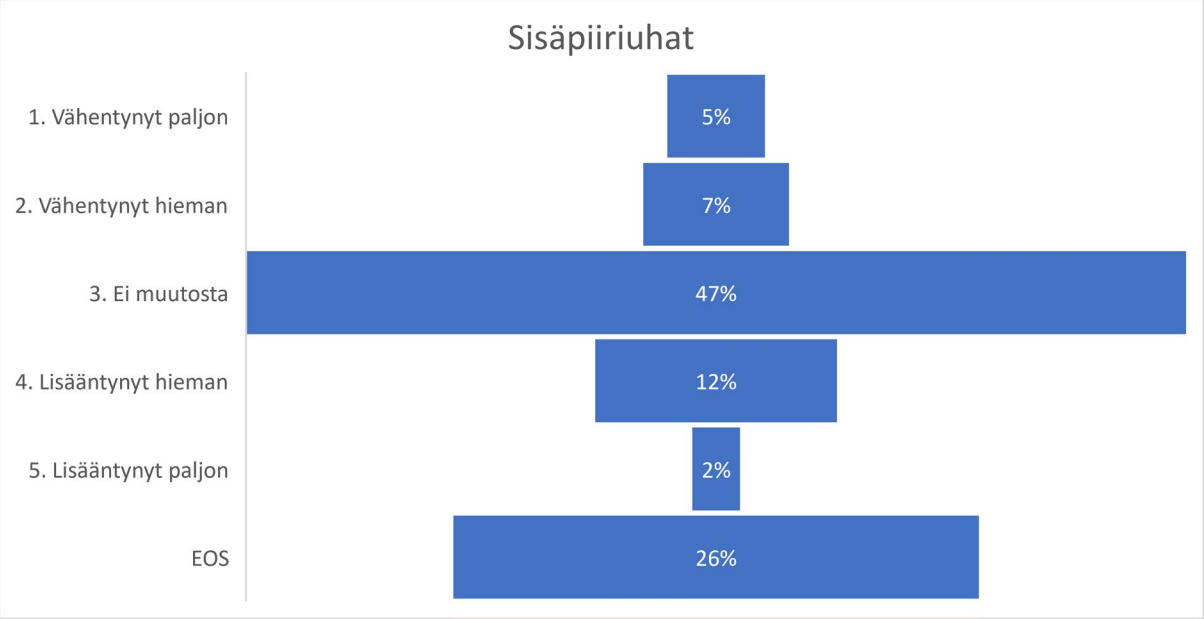
Henkilökunnan riittävä koulutus muuttuvien ja kehittyvien uhkien suhteen



1. Vähentynyt paljon	1,6 %
2. Vähentynyt hieman	4,0 %
3. Ei muutosta	35,5 %
4. Lisääntynyt hieman	35,5 %
5. Lisääntynyt paljon	6,4 %
EOS	17,1 %

Mikä vaikutus uhkahorisontin muutoksilla on henkilökunnan koulutustarpeeseen? Pitäisikö koulutusta antaa lisää määrällisesti vai laadullisesti? Vastausten jakautumisesta voisi ehkä päätellä, että monessa organisaatiossa selvästi pohditaan tätä. Uhkatietoinen ja koulutettu henkilökunta yksi parhaista aseista kyberuhkien torjumiseen.

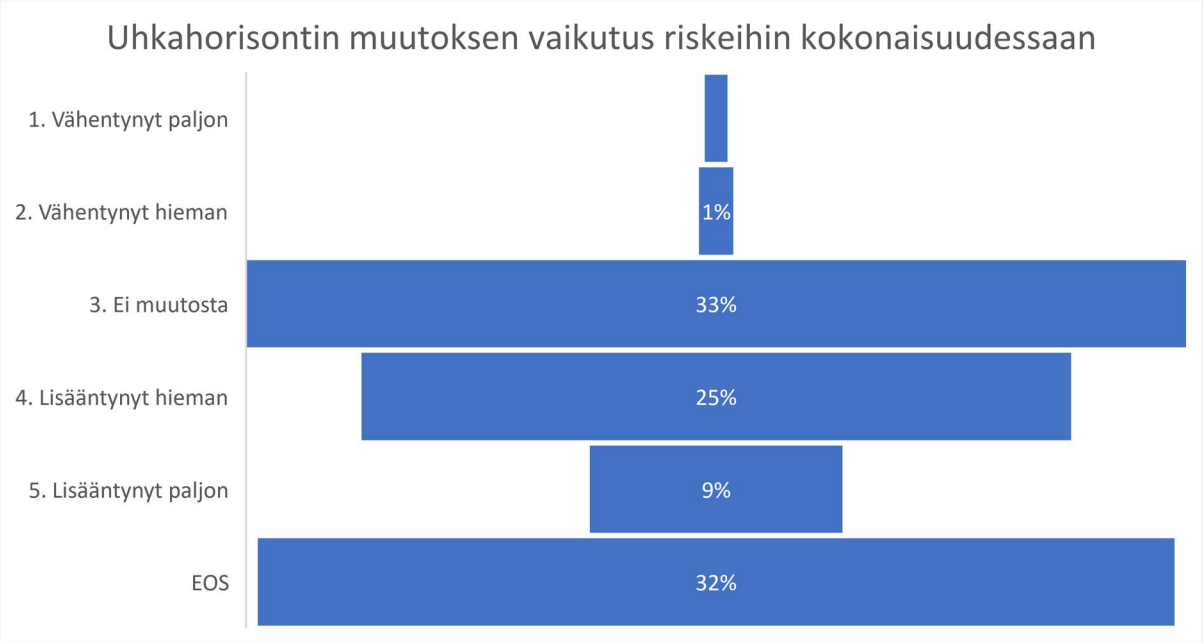
Sisäpiiriuhat



1. Vähentynyt paljon	4,9 %
2. Vähentynyt hieman	7,3 %
3. Ei muutosta	47,0 %
4. Lisääntynyt hieman	12,1 %
5. Lisääntynyt paljon	2,4 %
EOS	26,3 %

Vastaajat katsoivat, että uhkahorisontti ei ole muuttunut oleellisesti viimeisen parin vuoden aikana, ainoastaan vajaa 15 % katosi tämän uhan lisääntyneen jonkin verran tai huomattavasti. Vastaavasti lähes sama määrä vastaajista katosi, että sisäpiiriuhka olisi vähentynyt viimeisen parin vuoden aikana.

Uhkahorisontin muutoksen vaikutus riskeihin kokonaisuudessaan



1. Vähentynyt paljon	0,8 %
2. Vähentynyt hieman	1,2 %
3. Ei muutosta	32,7 %
4. Lisääntynyt hieman	24,7 %
5. Lisääntynyt paljon	8,8 %
EOS	31,9 %

Uhkahorisontin muutosta kokonaisuutena katsottuna vastaukset jakautuvat selvästi kolmeen eri osaan, joista niukasti suurin ryhmä on se, joiden mielestä uhkahorisontin muutos on kasvattanut riskejä joko jonkin verran tai merkittävästi. Tätä voidaan pitää jopa yllättävän pienenä määränä verrattuna siihen, kuinka poikkeuksellisia aikoja viimeiset vuodet on eletty.

JOHTOPÄÄTÖKSET

Tiedon puute, työntekijöiden osaamisen ylläpito ja välipitämättömyys yhä esteenä kyberturvallisuuden kehittämiselle – yhä useampi yritys voi vaarantaa yhteiskunnan resilienssiä ja viime kädessä kansallisen turvallisuuden

Helsingin seudun kauppakamari toteutti ensimmäisen Kyberuhkiin liittyvän selvityksen vuonna 2015. Seitsemässä vuodessa tiedon saatavuus ja työntekijöiden osaaminen ovat yhä kärkiesteitä kyberturvallisuuden kehittämiselle. Kyberturvallisuus on jatkuva kilpajuoksua rikollisten osaamisen kehittymisen kanssa ja siksi tiedonjakoa laajemmin yritysektorin kanssa on kehitettävä. Puolet (50 %) vastaajayrityksistä pitää työntekijöiden tietotaidon ylläpitoa suurimpana esteenä kyberturvallisuuden kehittämiselle. Kolmasosa (34 %) ei löydä riittävästi tietoa kyberuhista ja yli kolmasosa (40 %) pitää työntekijöiden piittaamattomuutta esteenä kyberturvallisuuden kehittämiselle.

Mikä yritys tahansa saattaa vaarantaa yhteiskunnan resilienssiä tai jopa kansallista turvallisuutta olemalla ketjun heikoin lenkki. Sen vuoksi jokaisella yrityksellä on digitaalisen liiketoiminnan mukanaan tuoma vastuu ja sen laiminlyöminen voi viime kädessä olla kansallisen turvallisuuden kysymys. Luottamuksellista tietoa voidaan varastaa tai digitaalisia tuhotöitä valmistella yrityksen tietoverkossa tai sen kautta. Yksikään yritys ei ole irrallinen saari, vaan jokainen yritys voi olla osa digitaalista rintamaa minä päivänä tahansa. Jokainen yritys voi vaikuttaa kokonaisuuteen ja siksi on tärkeää, että kyberuhkiin ja varautumiseen liittyvä selkokielinen tieto saavuttaa yritykset laajemmin kuin tähän mennessä.

Yritysten keskuudessa puutteita kyvyssä tunnistaa tunkeutumisia ja tiedossa siitä mitä rikollinen haluaa – tämä helpottaa vieraiden valtioiden ja muiden rikollisten kyberurkintaa

Viidesosa yrityksistä (21 %) ei tunnista niiden verkkoon tehtyjä tunkeutumisia eikä tiedä millaista tietoa tunkeutuja (36 %) haluaisi hakea heidän tietoverkostaan. Lisäksi lähes kolmasosa (28 %) yrityksistä luottaa kolmanteen tahoon operaattoriin tai palvelun-tarjoajaan ilmoitustahona. Rikollisen motiivin ja tavoitteen tiedostamisen kautta yrityksen on helpompi suojata tietoverkkoaan ja siellä olevia tietoja. Kaikilla yrityksillä ei voi olla resursseja tunnistamiseen mutta juuri se mahdollistaa vihamielisille valtioille ja rikollisille huomaamattoman tiedonkeruun tai reitin tuhotyön valmisteluun. Kriittisen infran yritysten on tärkeää tunnistaa tämä varautuessaan itseensä kohdistuviin oman toimitusketjunsa aiheuttamiin kyberuhkiin.

Kerättyä henkilöön liittyvää tietoa voidaan käyttää värväyksessä tai painostuksessa, jolla pyritään saamaan lisää tietoa tai kohteena oleva ihminen tekemään jotain haluttua. Tällainen taivuteltu ihminen ei toimiessaan organisaationsa verkossa jätä niin selvästi havaittavia jälkiä kuin ulkopuolinen hyökkääjä. Siksi tällaisen henkilön käyttäminen on joissain tilanteissa kultaakin arvokkaampi erityisesti vieraalle vallalle, joka vaikkapa haluaa valmistella tuhotyötä kriittisessä infrassa tai kerätä haluamaansa kohdetietoa samaa tarkoitusta varten.

Henkilöiden yksityisyyden, tuoton ja aineettoman omaisuuden menetykset raskaimpia seurauksia

Yritykset tunnistavat hyvin kyberhyökkäyksen raskaimpina seurauksina henkilötietojen (59 %), tuoton (42 %) ja aineettoman omaisuuden (34 %) menetykset. Samalla ne huomaamattaan tunnistavat keskeisimmät tiedot, joita yritysten tulisi suojata.

Tästä tietoisuudesta huolimatta yritykset kaipaavat lisää tietoa henkilökunnan osaamisen ylläpitämiseksi. Tietoa kaivataan myös uhista ja turvallisuusmenetelmistä. Nämä tiedot ovat kyberturvallisuuden kehittämisen perusteita, joten monet yritykset ovat helppoa hyökkäyspinta-alaa pahantahtoisille kybertoimijoille. Seitsemän vuoden aikana tilanne ei ole juurikaan muuttunut ja se on hyvin huolestuttavaa arvioitaessa Suomen kyberresilienssin kehitystä ja sen kehittämiseksi tehtyjen toimienpiteiden onnistumista yritysten tavoittamisen osalta.

Suurimpana kyberuhkana pidetään phishing- ja haittaohjelmahyökkäyksiä, mutta sisäistä uhka ei ole unohdettu

Enemmistö (77 %) vastaajista nimesi phishing- ja haittaohjelmahyökkäykset suurimmaksi kyberuhaksi. Vihamieliset valtiot ja muut rikolliset käyttävät niitä laajasti. Lähes kolmasosa (29 %) piti yhtiön sisäistä uhkaa merkittävänä kyberuhkana. Oma työntekijä voi toimia pitkäänkin tietoverkossa siten, ettei sitä erota normaalista työhön kuuluvasta verkkokäyttäytymisestä ja työntekijän on esimerkiksi helppo kytkeä annettu muistitikku tietokoneeseen yrityksen toimitiloissa palomuurin sisäpuolella. Noin kolmasosa vastaajista (32 %) nosti esille palvelunestohyökkäykset, joita on tänä vuonna nähty Suomessa normaalia enemmän.

Kyberturvallisuuttakin pitää johtaa – johdon sitoutumisen pitää olla sataprosenttista ja vastuiden selviä.

Kysyttäessä mitkä kolme suurinta estettä tehokkaan kyberturvallisuuden toteutumisessa ovat, kärkeen nousivat selvästi ihmisiin liittyvät asiat; riittävä tietotaito, sen ylläpito ja asenteet (piittaamattomuus). Rahoitus oli vasta kuudennella sijalla. Voisiko näitä tuloksia pitää johtajuuteen liittyvinä haasteina?

Onko organisaation johdolla tarpeeksi työkaluja osoittaa johtajuuttaan myös kyberturvallisuuteen liittyvissä asioissa vai mennäänkö siinä helposti vain asioiden johtamiseen, myönnetään rahoitusta ja resursseja teknisten kyvykkyyksien kasvattamiseen ja parantamiseen, mutta saatetaan unohtaa organisaation yksi tärkeimmistä resursseista kyberturvallisuuden turvaamisen saralla – ihmiset. Ihmiset tulee saada innostumaan, ei pakottaa, osallistumisesta yrityksen turvallisuuskulttuurin kehittämiseen.

Johtajuus tulee sataprosenttisesta sitoutumisesta kyberturvallisuuteen. Tähän liittyy oleellisesti myös se, että johto on kyennyt saamaan kaikki vastuut ja roolit selviksi ja luonut toimintaedellytykset (myös taloudelliset). Johdon tulee myös varmistaa avoin ja jatkuva dialogi kyberturvallisuudesta vastaavien tahojen kanssa esimerkiksi säännöllisten tilannekatsauksien muodossa johtoryhmälle.

Uhkahorisontti – yritykset huolissaan vihamielisistä valtioista

Huoli vihamielisten valtioiden toiminnan riskin lisääntymisestä näkyy useista uhkahorisontin vastauksista. Yli puolet (52 %) vastaajista kokee Venäjän hyökkäyssodan sodan lisänneen uhkatilannetta. Sodalla voi olla tähänastista tuntuvampia vaikutuksia Suomeen talvella 2023, jolloin erilainen haitanteko voi saada aikaan suuremman vaikutuksen kansalaisten psykologiseen resilienssiin heikentäen luottamusta yhteiskuntaan ja maan johtoa kohtaan. Yli neljäsosa (28 %) kokee hybridivaikuttamisen kohteeksi joutumisen uhan lisääntyneen ja neljäsosa (24 %) kokee valtiollisten toimijoiden vihamielinen toiminta uhan lisääntyneen.

Yli puolet (51 %) vastasi tietojenkalastelun ja social engineeringin lisääntyneen kahden viime vuoden aikana. Tämä voi olla indisio erilaisten kyberoperaatioiden ja hybriditoiminnan valmistelusta. Operaatioita voidaan valmistella erilaisen perinteisemmän urkinnan ja tietojenkalastelun keinoin.

Horisontin taakse on vaikea nähdä, mutta uhat, jotka sieltä nousevat saattavat realisoitua hyvinkin nopeasti niiden horisonttiin ilmaantumisen jälkeen. Kolmannes vastaajista arvioi, että uhkahorisontin muutoksella viimeisen parin vuoden aikana on ollut kokonaisuudessaan riskejä kasvattava vaikutus.

Covid-19 pandemia loi yllättäen uudenlaisia haasteita yritysturvallisuudelle esimerkiksi äkkinäisen ja laajamittaisen etätyöhön siirtymisen kautta. Puolet (51 %) vastaajista kokee etätöiden lisänneen tietoturvariskejä. Näistä haasteista selviäminen vaati nopeaa ja joustavaa reagointia, uudenlaisten menetelmien käyttöönottamista ratkaisukeskeisesti.

Venäjän aloittaman laajamittainen hyökkäyssota Ukrainaa vastaan on puolestaan nostanut uhkahorisonttiin uudenlaisia uhkia, joista useat ovat kyberfyysisiä ja kohdistuvat yrityksen vaikutusmahdollisuuksien ulkopuolella olevaan infrastruktuuriin. Tämä aiheuttaa uusia haasteita yritysten ja organisaatioiden kokonaisvaltaiseen kuin kyberturvallisuudenkin riskienhallintaan ja reagointiin.