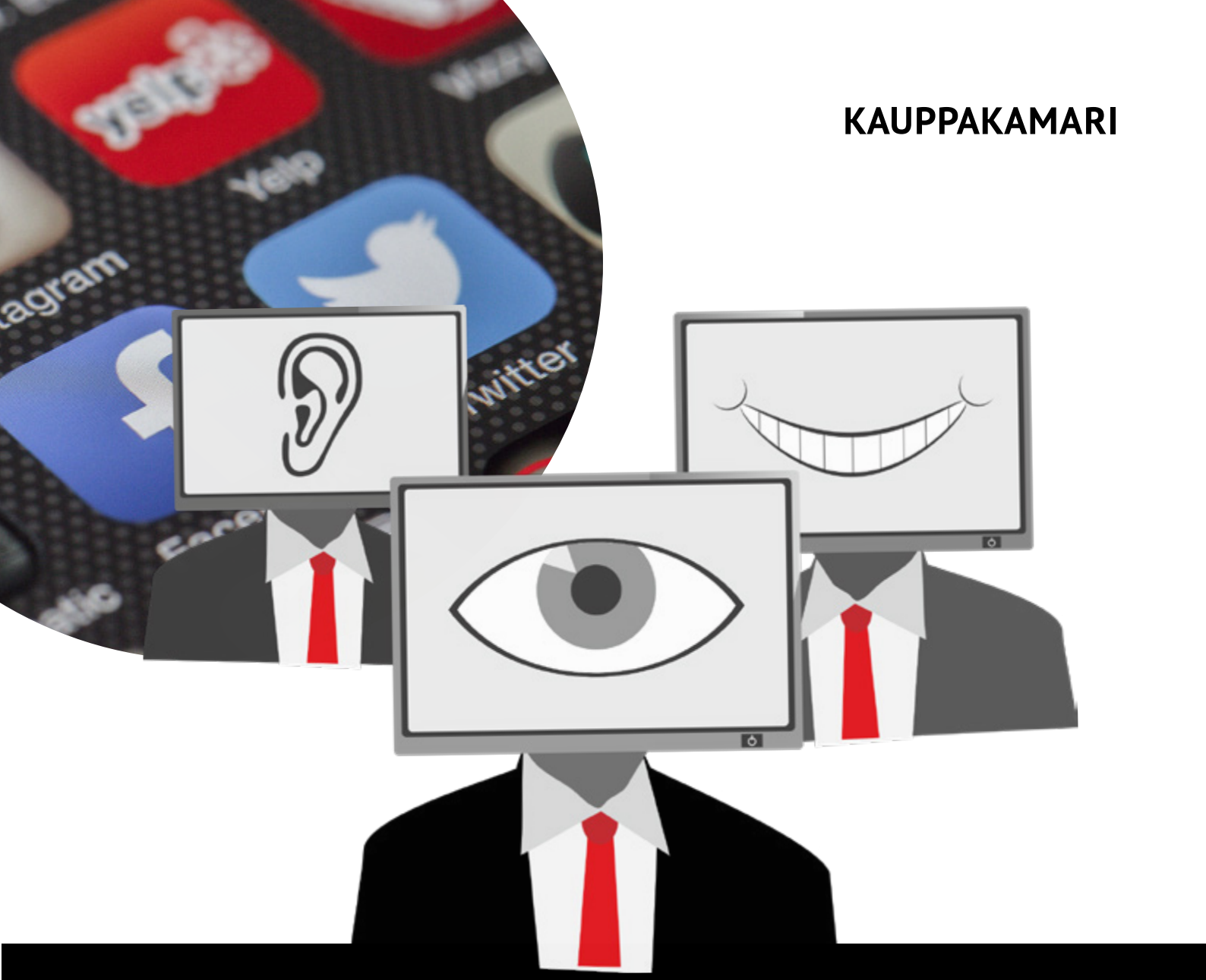
KAUPPAKAMARI



Elinkeinoelämä ja hybridivaikuttaminen

2018

Kesäkuu 2018

Helsingin seudun kauppakamari
Kalevankatu 12, 00100 Helsinki

www.helsinki.chamber.fi

SISÄLLYS

1 JOHDANTO

Elinkeinoelämä ja hybridivaikuttaminen 2018 -selvityksen tavoitteena on tutkia miten yritykset ymmärtävät hybridiuhat, millainen ilmiö hybridivaikuttaminen on, kuinka hybridiuhkat kohdistuvat yrityksiin ja miten yritykset ovat varautuneita niihin.

Hybridivaikuttaminen on laaja ja kehittyvä käsite. Vaikuttamista voidaan kohdistaa esimerkiksi poliittiseen päätöksentekoon, viranomaisten toimintaan ja elinkeinoelämään tai kaikkiin samanaikaisesti. Haastavaksi yksityiskohtaisen määrittelyn tekee se, että hybridivaikuttamiseen pyrkivä taho voi käyttää siihen vanhoja ja hyvin tunnettuja keinoja, mutta toisaalta myös sellaisia toimintatapoja, joita ei aiemmin ole osattu edes ajatella käytettäväksi. Kulloinkin haluttu lopputulos, kohde ja kohteen havaitut heikkoudet määrittelevät käytettävää keinovalikoimaa. Osin toiminta muodostuu vanhoista konsteista, alkaen yksittäisten ihmisten lahjomisesta tai kiristämisestä, päättyen toisaalta uusiin digitalisoitumisen avaamiin mahdollisuuksiin vaikuttaa kybertoiminnan kautta valittuun kohteeseen.

Hybridivaikuttamisen takana olevaa varsinaista tahoa voi olla vaikea tunnistaa, sillä toteutusvaiheessa sitä voi toteuttaa valtio, yritys, muu organisaatio kuten rikollisryhmittymä tai jopa yksittäinen henkilö. Se voi olla taloudellista tai poliittista vaikuttamista ja sen keinot voivat olla moninaisia kuten disinformaatiokampanjat, vaikutusaseman hankkiminen tarjoamalla taloudellisia etuja tai tekemällä sijoituksia yrityksiin tai poliittisiin toimijoihin ja äärimmilleen vietynä sisältäen esim. laajat valtioiden väliset taloudelliset kiristystoimet ja sotilaallisella voimalla uhkailun sekä sen rajatun käytön. Hybridivaikuttaminen on pääosin valtioiden poliittisiin tavoitteisiinsa pääsyksi käyttämää valtapolitiikkaa ja sen voisi kuvata sijaitsevan perinteisen sodankäynnin ulkopuolella, mutta propagandan, vakoilun, korruption ja diplomatian lähistöllä, niiden ympärillä ja osana niitä.

Hybridivaikuttaminen tarkoittaa nimensä mukaisesti useamman kuin yhden keinon käyttämistä tavoiteltaessa haluttua lopputulosta. Yritys voi olla lopullinen kohde, mutta todennäköisempää on että sitä käytetään reittinä tai välikappaleena lopulliseen strategiseen tavoitteeseen pyrittäessä. Yritykseen voi kohdistua esimerkiksi vain informaatiovaikuttamista, toiseen kohteeseen kybervaikuttamista ja kolmanteen kohteeseen fyysistä vaikuttamista. Se että yritys tunnistaa itseensä kohdistuvan vain yhdenlaista vaikuttamista ei sulje pois mahdollisuutta, että yritys on osana laajempaa hybridivaikuttamisoperaatiota. Hybridivaikuttamisoperaatiot voivat myös olla kestoltaan pitkäaikaisia ja mahdollisesti kohteestaan myönteiseltä vaikuttavia, mikä tekee osaltaan vaikeaksi tunnistaa niitä. Hybridivaikuttamisessa tukena käytettävä tieto on voitu kerätä vuosien aikana hybridivaikuttajatahon palkkalistoilla olevien henkilöiden toimesta, perinteisin ihmistenvälisin henkilötiedustelun keinoin tai sitten kybermaailman heikkouksia hyväksikäyttäen. Yritysten normaali rikosturvallisuus, henkilökunnan kouluttaminen ja tiedon jakaminen verkostoissa kumppanien ja viranomaisten kanssa ovat yritysten ensisijaisia työkaluja varauduttaessa hybridivaikuttamiseen.

Elinkeinoelämä on merkittävä osa yhteiskuntaa ja sen merkitys on lisääntynyt entisestään aiemmin viranomaisille kuuluneiden tehtävien ulkoistusten, yhteiskunnan digitalisoitumisen ja elinkeinoelämän ja viranomaisten välisen verkottumisen vuoksi. Yritykset kantavat usein myös omistajuuden lisäksi vastuun kriittisen infrastruktuurin toiminnasta normaali- ja poikkeusoloissa. Elinkeinoelämän roolia suomalaisen yhteiskunnan suojaamisessa hybridivaikuttamiselta korostaa myös usein muissa yhteyksissä perinteisesti eduksi katsottu maamme pienuus ja äärimmäisen verkottunut yhteiskunta. Toisaalta vaikuttaminen tällaisessa yhteiskunnassa voi olla tehokkaampaa kuin suuressa ja hajanaisessa yhteiskunnassa. Siksi Suomen osalta eri keinoin värvättyjen henkilöiden ja muiden tahojen merkitys voi olla suurempi kuin joissain muissa Euroopan maissa.

Tutkimustuloksista yritykset saavat myös kuvan oman toimialansa tilanteesta. Selvitys on osa Helsingin seudun kauppakamarin yritysturvallisuustyötä. Helsingin seudun kauppakamarilla on 7 000 jäsenyritystä kaikilta toimialoilta. Koko Suomessa kauppakamareilla on yli 20 000 jäsenyritystä.

Tutkimuksen toteuttaminen ja vastaajien taustatiedot

Selvitys käsittelee suomalaisten yritysten käsityksiä niihin kohdistuvista hybridiuhista ja niihin varautumisesta. Erityisesti selvitys keskittyy vastaajayrityksiin kohdistuviin tunkeutumisuhkiin. Selvitys perustuu 764 suomalaisen yrityksen antamiin vastauksiin.

Taloustutkimus toteutti kyselyn Helsingin seudun kauppakamarin toimeksiannosta. Yritykset vastasivat kyselyyn toukokuussa 2018. Tutkimustulokset on esitetty taulukkoina ja kuvioina, joista yksittäisen vastaajan mielipide ei käy ilmi.

Selvityksen ovat laatineet projektipäällikkö Panu Vesterinen Helsingin seudun kauppakamarista, Chris Fogle CyVantage Llc -yrityksestä ja johtava tutkija Pasi Eronen Foundation for Freedom of Democracies -ajatushautomosta. Selvitys on osa kauppakamarijärjestön yritysturvallisuustoimintaa.

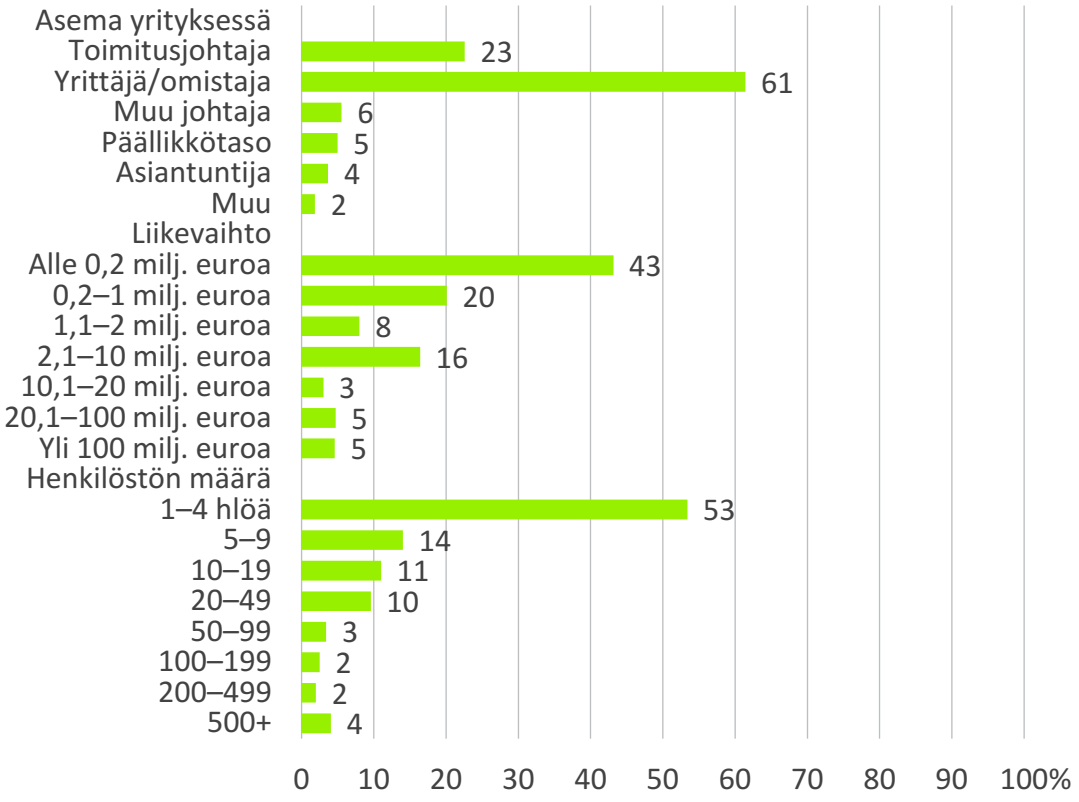
Kyselyyn vastanneista 762 yrityksestä 57 prosenttia edustaa palveluita, 16 prosenttia teollisuutta ja 14 prosenttia kauppaa. Rakennusalan yrityksistä on vastaajista 13 prosenttia.

Vastanneista yrityksistä 87 % on henkilömäärältään pieniä yrityksiä, jotka työllistävät alle 50 henkilöä. Viisi prosenttia vastaajista on keskisuuria yrityksiä, joiden palveluksessa on 50 – 200 työntekijää. Suuria yrityksiä, jotka työllistävät yli 200 henkilöä, oli kuusi prosenttia vastaajista.

Vastaajat olivat yritysten toimitusjohtajia (23 %), yrittäjiä tai omistajia (61 %), muita johtajia (6 %). Neljä prosenttia vastaajista oli asiantuntijatehtävissä. Päällikkötason tehtävissä vastaajista oli viisi prosenttia. Vastaajien rakenne kertoo siitä että tutkimus on tavoittanut hyvin yritysten päätöksentekijät – turvallisuuden kehittämisen kannalta ratkaisevan ryhmän.

Selvityksen lähdeluetteloon on koottu lisätietoa hybridiuhista yritysten turvallisuustoiminnan tueksi.

Selvityksen tavoitteena on tukea ja kehittää yritysten omaa riskienhallintatyötä. Tuloksista yritykset saavat paremman kokonaiskuvan hybridiuhista ja siitä miten uhkiin on osattu varautua.



2 YRITYKSET HYBRIDIVAIKUTTAMISEN KOHTEINA

Tämän selvityksen tavoitteena on tuoda esille tietoa yrityksiin kohdistuvasta hybridivaikuttamisesta. Hybridivaikuttaminen on luonteeltaan sellaista, että se jää suurimmaksi osaksi piiloon ja kun se on tunnistettavissa, on jo liian myöhäistä käynnistää vastatoimia. Siksi hybridivaikuttamisen nostaminen julkisuuteen tällaisen selvityksen kautta on tärkeää.

Hybridivaikuttamista kohdistuu elinkeinoelämään. Onnistunut hybridivaikuttaminen ei suurella todennäköisyydellä päädy tilastoihin. Se asettaa myös haasteen asian selvittämiselle.

Syyt, joiden vuoksi yritykseen voisi kohdistua hybridivaikuttavaa toimintaa

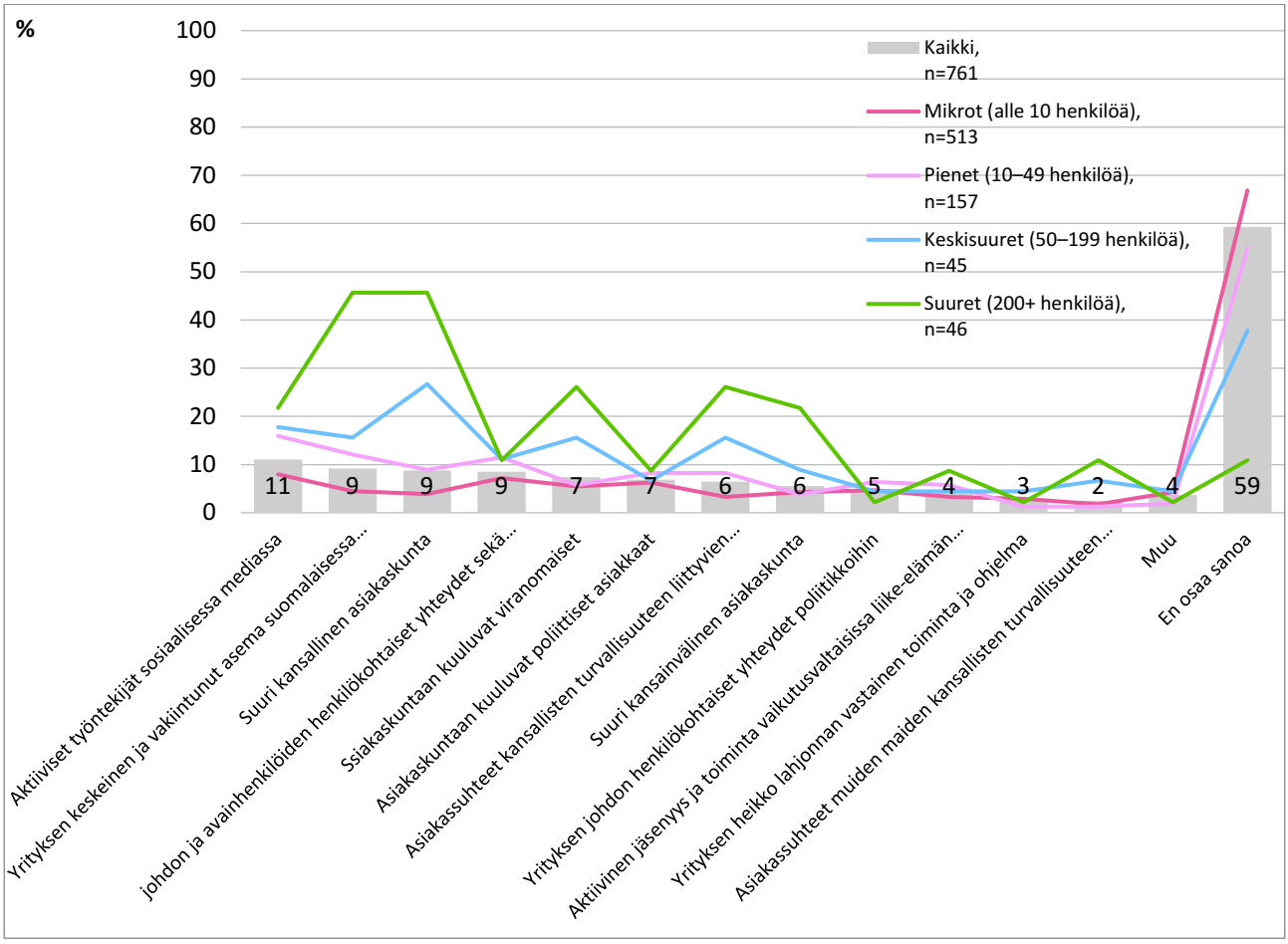
Yli puolet yrityksistä (59 %) ei osannut kertoa syitä, joiden vuoksi yrityksiin kohdistuisi toimintaa, jonka lopullisena tarkoituksena olisi vaikuttaa suomalaiseen tai muun maan väestöön tai hallintoon. Vastaus osoittaa aiheen olevan vaikea tunnistaa ja sen että elinkeinoelämän keskuudessa ei ole vielä ymmärretty sen roolia hybridivaikuttamisen kohteena.

Yleisimpänä syynä (11 %) mainittiin aktiiviset työntekijät, jotka toimivat sosiaalisessa mediassa ja joilla on paljon seuraajia. Julkisuudessa on käsitelty paljon eri maiden vaaleihin vaikuttamista ja siitä toiminnasta päivänvaloon on noussut lähes ainoastaan sosiaalisen median kautta tapahtunut vaikuttaminen. Yritykset eivät vielä tunnista miten monin eri syin ne voivat päätyä hybridivaikuttamisen kohteeksi. Sosiaalinen vaikuttaminen voi olla vain osasyy, jolla yritys tai sen työntekijä valikoituu kohteeksi. Aktiivisuus sosiaalisessa mediassa voi toisaalta nostaa pienenkin yrityksen kohteeksi. Jos sosiaalisessa mediassa julkaistaan sellaista materiaalia, joka paljastaa yrityksen toiminnasta ja suhteista viranomaisiin tai poliitikkoihin sellaista tietoa, voi tämä olla kohteeksi määrittävä tekijä.

Vastaajat nostivat kolme seuraavaa syytä esille seuraavaksi yleisimpinä syinä:

- Yrityksen keskeinen ja vakiintunut asema suomalaisessa yhteiskunnassa (9 %)
- Suuri kansallinen asiakaskunta (9 %)
- Yrityksen johdon ja avainhenkilöiden henkilökohtaiset yhteydet sekä johtaviin että toteuttavan tason viranomaisiin (9 %)

Kun mietitään miksi yritys voisi joutua hybridivaikuttamisoperaation osakohteeksi, on muistettava että kyseessä on usein valtioiden välinen toiminta. Tässä toiminnassa hyödynnetään erilaisia toimijoita, kuten ulkomaista tai kotimaista ammattirikollisuutta, tietämättään bulvaaneina toimivia tahoja, järjestöjen edustajia tai jotain muuta toimijaa. Tapa lähestyä ja käyttää yritystä hyväkseen riippuu lopullisesta tavoitteesta, kohteesta, yrityksen heikkouksista ja muista tekijöistä, joita kukaan muu kuin vaikuttamisoperaatiota suunnitteleva ja johtava ei tiedä. Helpompaa olisi ajatella niin että yritys saattaa joutua rikollisen toiminnan kohteeksi, oli sitten kyseessä järjestäytynyt rikollisuus, vakoilu tai hybriditoiminta, joka täyttää jonkin rikoksen tunnusmerkistön. Ja sen jälkeen kehittää yrityksen rikosturvallisuutta ja turvallisuusmyönteistä yrityskulttuuria.



Suurien vastaajien osalta esille nousivat seuraavat syyt joutua vaikuttamisen kohteeksi:
- Keskeinen ja vakiintunut asema suomalaisessa yhteiskunnassa (45 %)
- Suuri kansallinen asiakaskunta (45 %)
- Asiakassuhteet kansallisen turvallisuuteen liittyvien viranomaisten kanssa (25 %)
- Asiakaskuntaan kuuluvat viranomaiset (25 %)
- Suuri kansainvälinen asiakaskunta (45 %)

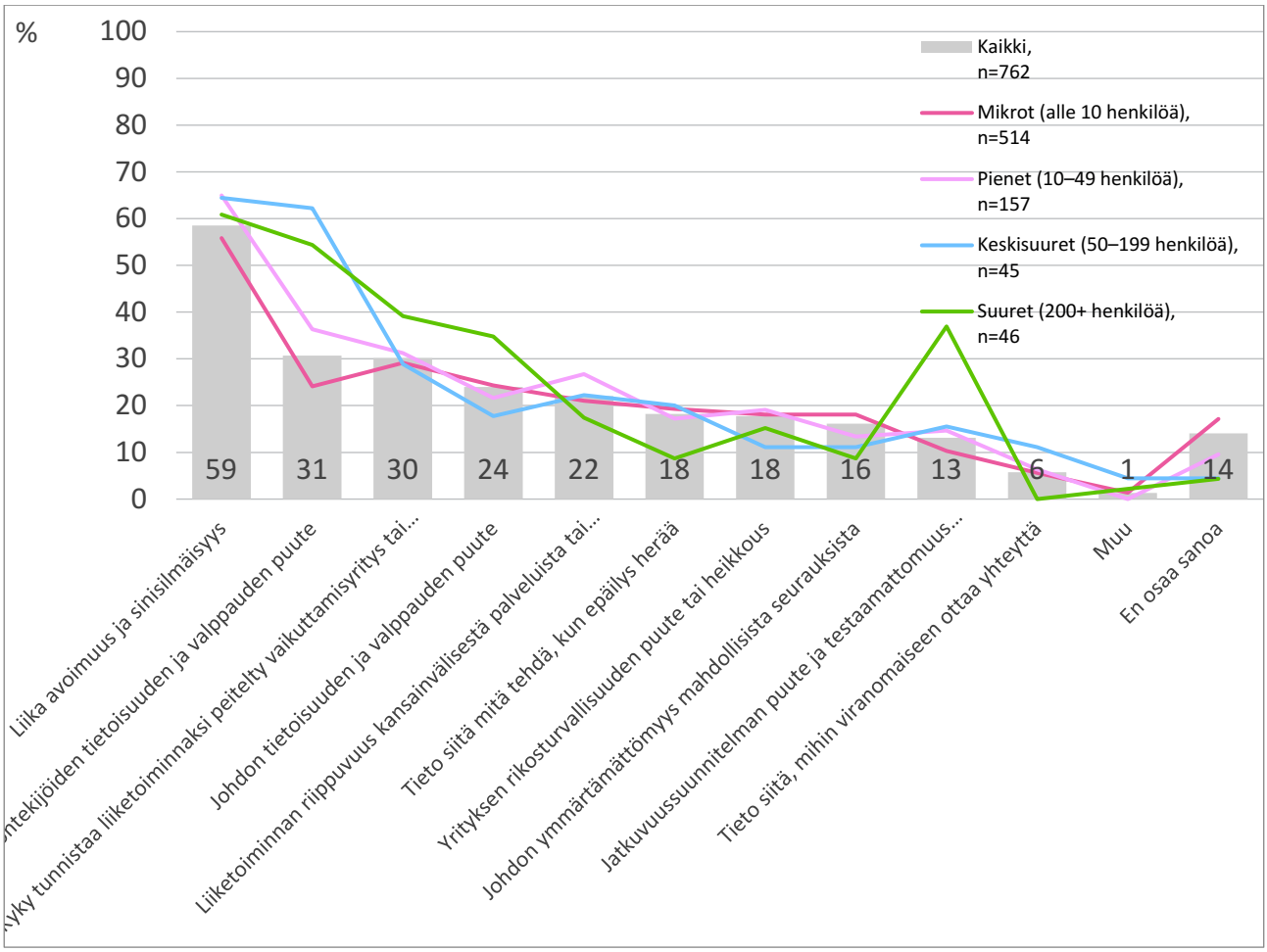
Keskikokoisten vastaajien osalta
- Suuri kansallinen asiakaskunta (25 %)
- Keskeinen ja vakiintunut asema suomalaisessa yhteiskunnassa (16 %)
- Asiakassuhteet kansallisen turvallisuuteen liittyvien viranomaisten kanssa (15 %)
- Asiakaskuntaan kuuluvat viranomaiset (15 %)
- Aktiiviset työntekijät sosiaalisessa mediassa (18 %)

Sekä suurien ja keskikokoisten vastaajien vastaukset kuvaavat yritysten toiminnan laajuudesta ja näkyvyydestä syntyvää maalipinta-alaa. Näiden yritysten on vaikea olla näkymättömiä ja siksi ne nousevat helpommin esille kun kartoitetaan mahdollisia kohteita ja niistä esille nousevia mahdollisuuksia päästä vaikuttamaan. Hybridivaikuttamisessa voidaan käyttää vuosien aikana kerättyä tietoa ihmisistä, heidän kontakteistaan ja heikkouksistaan. Näiden kautta voidaan esimerkiksi saada pääsy yrityksen tietoon.

Yritysten heikkoudet joiden kautta ulkomaiset tahot pyrkivät vaikuttamaan

Kolme merkittävintä suomalaisten yritysten heikkoutta, kun puhutaan ulkomaisten toimijoiden (rikollisten tai valtioiden) pyrkimyksistä vaikuttaa liiketoimintaan ovat liika avoimuus ja sinisilmäisyys (59 %), työntekijöiden tietoisuuden ja valppauden puute (31 %) sekä kyky tunnistaa liiketoiminnaksi peitelty vaikuttamisyritys tai hanke yrityksen hyödyntämiseksi tarkoituksena vaikuttaa varsinaiseen kohteeseen (30 %).

Hybridivaikuttamisesta ja vakoilusta ei ole tarpeeksi tietoa tarjolla. Avoimuus, sinisilmäisyys, tietoisuuden puute, valppauden puute tai kyky tunnistaa ovat kaikki asioita, jotka enemmän tai vähemmän voidaan korjata tiedon jakamisella ja koulutuksella siinä määrin kun niiden korjaaminen on mahdollista. Hybridivaikuttajan kannalta ihmisten hyödyntämisen rooli informaatio- ja kybervaikuttamisen rinnalla voi olla yllättävän suuri, eritoten koska Suomi on hyvin verkottunut ja pieni yhteiskunta.



Suurissa yrityksissä korostui myös jatkuvuussuunnitelman puute ja testaamattomuus (poikkeustilanteen kestokyky). Työntekijöiden tietoisuuden ja valppauden puute korostuu sekä keskisuurissa että suurissa yrityksissä. Muutoin näiden vastaajaryhmien linja oli sama kuin pienten yritysten.

Suurien vastaajien osalta esille noussut jatkuvuussuunnitelmien puute ja testaamattomuus kertoo siitä että nämä vastaajat tiedostavat mitä valtiollinen hybridivaikuttaminen voi aiheuttaa elinkeinoelämälle. Tuotannon katkaiseminen ja laajempi liiketoiminnan häiritseminen voivat olla osana ”näkyvän vaiheen” hybridivaikuttamista. Tällöin ratkaisevaan osaan nousee yritysten valmius kestää jatkuvuuttaan uhkaavien toimien seurauksia kuten sähkön- tai polttoaineensaannin rajallisuutta.

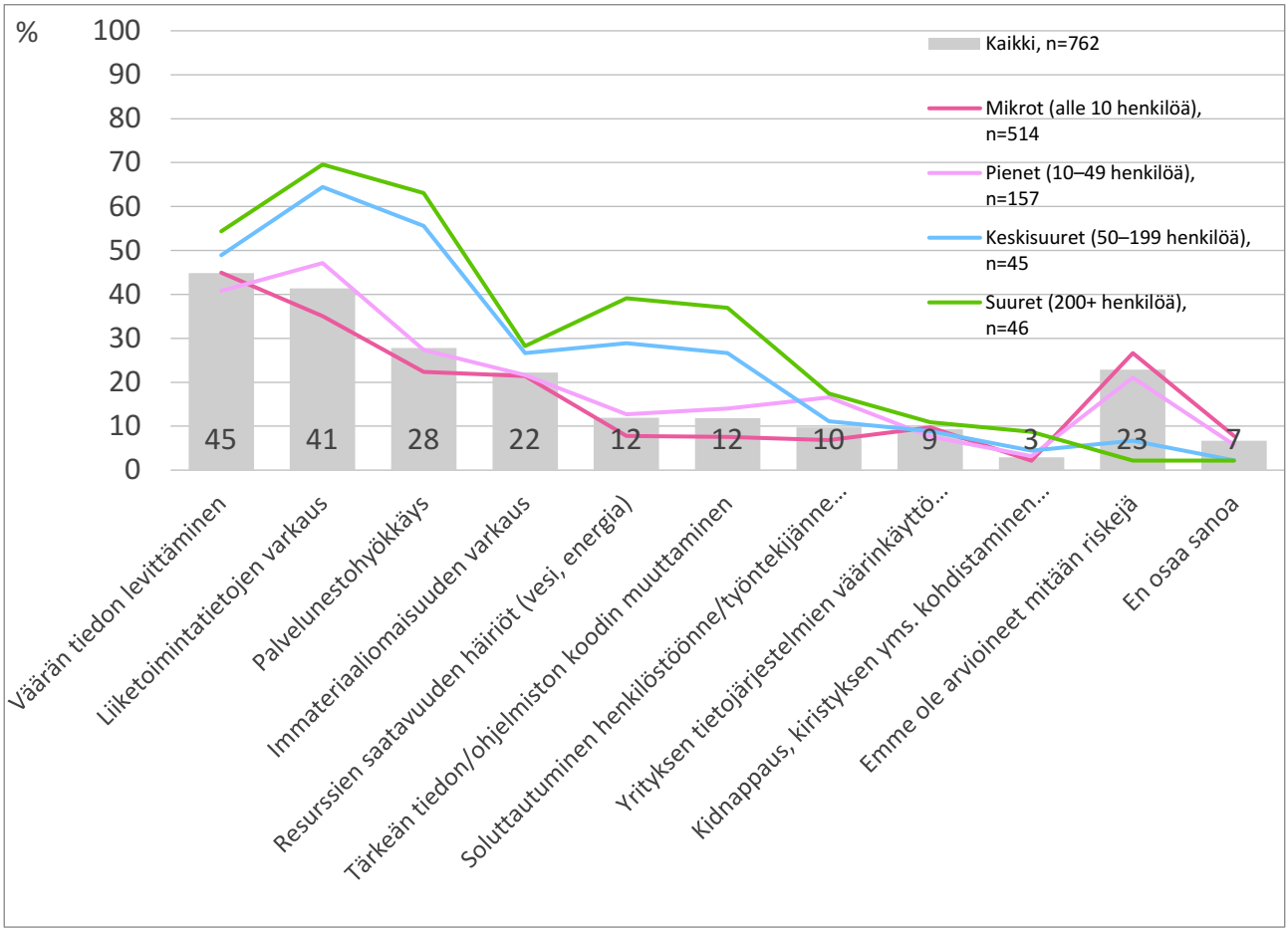
Hybridivaikuttamisen suurimmat riskit yrityksille

Hybridivaikuttaminen on riski muiden yritykseen kohdistuvien riskien joukossa. Siksi se voidaan ottaa osaksi normaalia riskienarviointia ja sitä kautta siihen voidaan tarpeen mukaan varautua riskienhallintaprosessin keinoin. Tällöin varautumisessa ei myöskään pääse tapahtumaan ylilyöntejä tai laiminlyöntejä hybridiuhkien arvioimattomuuden takia.

Kun vastaajilta kysyttiin suurimpia riskejä, nousivat esille väärän tiedon levittäminen (45 %), liiketoimintatietojen varkaus (41 %) ja palvelunestohyökkäys (28 %). Väärän tiedon levittäminen on riski, joka on ollut esillä julkisuudessa. Julkisuus saattaa selittää palvelunestohyökkäyksen korkean sijoituksen.

Suurien vastaajien ja keskisuurten vastaajien keskuudessa edellä mainittujen lisäksi esille nousivat resurssien saatavuuden häiriöt ja tärkeän tiedon tai ohjelmiston koodin muuttaminen. Yhteiskunnan toimivuuteen voidaan yrittää vaikuttaa osana hybridivaikuttamisoperaatiota. Resurssien saatavuuden häiriöt ja esimerkiksi tuotannon ohjausjärjestelmien ja logistiikkajärjestelmien tietojen tai koodin manipulointi voivat johtaa vakaviin häiriötilanteiseen, joilla on merkittäviä yhteiskunnallisia heijastevaikutuksia.

Miltei neljäsosa (23 %) kaikista vastaajista ei ollut arvioinut riskejä lainkaan.



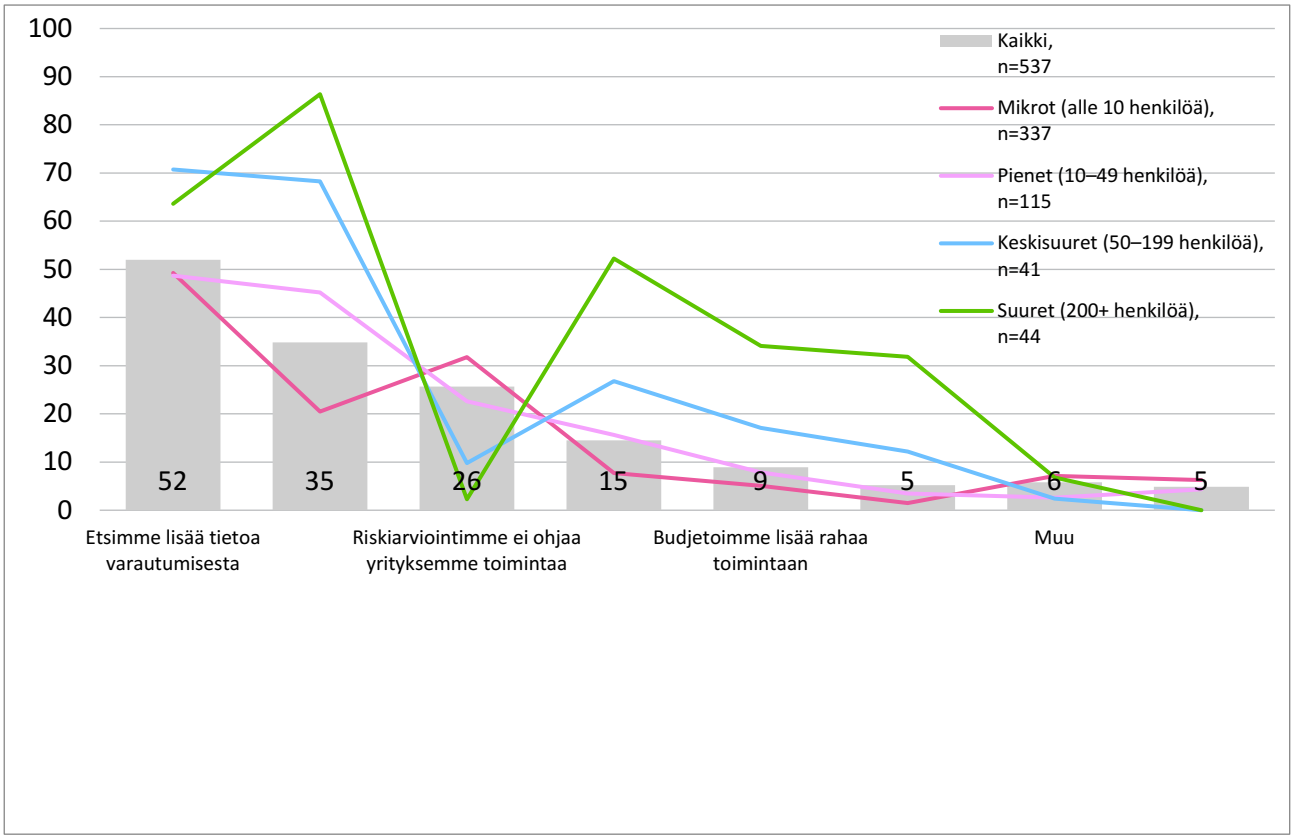
Miten riskiarvionne ohjaa yrityksenne toimintaa?

Riskit arvioineista yrityksistä puolet (52 %) kertoivat riskiarvion ohjaavan yrityksen toimintaa siten että he etsivät lisää tietoa varautumisesta ja noin kolmannes lisäämällä koulutusta (35 %).

Riskiarvio ei ohjaa yrityksen toimintaa noin joka neljännessä (26 %) riskiarvion tehneessä yrityksessä. Tehdessään riskienarvioinnin yritys käyttää resurssejaan siihen ja jos tuloksia ei käytetä, olisi viisaampaa ollut jättää riskienarviointi tekemättä ja käyttää resurssit johonkin muuhun josta seuraisi jotain konkreettista yrityksen hyväksi.

Suurista vastaajista puolet hakeutuu yhteistyön viranomaisten kanssa (52 %), kolmasosa budjetoi lisärahaa (34 %) ja samoin kolmasosa lisää henkilöresursseja (32 %) .

Vain pieni murto-osa kaikista vastaajista budjetoi lisää rahaa (9 %) tai rekrytoi lisää väkeä turvallisuustoimintoihin (6 %). Riskienarvioinnin ei kuulukaan automaattisesti johtaa näihin, mutta usein törmää tilanteeseen, jossa uusienkin riskien hallinta ja niihin varautuminen jätetään olemassa olevien henkilöresurssien varaan. Joissain tilanteissa nämä resurssit ovat jo täysin työllistettyjä. Silloin varautuminen uusiin riskeihin ei voi olla kovin tehokasta.

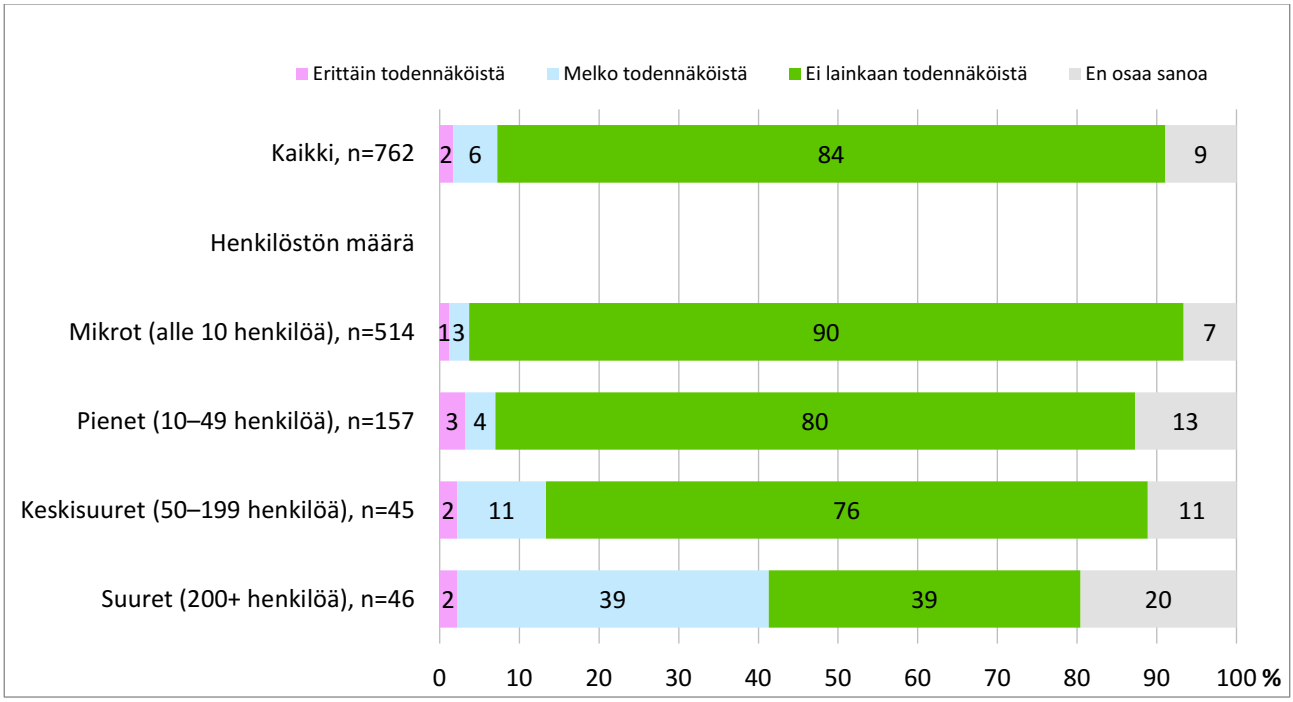


Rikollisten tai ulkomaisten valtion toimijoiden vaikuttamisen kohdistamisen todennäköisyys

Joka kymmenes vastaaja (8 %) piti mahdollisen että rikolliset tai ulkomaiset toimijat voisivat kohdistaa niihin vaikuttamista. Käytännössä hybridivaikuttamisen tai laittoman tiedustelun kohteina kiinnostavien yritysten määrä on kuitenkin suurempi. Hybridivaikuttamisen tunnistaminen on vaikeaa eivätkä kaikki yritykset edes tiedosta olevansa mahdollisia kohteita. Sen vuoksi tarve viranomaisten tuottamalle kouluttamiselle ja tiedonjakamiselle korostuu.

Valtaosa yrityksistä (84 %) eivät pidä todennäköisenä, että rikolliset tai ulkomaiset valtion toimijat voisivat kohdistaa yritykseen toimintaa, jonka lopullisena tarkoituksena olisi vaikuttaa Suomen sisäiseen vakauteen, talouteen, ulko- ja turvallisuuspolitiikkaan tai hallituksen toimintaan. Suurin osa yrityksistä ei tällä hetkellä välttämättä ole potentiaalisia kohteita hybridivaikuttamiselle. Yritys tai sen johtoon kuuluva, joka ei tänään ole mahdollinen kohde, voi olla sitä huomenna. Yksi tämän selvityksen tavoitteista on herättää tietoisuutta hybridivaikuttamisesta elinkeinoelämän keskuudessa.

Suurista yrityksistä (200+ henkilöä) 41 % arvioi heihin kohdistuvan hybridivaikuttamisen olevan vähintään melko todennäköistä. Suuret yritykset ovat näkyviä, niillä on usein laaja asiakaskunta, valtiollisia asiakkaita, suhteita poliitikkoihin, yhteiskunnan infraan liittyviä toimeksiantoja ja muita vastavia tekijöitä joiden kautta ne voivat valikoitua kohteiksi hybridivaikuttamisoperaatioihin. Keskisuurista vastaajista yli kymmenesosa (13 %) piti tätä vähintään melko todennäköisenä.

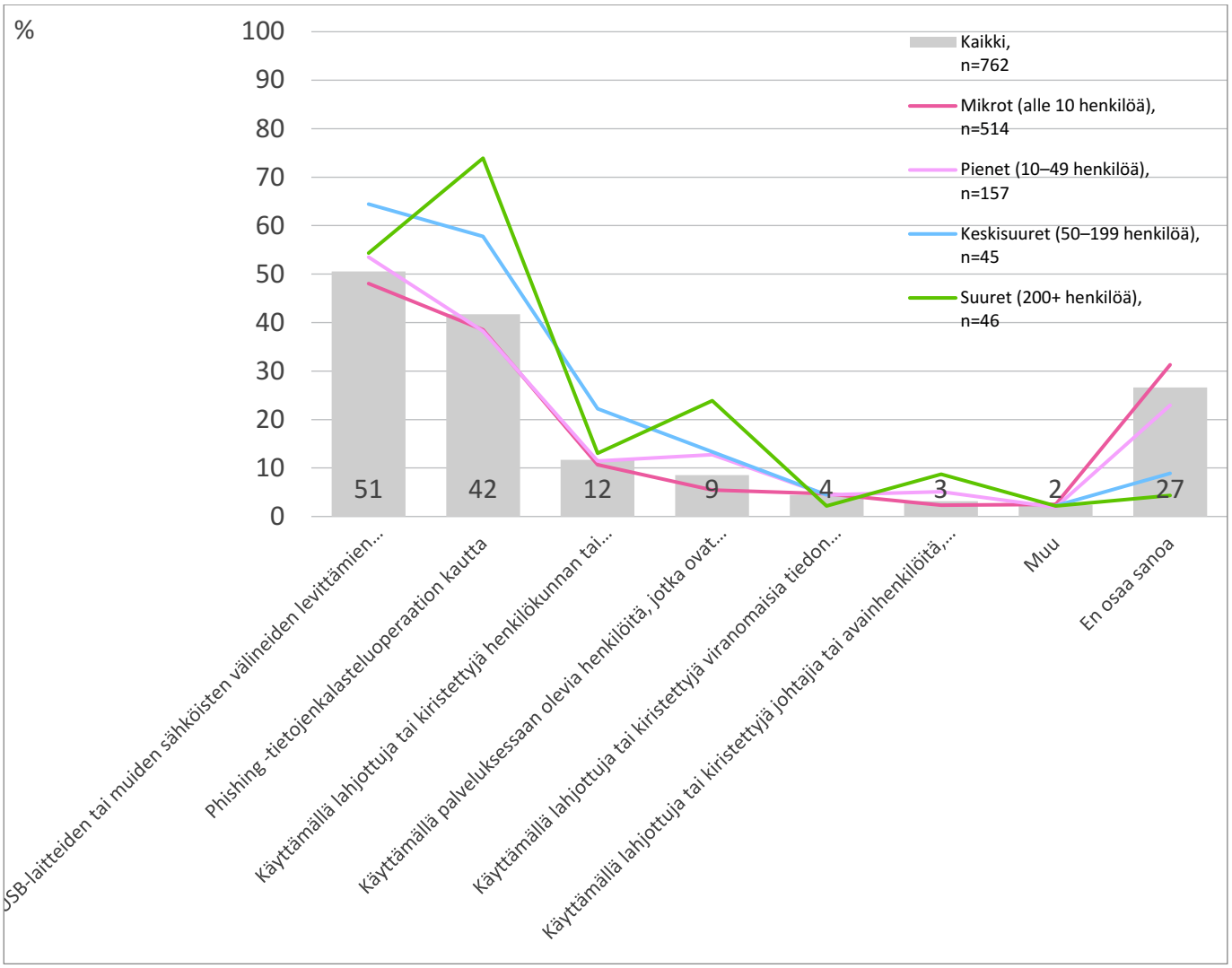


Rikollisten tai ulkomaisten tiedustelupalvelujen pääsy yrityksen tietoihin

Rikollisten tai ulkomaisten tiedustelupalveluiden uskotaan pääsevän kohteeksi valitsemansa yrityksen tietoihin ulkopuolisen USB-laitteiden tai muiden sähköisten välineiden levittäminen haittaohjelmien avulla (51 %) ja phishing –tietojenkalasteluoperaation kautta (42 %).

Edellä mainitut ovat varmasti yleisimpiä tapoja päästä tietojärjestelmien kautta kohdeyritysten tietoon käsiksi. Näin saatua tietoa voidaan käyttää ihmisiin vaikuttamiseen. Hyödynnettävä tieto voi olla varsin harmittoman tuntuista kuten kuka vastaa mistäkin asiakkuudesta, harrastaa samoissa ryhmissä kuin joku poliittinen päättäjä ja niin edelleen. Kun tämä tieto yhdistetään näin esille nousseen henkilön sosiaalisen median profiilitietoihin ja internet -käyttäytymiseen sekä muista lähteistä kerättyihin tietoihin, saattaa näistä syntyä jo varsin hyvä lähtökohta ammattimaiselle hybridivaikuttamisen osaajalle.

Suurien vastaajien keskuudessa nousivat muista kokoluokkia selkeämmin esille phishing-operaatiot (74 %) ja värvättyjen henkilöiden käyttäminen kohdeyrityksen sisällä tiedonkeruuseen (23 %). Kaikista vastaajista joka kymmenes (9 %) piti värvättyä henkilöä tienä yrityksen tietoon. Värvättyjen henkilöiden käyttäminen voi olla varsin tuloksellista, sillä he pääsevät tehtäviensä puolesta käsiksi monenlaiseen tietoon, tietävät myös missä mitäkin tietoa on, saavat selville helposti vaikutusasemassa olevien henkilöiden heikkoudet ja mitä yrityksessä tapahtuu. Kaikki tämä on tietoa, jota hyödyntämällä hybridivaikuttaja voi arvioida kannattaako kohteeseen käynnistää hybridivaikuttamisoperaatiota. Oli yritys sitten lopullinen kohde tai väline tai reitti lopulliseen kohteeseen vaikuttamisessa. Etuna ihmisten hyödyntämisessä on se että yrityksen sisällä toimivat henkilöt saavat nämä tiedot siten, ettei heistä jää juurikaan normaalista työnteosta poikkeavia jälkiä tai toiminnan tunnistaminen muutoin on lähes mahdotonta. Henkilön lahjominen tai kiristäminen ovat varteenotettavia värväyksen vaihtoehtoja, koska ne ovat huomaamattomia eikä kohde monessakaan tapauksessa halua itse tuoda tilannetta esille.

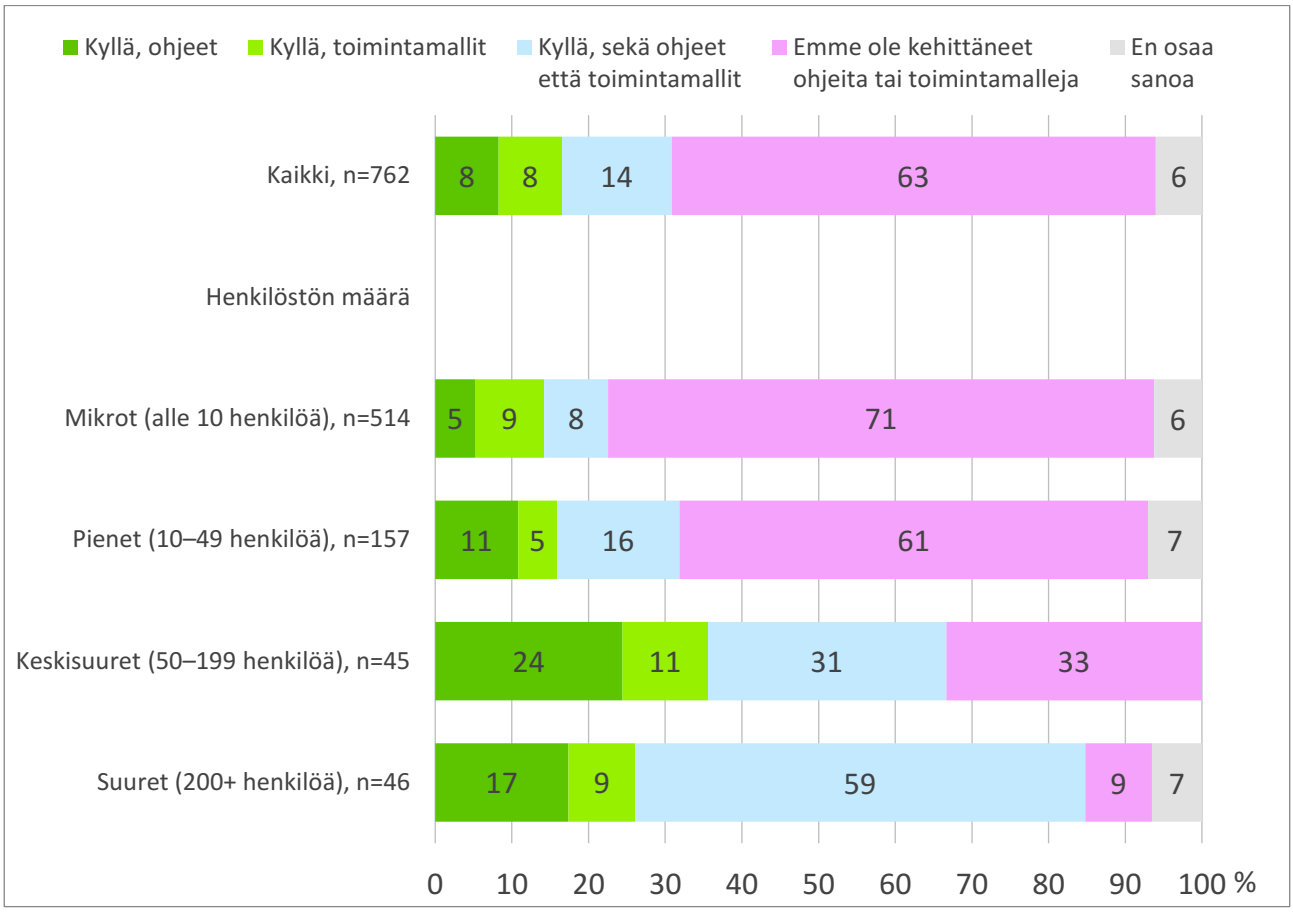

%
100
90
80
70
60
50
40
30
20
10
0
51
42
12
9
4
3
2
27
Kaikki, n=762
Mikrot (alle 10 henkilöä), n=514
Pienet (10–49 henkilöä), n=157
Keskisuuret (50–199 henkilöä), n=45
Suuret (200+ henkilöä), n=46
USB-laitteiden tai muiden sähköisten välineiden levittämien...
Phishing -tietojenkalastelu operaation kautta
Käyttämällä lahjottuja tai kiristettyjä henkilökunnan tai...
Käyttämällä palveluksessaan olevia henkilöitä, jotka ovat...
Käyttämällä lahjottuja tai kiristettyjä viranomaisia tiedon...
Käyttämällä lahjottuja tai kiristettyjä johtajia tai avainhenkilöitä,...
Muu
En osaa sanoa

3 YRITYSTEN VARAUTUMINEN HYBRIDIVAIKUTTAMISEEN

Ohjeet tai toimintamallit riskien varalle

Kaksi kolmasosaa vastaajista (63 %) ei ole kehittänyt ohjeita tai toimintamalleja suojatakseen yrityksen tietoja edellisen kysymyksen eri pääsytapojen estämiseksi. Noin joka kolmannella (30 %) on kehitettynä ohjeet, toimintamallit tai molemmat. Erityisesti yli 50 henkilöä työllistävillä yrityksillä on joko ohjeet tai toimintamallit tai molemmat (66 %). Suurin vastaajien keskuudessa vastaava prosentti on korkein (84 %).

Toisaalta hybridivaikuttamisen ja tietoon kohdistuvan muun rikollisuuden monimuotoisuuden ja laajan keinovalikoiman vuoksi kaikkeen ei voi edes laatia ohjeistuksia tai toimintamalleja. Näissä tilanteissa ratkaisevassa asemassa on työntekijöiden yleinen turvallisuusvalppaus, jota voidaan kehittää jakamalla tietoa, kouluttamalla ja rakentamalla pitkäjänteisesti turvallisuusmyönteistä yrityskulttuuria.



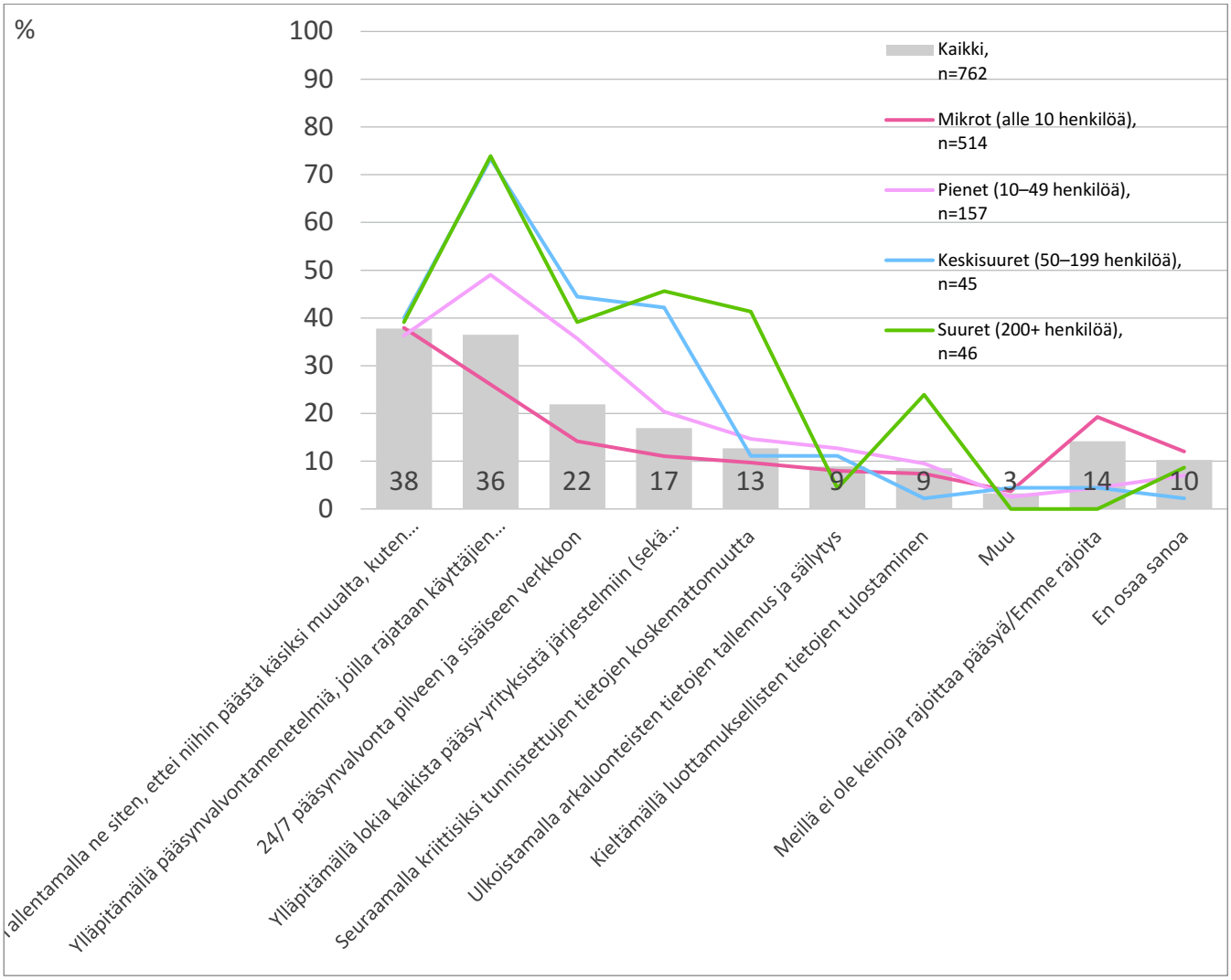
Pääsyn rajoitus tärkeisiin ja/tai luottamuksellisiin yritystietoihin

Kaikista vastaajista yli kolmasosa (38 %) rajoitti tärkeisiin ja/tai luottamuksellisiin yritystietoihin pääsyä siten, ettei niihin pääse käsiksi muualta, kuten tietojärjestelmästä tai internetistä. Samoin yli kolmasosa (36 %) ylläpitää pääsynvalvontamenetelmiä, joilla rajataan käyttäjien pääsyn tietoihin ja palveluihin.

Pääsynvalvontamenetelmien käyttö painottuu erityisesti suuriin ja keskisuuriin yrityksiin. Suurissa yrityksissä ylläpidetään myös lokia pääsy-yrityksistä järjestelmiin (45 %) sekä seurataan kriittisiksi tunnistettujen

tietojen koskemattomuutta (41 %). Lähes joka neljäs suuri vastaaja on kieltänyt luottamuksellisten tietojen tulostamisen (23 %) osana tiedon suojaamistoimiaan.

Yrityksen on suojattava tietojaan varautui se sitten hybridiuhkaan, vakoiluun tai tietomurtoihin. Mitä suurimpi joukko työntekijöitä pääsee yrityksen luottamukselliseen tietoon, jota ei työnsä puolesta tarvitse, sitä helpompaa on saada joku hankkiutumaan tietoon käsiksi ja toisaalta myös rajoitetun pääsyn ennaltaehkäisevä vaikutus jää saavuttamatta. Yritys vastaa oman tietonsa luokittelemisesta ja sen asianmukaisesta suojaamisesta. Tiedon luokittelu on tiedon suojaamisen perusta, ilman sitä on vaikea tietää mitä pitää suojata ja kenellä on tarve päästä tietoon käsiksi.

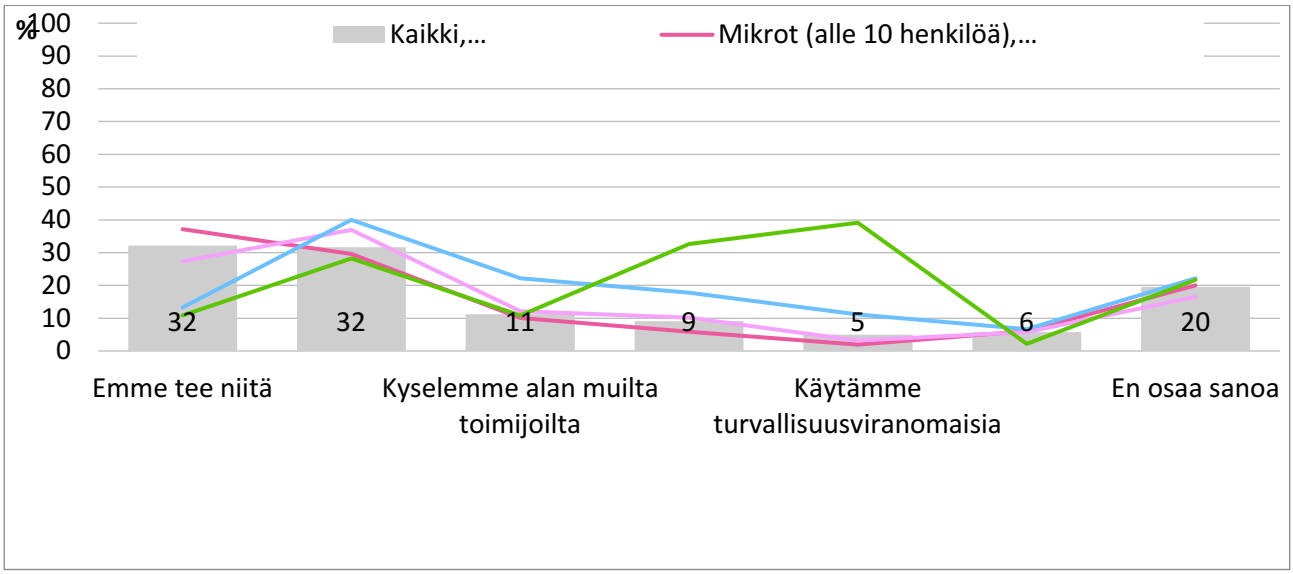


Ulkomaisten liikekumppanien ja heidän yhteyksiensä taustatutkimukset

Ulkomaisten liikekumppaneiden (yritysten ja/tai yksityishenkilöiden) ja heidän yhteyksiensä taustatutkimukset useimmiten joko jätetään tekemättä (32 %) tai tehdään itse (32 %). Suurista yrityksistä noin joka kolmas käyttää turvallisuusviranomaisia (39 %) tai erikoistuneita palveluntarjoajia (32 %).

Taustantarkastukset ovat tarpeen esimerkiksi jo lahjonnanvastaisen toiminnan, rahanpesun ja terrorismin rahoittamisen estämiseksi. Kansainvälisesti toimivan yrityksen on hyvä selvittää liikekumppaniensa taustat jo monen muun syyn kuin hybridivaikuttamisen vuoksi. Tässä yrityksillä on paljon parannettavaa.

Yrityksillä on paljon hyödyntämätöntä potentiaalia yhteistyön vähäisyyden vuoksi. Kun toimitaan kansainvälisillä markkinoilla, voisivat yritykset tehdä enemmän yhteistyötä muissakin asioissa kuin taustatarkastusten osalta. Aivan kuten kyberturvallisuuden saralla, yritykset voisivat käynnistää yhteistyömalleja, joissa vaihdettaisiin kilpailuneutraalia tietoa yritysten kesken.

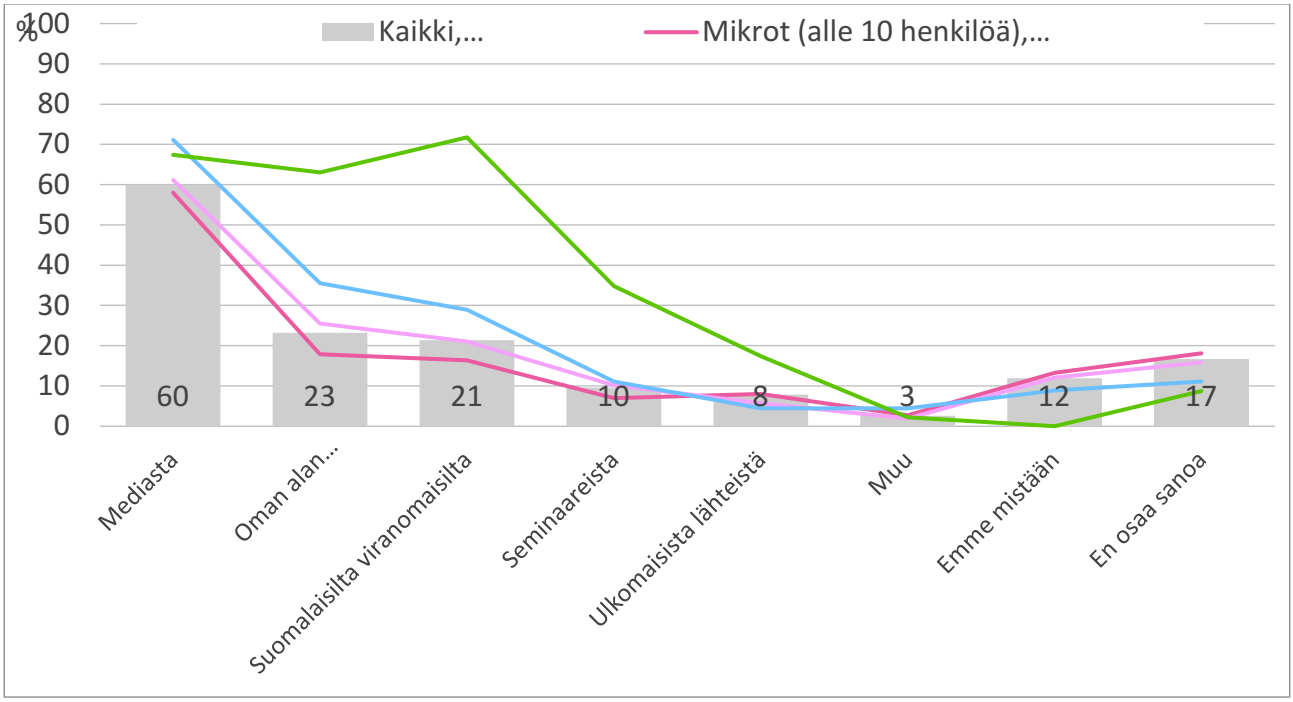


Tiedonsaantikanavat hybridioperaatioihin liittyvästä toiminnasta/toimijoista

Suurin osa yrityksistä (60 %) saa tietoa hybridioperaatioihin liittyvästä toiminnasta tai toimijoista mediasta. Tämän lisäksi tietoa saadaan oman alan tiedonvaihtoryhmistä (23 %) ja suomalaisilta viranomaisilta (21 %). Viranomaiset tiedon lähteenä korostuu suurien yritysten keskuudessa (70 %).

Hybridioperaatioihin liittyviltä uutisilta on vaikea välttyä. Lähes joka viikko viimeisen parin vuoden aikana mediassa on kirjoitettu maailmalla tapahtuneista operaatioista ja sellaiseksi epäilystä toiminnasta. Aihealueelta on julkaistu tutkimuksia, jotka ovat saaneet medianäkyvyyttä. Siksi on luonnollista että media on tähän asti ollut pääasiallinen tiedonlähde yrityksille.

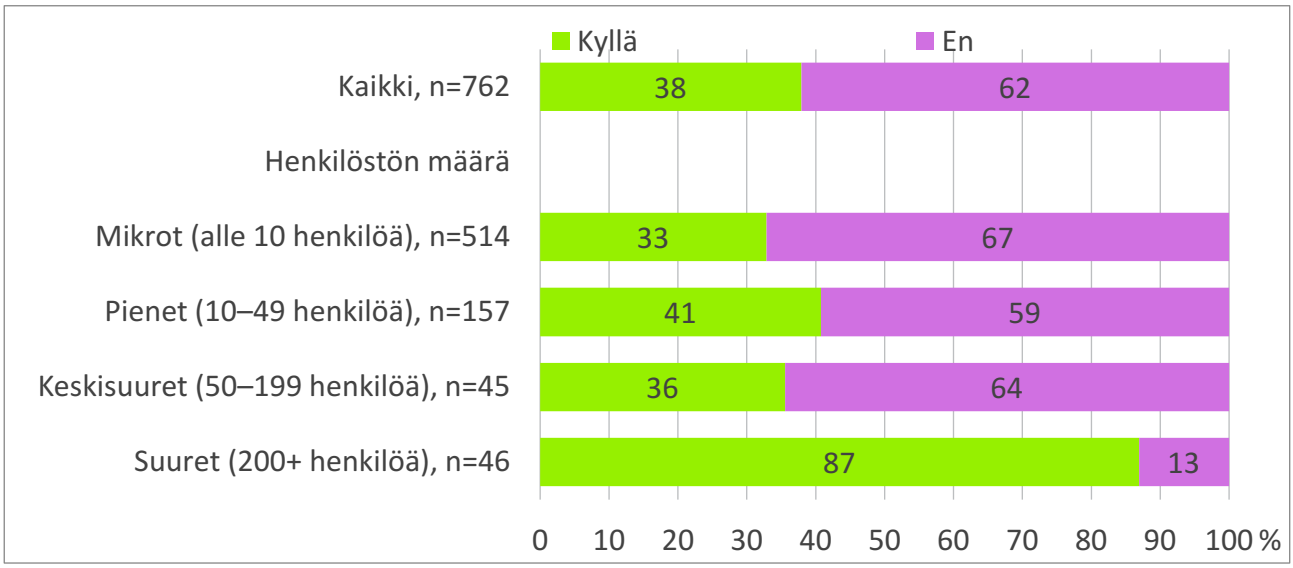
Kaiken kaikkiaan on hyvä että tietoa saadaan useasta eri lähteestä, mutta kuten muunkin tiedon suhteen on tärkeää säilyttää lähdekritiikki. Sen vuoksi on tärkeää että viranomaiset ottavat vahvemman roolin elinkeinoelämälle tarkoitetun hybridivaikuttamiseen liittyvän viestinnän ja materiaalintuottamisen suhteen. Viranomaiset olisivat myös luonnollisia tiedonjakoyhteisöjen alkuunpanijoita ja myöhemmin niiden tiedontuottajia.



Tietävätkö yritykset miltä suomalaiselta viranomaiselta saa tietoa ja apua epäilemäänsä hybridioperaatioon liittyen

Epäillessään yritykseen kohdistuvan hybridioperaatioon liittyvää toimintaa, yrityksistä suurin osa (62 %) ei tiedä miltä viranomaiselta saa tietoa ja apua. Ainoastaan suurissa yrityksissä selkeästi tiedetään mistä tietoa ja apua saa (87 %).

Kahden kolmasosan tietämättömien joukko ei ole yllätys, sillä hybridiuhat ovat suhteellisen uusi aihe ja elinkeinoelämästä sen kohteena ei ole juurikaan puhuttu ennen tätä selvitystä. Hybridiuhkien torjunnasta ja tiedon jakamisesta vastaavat viranomaiset tarvitsevat huomattavasti suuremmat resurssit kuin heillä tällä hetkellä on. Tämä koskee myös elinkeinoelämälle suuntautuvasta viestinnästä ja koulutuksesta vastaavia resursseja.

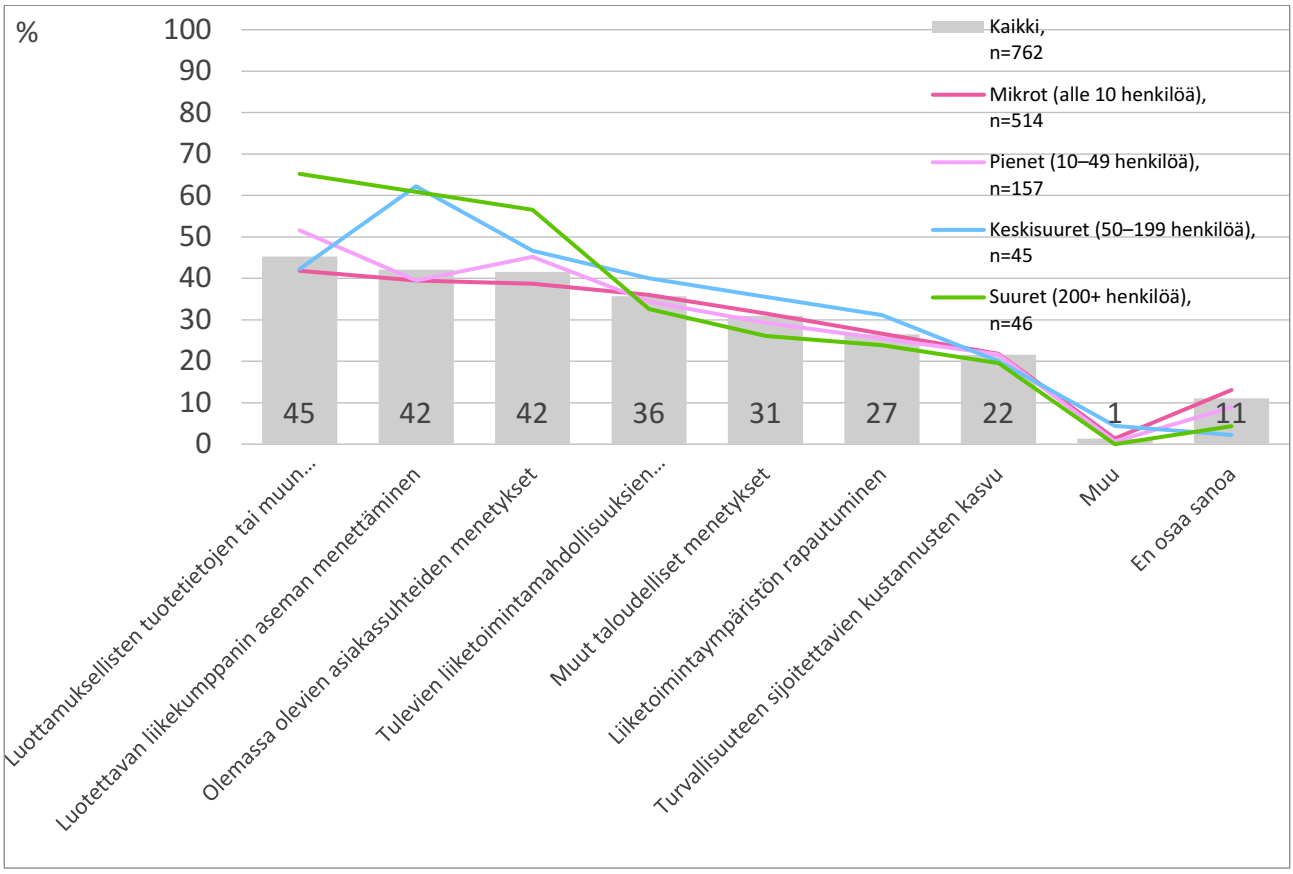


4 RIKOLLISUUDEN JA HYBRIDIVAIKUTTAMISEN SEURAUKSET

Vakavimmat rikollisuuden aiheuttamat seuraukset liike-elämälle

Kolme vakavinta rikollisuuden aiheuttamaa seurausta liike-elämälle ovat luottamuksellisten tuotetietojen tai muun yritystiedon menettäminen (45 %), luotettavan liikekumppanin aseman menettäminen (42 %) ja olevassa olevien asiakassuhteiden menetykset (42 %). Nämä vaihtoehdot korostuvat myös suurien vastaajien keskuudessa.

Yrityksiin kohdistuva rikollisuus ei aiheuta ainoastaan taloudellisia menetyksiä (31 %), vaan sen seurauksena voi tapahtua tiedon, luotettavan toimijan maineen, asiakkaiden ja koko liiketoimintaympäristön rapautuminen. Tämän tulisi ohjata sekä yritysten että viranomaisten yritysturvallisuustyöhön kohdistamia toimenpiteitä.



Vakavimmat seuraukset hybridivaikuttamisesta

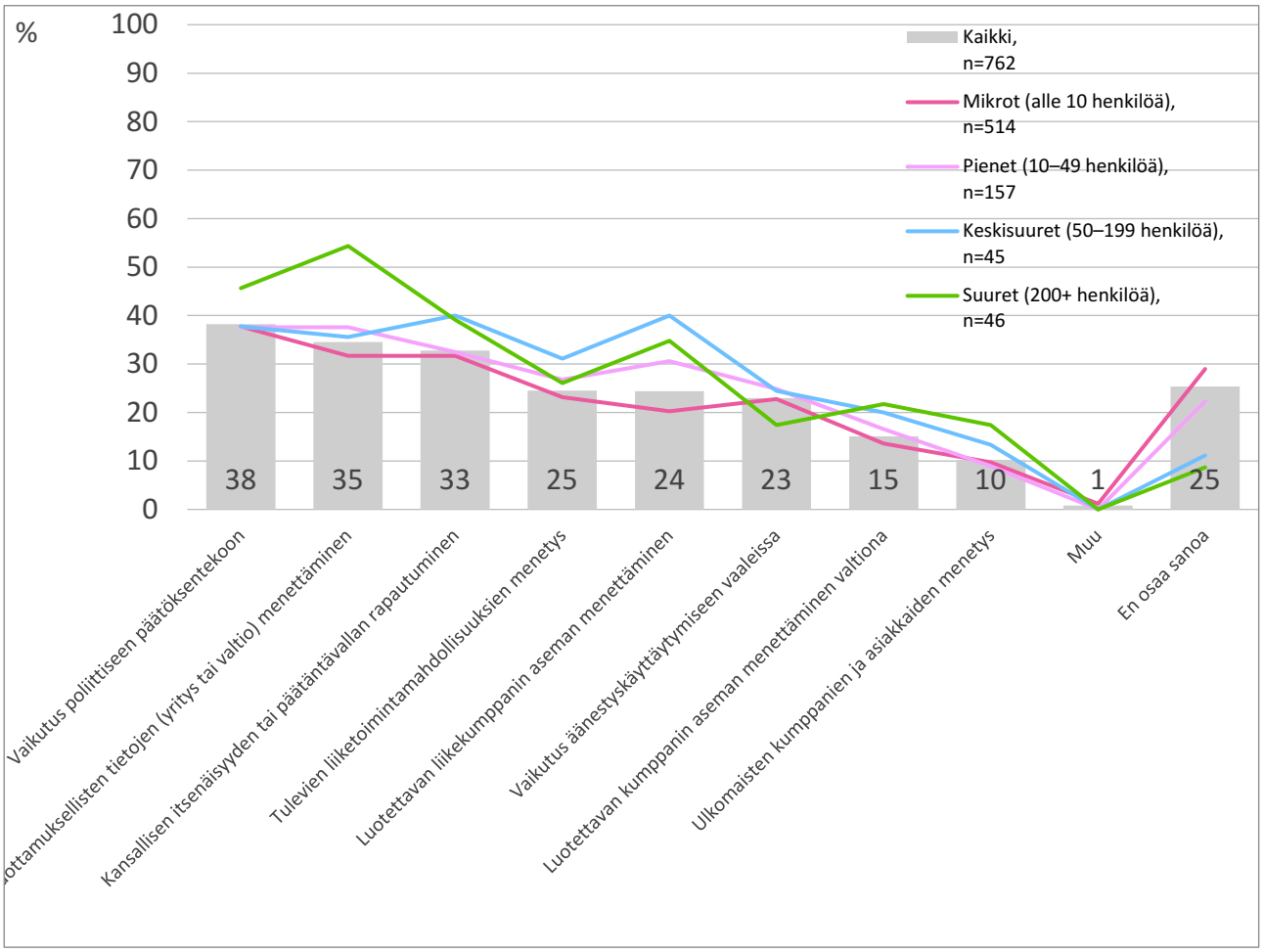
Kolme vakavinta seurasta hybridivaikuttamisesta ovat vaikutus poliittiseen päätöksentekoon (38 %), luottamuksellisten tietojen (yritys tai valtio) menettäminen (35 %) ja kansallisen itsenäisyyden tai päätäntävallan rapauttaminen (33 %).

Pohdittaessa hybridivaikuttamisen keinovalikoimaa poliittiseen päätöksenteon suhteen, voidaan löytää yhtymäkohtia yritysten toimintaan vaikuttamisen suhteen. Poliitikkoon voidaan kohdistaa kiristystä, lahjontaa

tai muuta vaikuttamista aivan kuten yritysjohtajaan. Poliitikkoa voidaan ohjailla lahjoituksin vaalikampanjaan, kun taas yritykselle voidaan tarjota normaalia kannattavampia liiketoimia palkkiona halutunlaisesta toiminnasta. Toisaalta yritystä tai yhdistystä voidaan käyttää välikätenä kollaboratioon suostuvien tai taivuteltujen poliitikkojen vaalikampanjoiden tukemisessa.

Perinteisesti hybridivaikuttamista on pidetty valtioiden välisenä valtioihin kohdistuvana toimintana, mutta aivan yhtä hyvin se voi kohdistua yksittäisen yrityksen toimintaan kohdemaassa, mikäli sen halutaan toimivan tietyllä tavoin. Jälleen keinovalikoima riippuu monista tapauskohtaisista seikoista kuten yrityksen ja sen avainhenkilöiden heikkouksista, halutusta tavoitteesta, yrityksen asemasta kohdemaassa ja kotimaassa. Hybridivaikuttaminen voi toisaalta kohdistua yrityksen kotimaan sijaan sen sijaintimaahan mikäli yrityksellä on siellä sellainen asema tai kontakteja, jotka ovat tarpeen hybridivaikuttajalle.

Toimijoina hybridivaikuttamisessa voivat olla ulkomaisen valtion palveluksessa toimivat henkilöt, ulkomaiset elinkeinoelämän tai järjestöjen edustajat, ulkomaiset tai kotimaiset rikolliset. Huomionarvosta on että ulkomainen ei tarkoita vain vaikuttajavaltion kansalaisia, vaan toimija voi olla kolmannen maan kansalainen, joka toimii vaikuttajavaltion hyväksi. Hybridivaikuttaminen on useamman toiminnan summa ja siinä käytettäville keinoille ei ole rajoituksia tai sääntöjä.

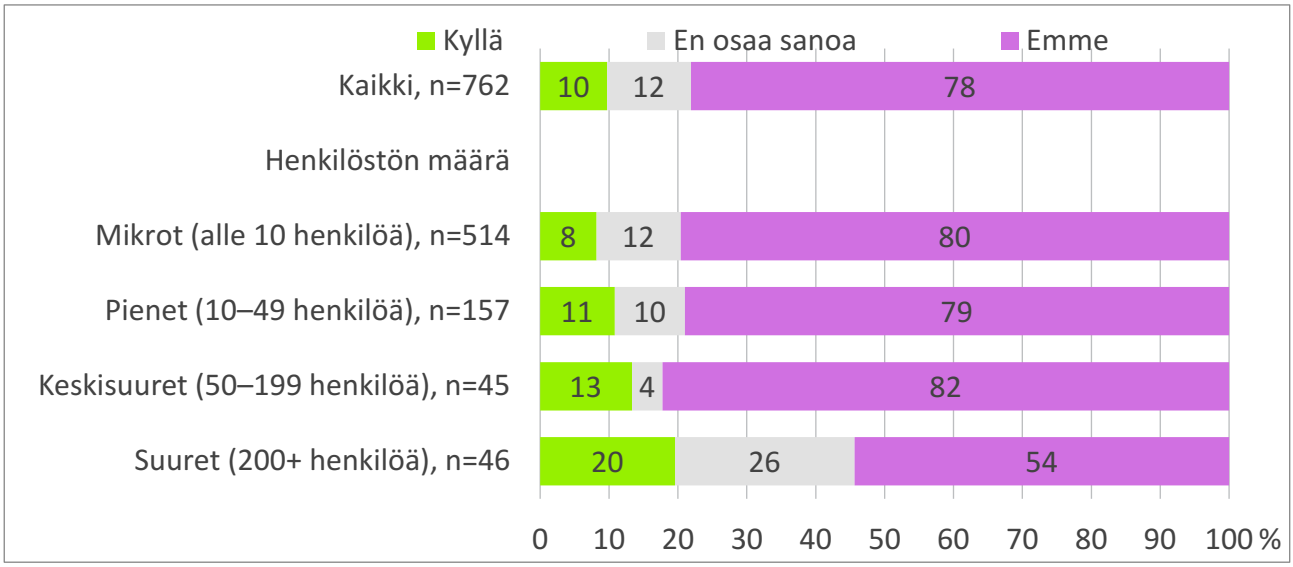


Onko havainnut omaan liiketoimintaan tai jonkun muun liiketoimintaan kohdistunutta toimintaa, joka voisi olla hybridivaikutusoperaatio tai sen osa

Suurin osa yrityksistä (78 %) ei ole havainnut omaan liiketoimintaan ja jonkun muun liiketoimintaan kohdistunutta toimintaa, joka voisi olla hybridivaikutusoperaation tai sen osa (taustalla ulkomainen rikollisjärjestö tai valtio). Kaikista vastaajista kuitenkin joka kymmenes (10 %) on havainnut tällaista toimintaa.

Yrityksen koon kasvaessa havaintoja on tehty enemmän. Suurista yrityksistä jo joka viides (20 %) on havainnut tällaista toimintaa. Suuret yritykset ovat jo asiakaskuntansa, kontaktiensa ja asemansa puolesta luonnollisesti herkemmin kohteina hybridivaikuttamiselle.

Se että joka viides tähän selvitykseen vastanneista suurista yrityksistä on kokenut hybridivaikuttamista, kertoo että toiminta on todennäköisesti laajempaa kuin on ajateltu. Hybridivaikuttamista ei ole joka tapauksessa helppo tunnistaa ja osa siitä jää piiloilmiöksi. Suuriin yrityksiin kohdistuvan hybridivaikuttamisen yleisyyttä on mahdoton arvioida, mutta se voi olla huomattavan suuri. Viranomaisten on hyvä ottaa elinkeinoelämään kohdistuva tai sitä hyväksikäyttävä hybridivaikuttaminen huomioon tulevissa suunnitelmissaan.

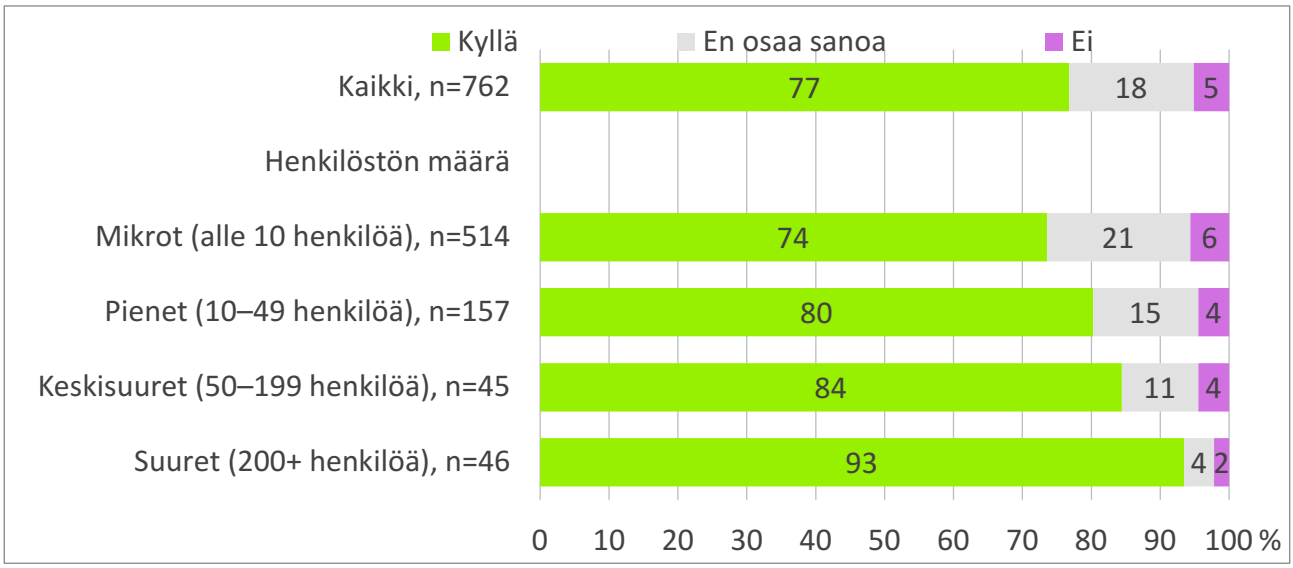


5 ODOTUKSET HYBRIDIVIRANOMAISILTA JA YHTEISTYÖ

Pitääkö suomalaisten viranomaisten tukea liike-elämää esim. tekemällä oppaita hybridiuhista ja järjestämällä koulutuksia ja harjoituksia?

Yrityksistä suurin osa (77 %) on sitä mieltä, että suomalaisten viranomaisten tulisi tukea liike-elämää esim. tekemällä oppaita hybridiuhista ja järjestämällä koulutuksia ja harjoituksia. Suurista vastaajista (93 %) ja keskisuurista vastaajista (84 %) on tätä mieltä. Yritysten tarve tiedolle ja koulutukselle ei jää epäselväksi.

Viranomaisilla on erittäin tärkeä rooli neutraalin ja luotettavan materiaalin tuottamisessa. Elinkeinoelämälle paras ja tehokkain tapa varautua hybridivaikuttamisen varalle on koulutus ja tieto. Uhkana hybridivaikuttaminen on monimuotoinen ja epäsäännönmukainen. Siksi sen varalle ei voi tehdä kovin yksityiskohtaisia ohjeita tai toimintamalleja. Yleinen tietämys ja osaaminen nousevat ratkaisevaan asemaan. Tunnistamisen tai epäilyn synnyttyä on tiedettävä kehen tai mihin otetaan yhteyttä hyvää yhteistyötä ja aktiivisuutta viranomaisten suunnalta.

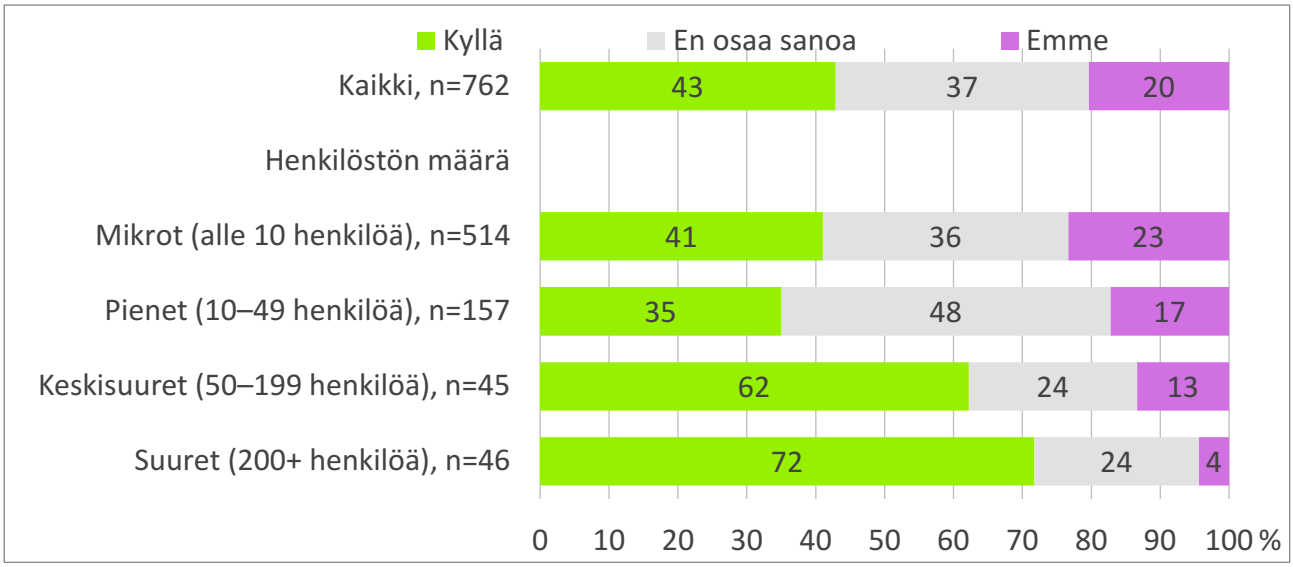


Jakaako yritys tietoa suomalaisille turvallisuusviranomaisille, kun havaitsee yritykseen kohdistuvia epäilyttäviä toimia, joko ulkomailla tai täällä Suomessa?

Yrityksistä hieman alle puolet (43 %) jakavat omatoimisesti tietoa suomalaisille turvallisuusviranomaisille havaitessaan yritykseen kohdistuvia epäilyttäviä toimia ulkomailla tai Suomessa. Suurista yrityksistä suurin osa (72 %) jakaa tietoa.

Tiedonsaaminen epäilyistä on viranomaisten toiminnan kannalta hyödyllistä. Tiedon avulla viranomainen voi ylläpitää tilannekuvaa ja analysoimalla tietoja se voi kyetä luomaan käsityksen siitä, mihin hybridivaikuttaja on pyrkimässä. Tiivis yhteistyö elinkeinoelämän kanssa vahvistaa koko yhteiskunnan varautumista hybridivaikuttamiseen.

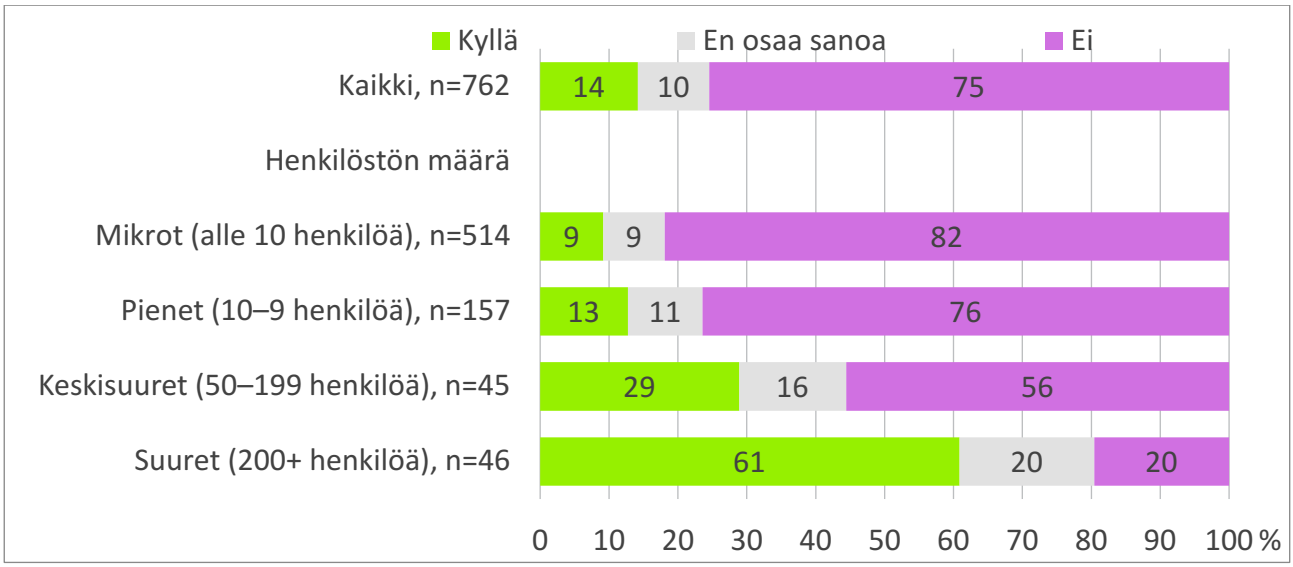
Viranomaisten suuntaan aktiivinen yrityskenttä vaikeuttaa hybridivaikuttajan työtä. Kun hybridivaikuttaja valikoi yritystä kohteekseen, sen on huomioitava se riski siitä että yritys voi tehdä varoituksen toiminnasta ja itse hybridivaikutusoperaatio voi päätyä tarkkailun alle. Tältä osin voidaan puhua eräänlaisesta yhteiskunnan kokonaisvarautumisesta, jossa elinkeinoelämällä on oma roolinsa.



Tekeekö yritys yhteistyötä Suomen viranomaisten kanssa liike-elämään ja yhteiskuntaan vaikuttamiseen tai häiritsemiseen tähtäävän rikollisuuden tai valtioiden laittoman toiminnan tunnistamiseksi ja torjumiseksi

Suurin osa yrityksistä (75 %) ei tee yhteistyötä Suomen viranomaisen kanssa liike-elämään ja yhteiskuntaan vaikuttamiseen tai häiritsemiseen tähtäävän rikollisuuden tai valtioiden laittoman toiminnan tunnistamiseksi tai torjumiseksi. Yrityksen koon kasvaessa yhteistyötä tehdään enemmän. Suurista yrityksistä jo yli puolet (61 %) tekee yhteistyötä Suomen viranomaisen kanssa.

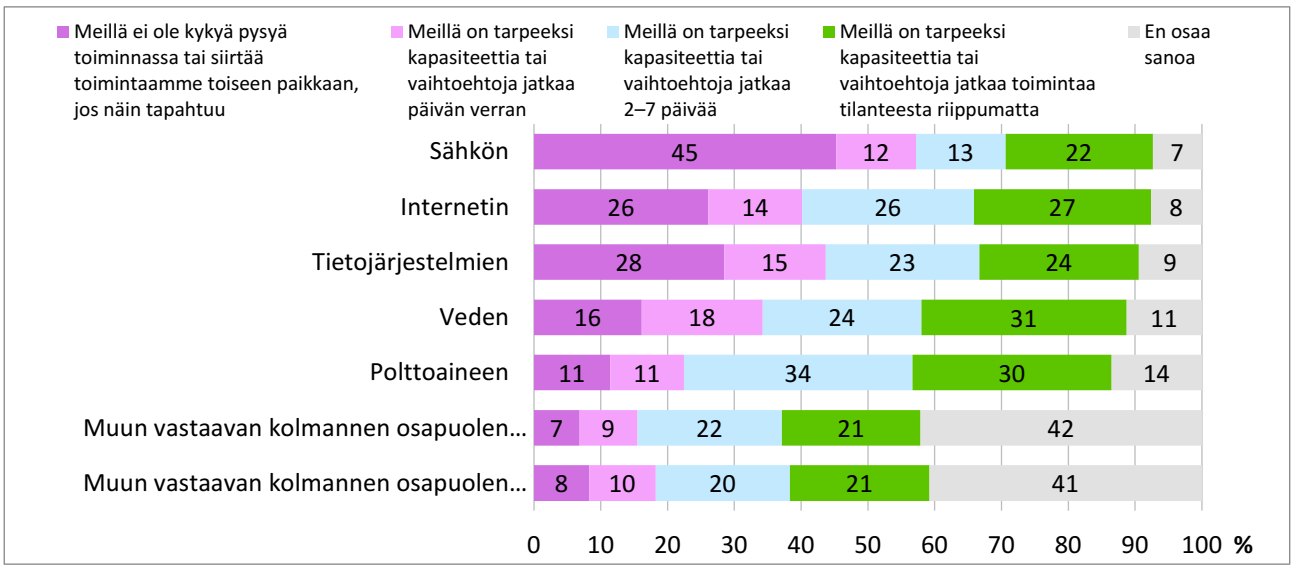
Viranomaisten on hyvä sijoittaa lisää resursseja yhtistyöhön elinkeinoelämän kanssa. Kuten edellisen vastauksen osalta kävi ilmi, yritykset voivat toimia yhteistyössä viranomaisten kanssa alkaen epäilyjen ilmoittamisesta. Verkottuminen elinkeinoelämän kanssa on toimintaa, joka maksaa itsensä takaisin. Valtio vahvistaa varautumisen tehoa ottamalla elinkeinoelämän mukaan hybridivaikuttamisen vastaiseen toimintaan ja jakamalla tietoa sen kanssa.



6 YRITYSTEN KYKY KESTÄÄ ERI RESURSSIEN SAATAVUUDEN HÄIRIÖITÄ

Seuraavien asioiden menetyksen kestäminen

Hybridivaikuttaminen voi johtaa tilanteeseen, jossa normaalitilanteessa käytettävissä olevat resurssit ja järjestelmät eivät olekaan yritysten käytettävissä. Tällainen tilanne edustaa hybridivaikuttamisen toista päätä, jossa ei enää toimita peitellysti. Siksi yrityksellä tulee olla jatkuvuussuunnitelma, jonka avulla se kykenee jatkamaan toimintaansa näissä tilanteissa. Jatkuvuussuunnitelmat alkavat olla tarpeen jo kyberhyökkäysten ja silloin tällöin sääolojen vuoksi. Yrityksen toiminnan jatkuvuutta uhkaavat tilanteet saattavat lähitulevaisuudessa tulla arkipäiväisemmiksi kuin ne mykyään ovat.



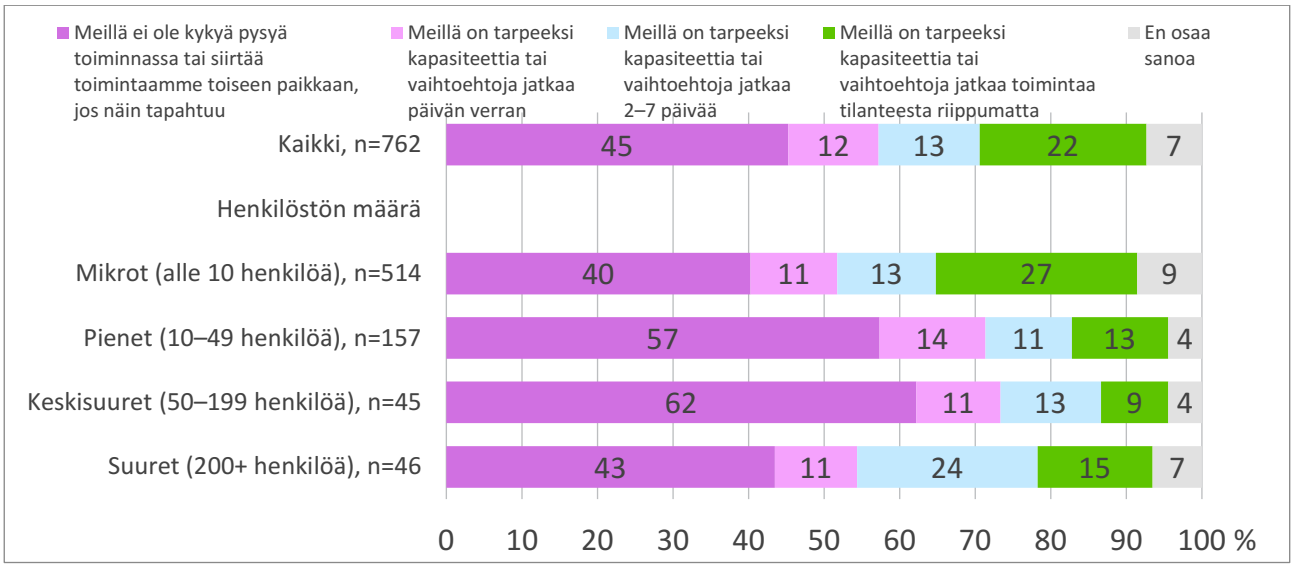
Sähkö

Kriittisin tekijä yrityksen toiminnan kannalta on sähkön menetys. Miltei puolella vastaajayrityksistä (45 %) ei ole kykyä pysyä toiminnassa tai siirtää toimintaa toiseen paikkaan. Ainostaan mikroyrityksistä (alle 10 henkilöä työllistävät) noin joka neljännellä (27 %) on tarpeeksi kapasiteettiä tai vaihtoehtoja jatkaa toimintaa tilanteesta riippumatta. Selityksenä saattaa olla se, että mikroyrityksen on helppo siirtyä etätyöhön, jolloin voi olla helppoa toimia paikasta, jossa sähköä on saatavilla.

Yhden päivän ajan selviää kymmenesosa (12 %) vastaajayrityksistä. Yhden päivän jälkeen siis melkein kaksi kolmasosaa (57 %) yrityksistä ei kykene jatkamaan toimintaansa. Suuristakin yrityksistä yli puolet (54 %) on tässä vaiheessa kyvyttömiä jatkamaan toimintaa.

Toimialoittain sähkönjakelun katkoksia kestettäisiin seuraavasti:

Teollisuus: 61 % / ei lainkaan ja 8 % / yhden päivän
Rakentaminen: 52 % / ei lainkaan ja 15 % / yhden päivän
Kauppa: 43 % / ei lainkaan ja 10 % / yhden päivän
Palvelut: 40 % / ei lainkaan ja 13 % / yhden päivän



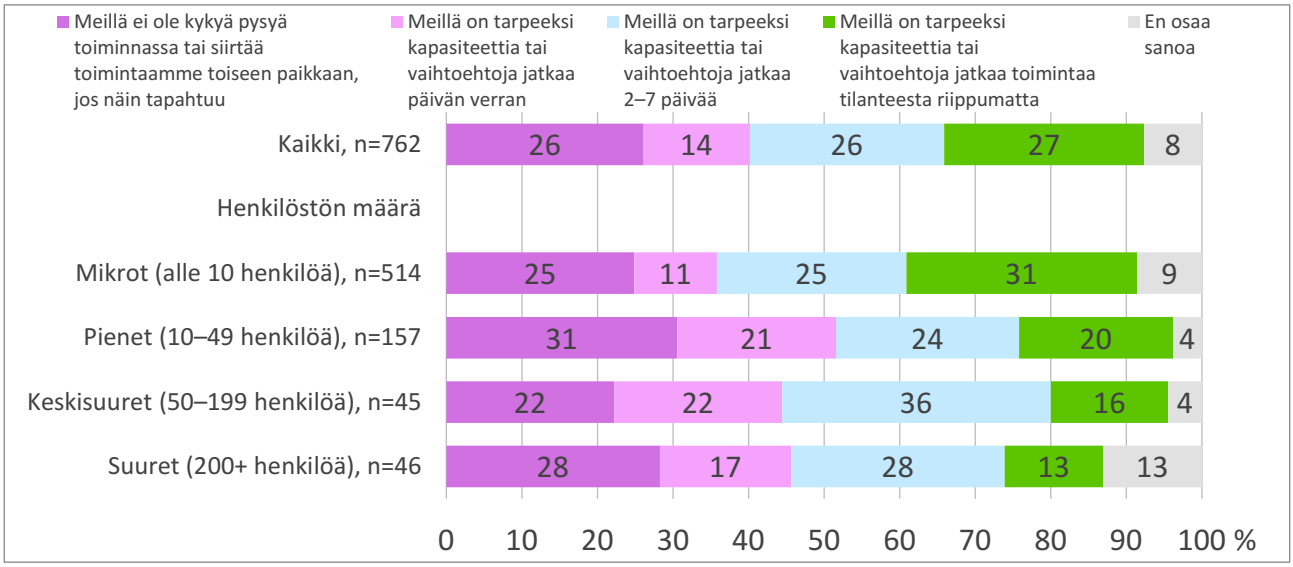
Internet

Internetin menetyksen yrityksistä kestää noin joka neljäs (27 %) ja jotakuinkin sama osuus ei pystyisi olemaan toiminnassa.

Yhden päivän ajan selviää seitsemäsosa (14 %) vastaajayrityksistä. Yhden päivän jälkeen siis neljä kymmenestä (40 %) yrityksestä ei kykene jatkamaan toimintaansa. Suuristakin yrityksistä melkein puolet (45 %) on tässä vaiheessa kyvyttömiä jatkamaan toimintaa.

Toimialoittain internetin katkoksia kestettäisiin seuraavasti:

Teollisuus: 19 % / ei lainkaan ja 18 % / yhden päivän
Rakentaminen: 21 % / ei lainkaan ja 11 % / yhden päivän
Kauppa: 30 % / ei lainkaan ja 22 % / yhden päivän
Palvelut: 28 % / ei lainkaan ja 11 % / yhden päivän



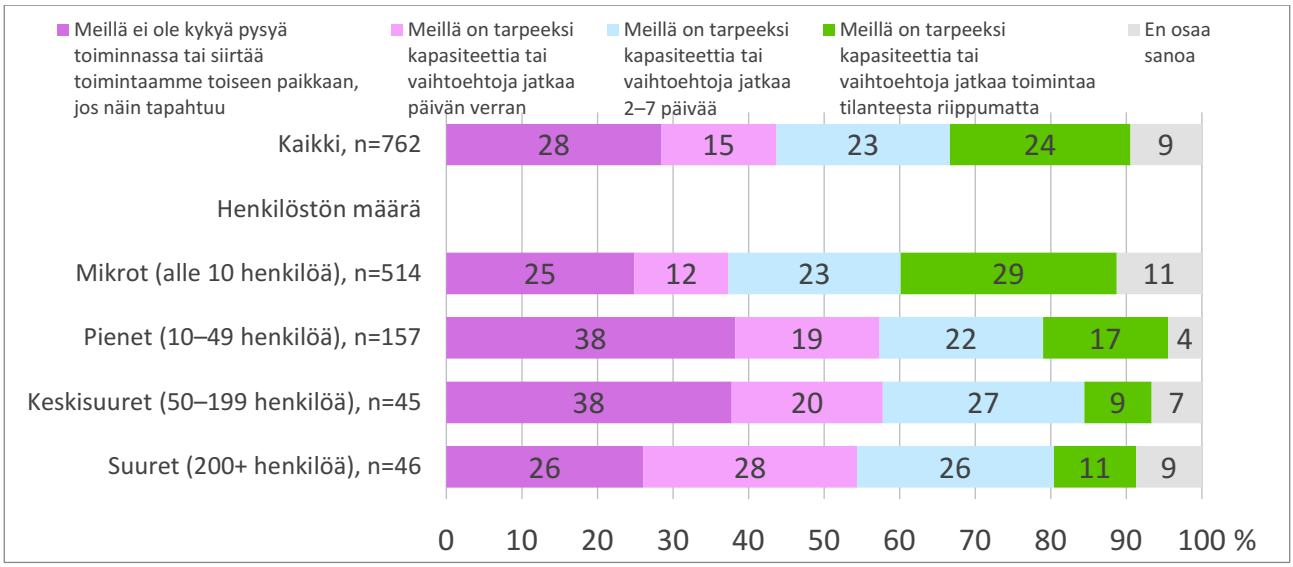
Tietojärjestelmät

Tietojärjestelmien menetyksen kestää noin joka neljäs (24 %). Hieman suurempi osuus, 28 %, ei pysty toimimaan lainkaan ilman niitä.

Yhden päivän ajan selviää noin kuudesosa (15 %) vastaajayrityksistä. Yhden päivän jälkeen siis useampi kuin neljä kymmenestä (43 %) vastaajayrityksestä ei kykene jatkamaan toimintaansa. Suuristakin yrityksistä yli puolet (54 %) on tässä vaiheessa kyvyttömiä jatkamaan toimintaa.

Toimialoittain tietojärjestelmien katkoksia kestettäisiin seuraavasti:

Teollisuus: 27 % / ei lainkaan ja 21 % / yhden päivän
Rakentaminen: 22 % / ei lainkaan ja 11 % / yhden päivän
Kauppa: 30 % / ei lainkaan ja 23 % / yhden päivän
Palvelut: 30 % / ei lainkaan ja 13 % / yhden päivän



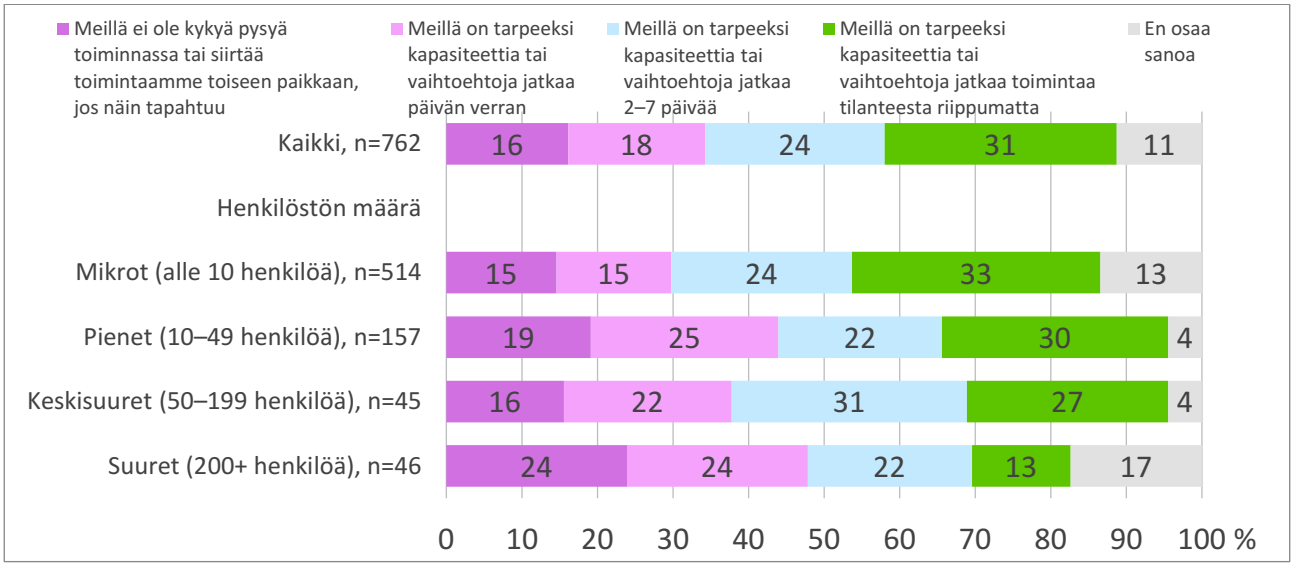
Vesi

Veden menetyksen kestää noin joka kolmas (31 %). Toiminta pysähtyy noin seitsemäsosassa (16 %) yrityksistä.

Yhden päivän ajan selviää viidesosa (18 %) vastaajayrityksistä. Yhden päivän jälkeen siis melkein kolmasosa (34 %) yrityksistä ei kykene jatkamaan toimintaansa. Suuristakin yrityksistä melkein puolet (48 %) on tässä vaiheessa kyvyttömiä jatkamaan toimintaa.

Toimialoittain vesikatkoksia kestettäisiin seuraavasti:

Teollisuus: 22 % / ei lainkaan ja 18 % / yhden päivän
Rakentaminen: 19 % / ei lainkaan ja 20 % / yhden päivän
Kauppa: 13 % / ei lainkaan ja 21 % / yhden päivän
Palvelut: 15 % / ei lainkaan ja 17 % / yhden päivän



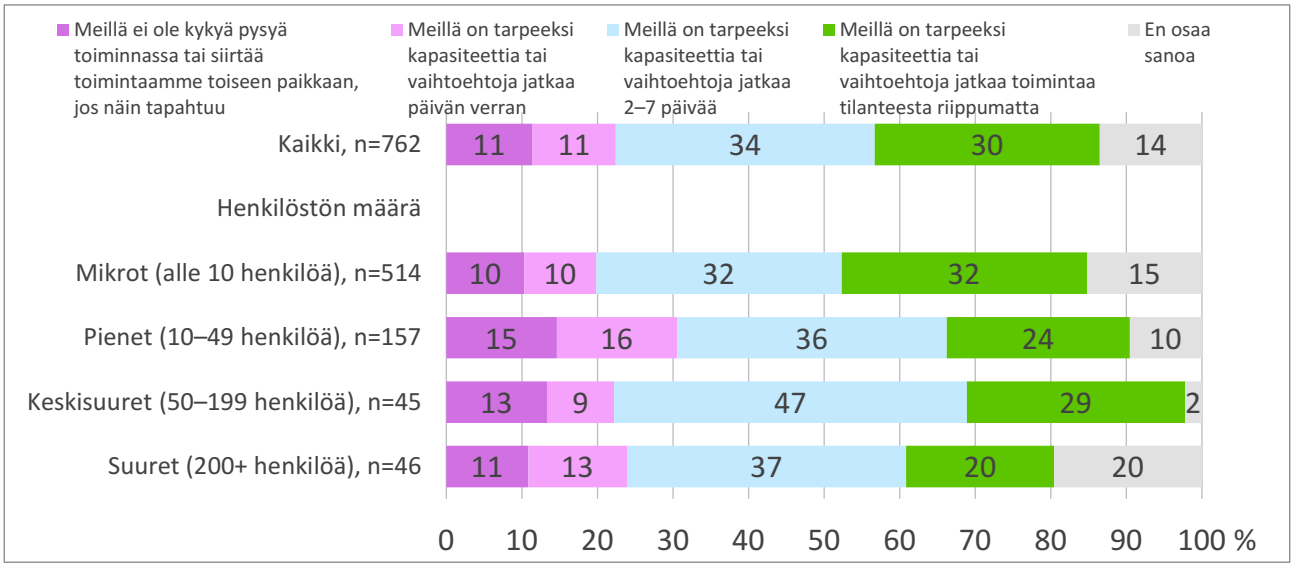
Polttoaine

Polttoaineen menetyksen kestää noin joka kolmas (30 %). Tarpeeksi kapasiteettia tai vaihtoehtoja jatkaa toimintaa 2–7 päivää noin myös noin kolmasosalla (34 %).

Yhden päivän ajan selviää kymmenesosa (11 %) vastaajayrityksistä. Yhden päivän jälkeen siis viidesosa (22 %) yrityksistä ei kykene jatkamaan toimintaansa. Suuristakin yrityksistä melkein puolet (48 %) on tässä vaiheessa kyvyttömiä jatkamaan toimintaa.

Toimialoittain polttoainejakelun katkoksia kestettäisiin seuraavasti:

Teollisuus: 11 % / ei lainkaan ja 16 % / yhden päivän
Rakentaminen: 16 % / ei lainkaan ja 14 % / yhden päivän
Kauppa: 8 % / ei lainkaan ja 8 % / yhden päivän
Palvelut: 11 % / ei lainkaan ja 10 % / yhden päivän

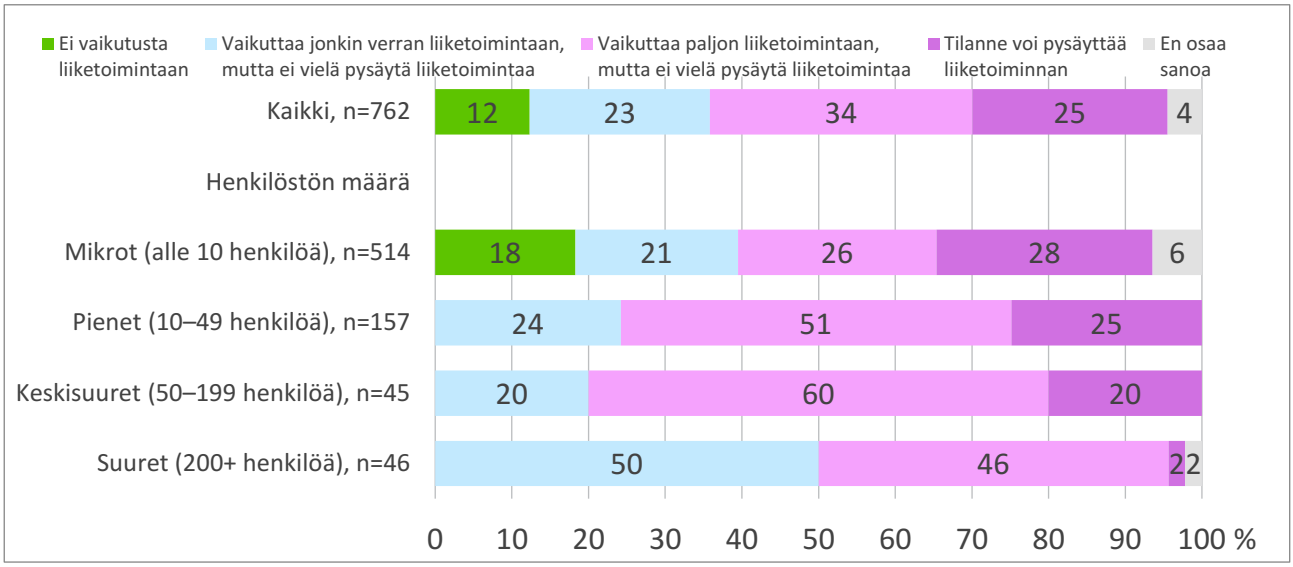


Työvoiman odottamattoman menetyksen (sairastelu) vaikutus yrityksen toimintaan

Käytettävissä olevan työvoiman odottamaton menetys poikkeuksellisen laajan sairastelun vuoksi vaikuttaa paljon yrityksen liiketoimintaan, mutta ei vielä pysäytä sitä noin kolmasosassa yrityksistä (34 %). Neljäsosassa (25 %) yrityksistä tilanne voisi pysäyttää liiketoiminnan. Mitä pienemmästä yrityksestä on kyse, sitä suuremmalla todennäköisyydellä tilanne pysäyttäisi liiketoiminnan.

Toimialoittain työvoiman odottamaton menetys voisi pysäyttää toiminnan kokonaan seuraavasti:

Teollisuus: 23 %
Rakentaminen: 28 %
Kauppa: 18 %
Palvelut: 28 %



7 JOHTOPÄÄTÖKSET

Elinkeinoelämään kohdistuva hybridivaikuttaminen on jo arkipäivää?

Joka kymmenes vastaajayritys kertoo siihen kohdistuneen hybridivaikuttamista. Yleisintä hybridivaikuttaminen on suurien yritysten keskuudessa, niistä joka viides on ollut sen kohteena. Yrityksiin kohdistuu huomattavissa määrin hybridivaikuttamiseksi luettavaa toimintaa. Tämä korostaa tarvetta elinkeinoelämän ja viranomaisten yhteistyön laajentamiseksi sekä syventämiseksi ja sen riittäväksi resursoimiseksi.

Suuret yritykset hybridivaikuttajien kohteena

Neljä kymmenestä (41 %) suuresta yrityksestä pitää vähintään melko todennäköisenä, että ne voivat päätyä rikollisten tai ulkomaisten toimijoiden vaikuttamisen kohteeksi.

Tiedustelupalvelut ja rikolliset pääsevät verkon kautta ja tietojenkalastelulla yrityksen tietoihin - suurilla yrityksillä huoli sisäisestä uhasta

Yleisin tapa (51 %) yritysten mielestä on usb-laitteiden tai muiden sähköisten välineiden kautta tapahtuva tunkeutuminen. Tietojen kalastelu (42 %) on toiseksi yleisin tapa. Joka neljäs (25 %) suuri yritys on huolissaan hybridivaikuttajan värväämistä työntekijöistään. Tietoihin käsiksi pääsy altistaa yritykset myös tietojen manipuloinnille ja toiminnan sabotoinnille. Hybridivaikuttajilla on monia tapoja päästä yritysten tietoihin ja etumatkaa, joka yritysten tulisi kuroa umpeen.

Elinkeinoelämä huolissaan poliittisesta päätöksenteosta ja päätäntävallan rapautumisesta

Vaikutusta poliittiseen päätöksentekoon (38 %) ja kansallisen itsenäisyyden tai päätäntävallan menetystä (33 %) pidetään hybridivaikuttamisen vakavimpien seurausten joukossa. Yritykset tunnistavat hyvin hybridivaikuttamisen ja kansallisen turvallisuuden välisen yhteyden.

Avoimuus ja sinisilmäisyys avaavat ovet hybridivaikuttajalle

Miltei kaksi kolmasosaa (59 %) vastaajayrityksistä pitävät suomalaisuuteen perinteisesti kuuluvaa liiallista avoimuutta ja sinisilmäisyyttä suurimpana heikkoutena hybridivaikuttamisen suhteen. Suomi on pieni ja verkottunut yhteiskunta ja siksi tätä haavoittuvuutta voidaan pitää merkittävänä. Tiedonjakaminen ja kouluttaminen ovat tehokas tapa korjata tämä.

Huomattava määrää yrityksistä jakaa tietoa viranomaisille ja haluaa tukea viranomaisilta

Elinkeinoelämä on valmis jakamaan ja jakaa tietoa viranomaisille. Neljä kymmenestä (43 %) vastaajayrityksestä jakaa tietoa suomalaisille turvallisuusviranomaisille havaitessaan ulkomailla tai Suomessa yrityksseensä kohdistuvia epäilyttäviä toimia. Suurista yrityksistä yli kaksi kolmasosaa (72 %) tekee niin. Valtaosa vastaajayrityksistä (77 %) kaipaa viranomaisten tekemiä oppaita ja järjestämää koulutusta tukena hybridiuhkiin varautumisessa.

Elinkeinoelämä haavoittuvaista resurssien saatavuuden katkoille

Elinkeinoelämän toiminnan jatkuvuus on hyvin haavoittuvaista resurssien saatavuuden katkoille. Yhden päivän katko sähkönsaannissa pysäyttää melkein kaksi kolmasosaa yrityksistä (57 %), päivän katko internetin saatavuudessa pysäyttää yli kolmasosan (38 %) ja tietojärjestelmien käytön estyminen päiväksi pysäyttää neljä kymmenestä yrityksestä (43 %).

LÄHTEITÄ JA LISÄTIETOA

Cederberg, Aapo ja Eronen, Pasi (2015) How Are Societies Defended against Hybrid Threats. Geneva Centre for Security Policy. https://www.gcsp.ch/News-Knowledge/Publications/How-are-Societies-Defended-against-Hybrid-Threats

Elinkeinoelämän keskusliitto (2018) Kybervakoilu – mitä jokaisen yrityksen tulisi tietää. https://ek.fi/ajankohtaista/2018/06/04/kybervakoilu-%E2%88%92-mita-jokaisen-yrityksen-tulisi-tietaa/

Helsingin seudun kauppakamari (2010) Innovaatioiden ja tiedon suojaaminen.

Helsingin seudun kauppakamari (2008). Heljaste, Korkiamäki, Laukkala, Mustonen, Peltonen ja Vesterinen. Yrityksen turvallisuusopas.

Helsingin seudun kauppakamari (2015 ja 2016). Yrityksiin kohdistuvat kyberuhat -selvitykset.

Helsingin seudun kauppakamari (2011). Turvaa logistiikka. Panu Vesterinen (toim).

Kansallinen yritysturvallisuutta edistävä yhteistyöryhmä (2006, 2012) Elinkeinoelämän ja viranomaisten yhteinen yritysturvallisuusstrategia. Http://www.intermin.fi ja Http://www.keskuskauppakamari.fi.

Keskuskauppakamari ja Helsingin seudun kauppakamari (2017, 2012, 2008 ja 2005) Yritysten rikosturvallisuus –riskit ja niiden hallinta -selvitykset.

Keskusrikospoliisi (2011) Korruptiorikollisuuteen 2014-2015 .

Keskusrikospoliisi. Yrityksiin kohdistuvan rikollisuuden ja niitä hyödyntävän rikollisuuden tilannekuvat ja teematilannekuvat.

Keskusrikospoliisin sivuilla on elinkeinoelämän ja viranomaisten yhteistyönä laadittu rikosten torjunnan toimintamalli ja tarkistuslista riskien kartoituksen avuksi. Http://www.poliisi.fi/krp.

MCDC (2017) MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare. https://www.gov.uk/government/publications/countering-hybrid-warfare-project-understanding-hybrid-warfare

Nikkari, Timo. Tampereen yliopisto, tietojen käsittelytieteiden laitos (2007). Sisäinen tietoturva. Tietovuodon vaikutukset PK-yrityksen toimintaan ja toimintatapojen vaikutus sisäiseen tietoturvallisuuteen. Pro gradu-tutkielma.

Sisäministeriö (2017). Tietoverkkorikollisuuden torjuntaa koskeva selvitys. Sisäministeriön julkaisu 14 / 2017. Helsinki 2017.

Suojelupoliisi: Insider-teot: Työntekijän tekemä tietovarkaus tai sabotaasi uhka yrityksen toiminnalle. 2018

Suojelupoliisi (2009) Yrityksiin kohdistunut laiton tiedonhankinta Suomessa vuosina 2007 – 2008.

Suojelupoliisi (2018) Suojelupoliisin vuosikirja 2017. http://www.supo.fi/julkaisut/esitteet

The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) (2018) Countering Hybrid Threats. https://www.hybridcoe.fi/hybrid-threats/

Turvallisuuskomitea (2017) Turvallinen Suomi 2018 – Tietoja Suomen kokonaisturvallisuudesta. https://turvallisuuskomitea.fi/turvallinen-suomi-2018-tietoa-suomen-kokonaisturvallisuudesta/

Turvallisuuskomitea (2017) Yhteiskunnan turvallisuusstrategia. https://turvallisuuskomitea.fi/yhteiskunnan-turvallisuusstrategia-2017/

LIIKE-ELÄMÄ JA HYBRIDIVAIKUTTAMINEN 2018 KYSYMYKSET

T1 Aloitamme tutkimuksen kysymällä ensin muutamia taustatietoja. Asemanne yrityksessä? SINGLE

1. Toimitusjohtaja
2. Yrittäjä/omistaja
3. Muu johtaja
4. Päällikkötaso
5. Asiantuntija
6. Jokin muu, mikä?_____

T2 Yrityksenne liikevaihto vuonna 2017? SINGLE

1. Alle 0,2 milj. euroa
2. 0,2–1 milj. euroa
3. 1,1–2 milj. euroa
4. 2,1–10 milj. euroa
5. 10,1–20 milj. euroa
6. 20,1–100 milj. euroa
7. Yli 100 milj. euroa

T3 Yrityksenne toimipaikkojen määrä? NUMERIC

kpl: _____

T4 Henkilöstön määrä? SINGLE

1. 1–4
2. 5–9
3. 10–19
4. 20–49
5. 50–99
6. 100–199
7. 200–499
8. 500+

T5 Millaista kaupankäyntiä yrityksenne harjoittaa? Voitte valita useita. MULTI

1. Business-to-business (b2b) eli yritysten välinen kauppa
2. Business-to-consumer (b2c) eli kuluttajille suunnattu kauppa
3. Business-to-government (b2g) eli julkishallinnolle suunnattu kauppa

T6 Yrityksellänne on liiketoimintaa…? Voitte valita useita. MULTI

1. Suomessa
2. muissa EU-maissa

3. EU:n ulkopuolella

T7 Yrityksenne päätoimiala? SINGLE

1. Teollisuus
2. Rakentaminen
3. Kauppa
4. Palvelut

1. Mitä seuraavista riskeistä olette arvioineet yrityksenne kannalta? Valitse korkeintaan neljä merkittävintä
a) Sosiaalisessa mediassa tai muissa sähköisissä lähteissä levitetty väärä tieto
b) Luottamuksellisten liiketoimintatietojen varkaus
c) Immateriaaliomaisuuden varkaus
d) Palvelunestohyökkäys
e) Yrityksen tietojärjestelmien väärinkäyttö kryptovaluutan louhimiseen
f) Tärkeän tiedon tai ohjelmiston koodin muuttaminen tarkoituksena aiheuttaa vahinkoa, kuten teollisen prosessin häiriintyminen manipuloidun ohjaustiedon avulla koneita rikkomalla
g) Kidnappaus, kiristyksen tai muunlaisen värväämisen kohdistaminen johtajiin tai avainhenkilöihin
h) Soluttautuminen henkilöstöönne tai työntekijänne värvääminen
i) Energian, veden tai muiden keskeisten resurssien saatavuuden häiriöt liiketoiminnalle
j) Emme ole arvioineet mitään riskejä
k) En osaa sanoa

2. Miten riskiarvionne ohjaa yrityksenne toimintaa?
a) budjetoimme lisää rahaa toimintaan
b) rekrytoimme henkilöresursseja yrityksen turvallisuustoimintoihin
c) lisäämme koulutusta
d) hakeudumme yhteistyöhön viranomaisten kanssa
e) etsimme lisää tietoa varautumisesta
f) muutoin, miten_____
g) Riskiarviointimme ei ohjaa yrityksemme toimintaa
h) En osaa sanoa

3. Mitkä ovat kolme todennäköisintä syytä, joiden vuoksi yritykseenne kohdistuisi toimintaa, jonka lopullisena tarkoituksena olisi vaikuttaa suomalaiseen tai muun maan väestöön tai hallintoon?
a) asiakaskuntaan kuuluvat viranomaiset
b) asiakaskuntaan kuuluvat poliittiset asiakkaat
c) yrityksen johdon henkilökohtaiset yhteydet poliitikkoihin
d) aktiiviset työntekijät, jotka toimivat sosiaalisessa mediassa ja joilla on paljon seuraajia
e) johdon ja avainhenkilöiden henkilökohtaiset yhteydet sekä johtaviin että toteuttavan tason viranomaisiin
f) aktiivinen jäsenyys ja toiminta vaikutusvaltaisissa liike-elämän järjestöissä, kuten kauppakamarijärjestössä
g) yrityksen keskeinen ja vakiintunut asema suomalaisessa yhteiskunnassa
h) asiakassuhteet kansallisten turvallisuuteen liittyvien viranomaisten, kuten puolustusvoimien, poliisin tai rajavartiolaitoksen kanssa

i) asiakassuhteet muiden maiden kansallisten turvallisuuteen liittyvien viranomaisten, kuten puolustusvoimien, poliisin tai rajavartiolaitoksen kanssa
j) yrityksen heikko lahjonnan vastainen toiminta ja ohjelma
k) suuri kansallinen asiakaskunta
l) suuri kansainvälinen asiakaskunta
m) Joku muu syy, mikä_____
n) En osaa sanoa

4. Kuinka todennäköistä on, että rikolliset tai ulkomaiset valtion toimijat voisivat kohdistaa yritykseenne toimintaa, jonka lopullisena tarkoituksena on vaikuttaa Suomen sisäiseen vakauteen, talouteen, ulko- ja turvallisuuspolitiikkaan tai hallituksen toimintaan?
a) Erittäin todennäköistä
b) Melko todennäköistä
c) Ei lainkaan todennäköistä
d) En osaa sanoa

5. Miten uskotte rikollisten tai ulkomaisten tiedustelupalvelujen pääsevän kohteekseen valitsemansa yrityksen tietoihin? Valitse kaksi todennäköisintä vaihtoehtoa
a) Phishing -tietojenkalasteluoperaation kautta
b) USB-laitteiden tai muiden sähköisten välineiden levittämien haittaohjelmien avulla
c) Käyttämällä palveluksessaan olevia henkilöitä, jotka ovat yrityksenne henkilökuntaa
d) Käyttämällä lahjottuja tai kiristettyjä johtajia tai avainhenkilöitä, jotka tarjoavat pääsyn
e) Käyttämällä lahjottuja tai kiristettyjä henkilökunnan tai palveluntarjoajan edustajia, jotka tarjoavat pääsyn
f) Käyttämällä lahjottuja tai kiristettyjä viranomaisia tiedon saamiseksi heidän toimivaltuuksiensa avulla
g) Muuten, miten_____
h) En osaa sanoa

6. Oletteko kehittäneet ohjeet tai toimintamalleja edellä mainittujen riskien varalle?
a) Kyllä, ohjeet
b) Kyllä, toimintamallit
c) Kyllä, sekä ohjeet että toimintamallit
d) Emme ole kehittäneet ohjeita tai toimintamalleja
e) En osaa sanoa

6b. Millaisia ohjeita ja/tai toimintamalleja olette kehittäneet? KYSYTÄÄN, JOS 6 VALNNUT a, b tai c (AVOIN)

7. Mitkä ovat kolme merkittävintä suomalaisten yritysten heikkoutta, kun puhutaan ulkomaisten toimijoiden (rikollisten tai valtioiden) pyrkimyksistä vaikuttaa liiketoimintaan?
a) Kyky tunnistaa liiketoiminnaksi peitelty vaikuttamisyritys tai hanke yrityksen hyödyntämiseksi tarkoituksena vaikuttaa varsinaiseen kohteeseen
b) Tieto siitä mitä tehdä, kun epäilys herää
c) Tieto siitä, mihin viranomaiseen ottaa yhteyttä
Liika avoimuus ja sinisilmäisyys
d) Yrityksen rikosturvallisuuden puute tai heikkous
e) Työntekijöiden tietoisuuden ja valppauden puute

f) Johdon tietoisuuden ja valppauden puute
g) Johdon ymmärtämättömyys mahdollisista seurauksista
h) Jatkuvuussuunnitelman puute ja testaamattomuus (poikkeustilanteen kestokyky)
i) Liiketoiminnan riippuvuus kansainvälisestä palveluista tai osaamisesta (pilvipalvelut, asiantuntijat…)
j) Muu, mikä_____
k) En osaa sanoa

8. Miten rajoitatte pääsyn tärkeisiin ja/tai luottamuksellisiin yritystietoihin?
a) Tallentamalla ne siten, ettei niihin päästä käsiksi muualta, kuten tietojärjestelmästä tai internetistä käsin
b) Ylläpitämällä pääsynvalvontamenetelmiä, joilla rajataan käyttäjien pääsyn tietoihin ja palveluihin
c) Seuraamalla kriittisiksi tunnistettujen tietojen koskemattomuutta
d) Ulkoistamalla arkaluonteisten tietojen tallennus ja säilytys
e) 24/7 pääsynvalvonta pilveen ja sisäiseen verkkoon
f) Ylläpitämällä lokia kaikista pääsy-yrityksistä järjestelmiin (sekä onnistuneet että epäonnistuneet)
g) Kieltämällä luottamuksellisten tietojen tulostaminen
h) Muulla tavoin, miten _____
i) Meillä ei ole keinoja rajoittaa pääsyä/Emme rajoita
j) En osaa sanoa

9. Miten teette ulkomaisten liikekumppanien (yritysten ja/tai yksityishenkilöiden) ja heidän yhteyksiensä taustatutkimukset?
a) Emme tee niitä
b) Selvitämme itse
c) Kyselemme alan muilta toimijoilta
d) Käytämme erikoistuneita palveluntarjoajia
e) Käytämme turvallisuusviranomaisia
f) Teemme selvitykset muulla tavoin
g) En osaa sanoa

10. Mitkä ovat kolme vakavinta rikollisuuden aiheuttamaa seurausta liike-elämälle?
a) Tulevien liiketoimintamahdollisuuksien menettäminen
b) Olemassa olevien asiakassuhteiden menetykset
c) Luottamuksellisten tuotetietojen tai muun yritystiedon menettäminen
d) Turvallisuuteen sijoitettavien kustannusten kasvu
e) Luotettavan liikekumppanin aseman menettäminen
f) Muut taloudelliset menetykset
g) Liiketoimintaympäristön rapautuminen
h) Jokin muu, mikä_____
i) En osaa sanoa

11. Mitkä ovat kolme vakavinta seurausta hybridivaikuttamisesta?
a) Luottamuksellisten tietojen (yritys tai valtio) menettäminen
b) Vaikutus poliittiseen päätöksentekoon
c) Vaikutus äänestyskäyttäytymiseen vaaleissa
d) Kansallisen itsenäisyyden tai päätäntävallan rapautuminen

e) Tulevien liiketoimintamahdollisuuksien menetys
f) Luotettavan kumppanin aseman menettäminen valtiona
g) Ulkomaisten kumppanien ja asiakkaiden menetys
h) Luotettavan liikekumppanin aseman menettäminen
i) Jokin muu, mikä_____
j) En osaa sanoa

12. Mistä saatte tietoja hybridioperaatioihin liittyvästä toiminnasta tai toimijoista?
a) Mediasta
b) Suomalaisilta viranomaisilta
c) Oman alan tiedonvaihtoryhmistä
d) Ulkomaisista lähteistä
e) Seminaareista
f) Muualta, mistä_____
g) Emme mistään
h) En osaa sanoa

13. Tiedättekö miltä suomalaiselta viranomaiselta saatte tietoa ja apua, jos epäilette yritykseenne kohdistuvan hybridioperaatioon liittyvää toimintaa?
a) Kyllä
b) En

14. Pitääkö suomalaisten viranomaisten tukea liike-elämää esim. tekemällä oppaita hybridiuhista ja järjestämällä koulutuksia ja harjoituksia?
a) Kyllä
b) Ei

15. Jaatteko omatoimisesti tietoa suomalaisille turvallisuusviranomaisille, kun havaitsette yritykseenne kohdistuvia epäilyttäviä toimia, joko ulkomailla tai täällä Suomessa?
a) Kyllä
b) Emme
c) En osaa sanoa

16. Oletteko havainneet omaan liiketoimintaanne tai jonkun muun liiketoimintaan kohdistunutta toimintaa, joka voisi olla hybridivaikutusoperaatio tai sen osa (taustalla ulkomainen rikollisjärjestö tai valtio)?
a) Kyllä
b) Emme
c) En osaa sanoa

16b. KYSYTÄÄN JOS VASTANNUT 1 KYSYMYKSESSÄ 16, AVOIN Millaista toimintaa olette havainneet?

17. Tekeekö yrityksenne yhteistyötä Suomen viranomaisten kanssa liike-elämään ja yhteiskuntaan vaikuttamiseen tai häiritsemiseen tähtäävän rikollisuuden tai valtioiden laittoman toiminnan tunnistamiseksi ja torjumiseksi?
a) Kyllä
b) Ei

18. Miten hyvin yrityksenne kestää seuraavien asioiden menetyksen
a) sähkön
b) internetin
c) tietojärjestelmien
d) veden
e) polttoaineen
f) muun vastaavan kolmannen osapuolen tarjoaman resurssin
g) muun vastaavan kolmannen osapuolen tarjoaman palvelun

VASTAUSASTEIKKO
a) Meillä ei ole kykyä pysyä toiminnassa tai siirtää toimintaamme toiseen paikkaan, jos näin tapahtuu
b) Meillä on tarpeeksi kapasiteettia tai vaihtoehtoja jatkaa päivän verran
c) Meillä on tarpeeksi kapasiteettia tai vaihtoehtoja jatkaa 2–7 päivää
d) Meillä on tarpeeksi kapasiteettia tai vaihtoehtoja jatkaa toimintaa tilanteesta riippumatta

19. Miten käytettävissä olevan työvoiman odottamaton menetys poikkeuksellisen laajan sairastelun vuoksi vaikuttaisi yrityksenne toimintaan?
a) Ei vaikutusta liiketoimintaan
b) Vaikuttaa jonkin verran liiketoimintaan, mutta ei vielä pysäytä liiketoimintaa
c) Vaikuttaa paljon liiketoimintaan, mutta ei vielä pysäytä liiketoimintaa
d) Tilanne voi pysäyttää liiketoiminnan
e) En osaa sanoa

KAUPPAKAMARI

Kalevankatu 12, 00100 Helsinki
etunimi.sukunimi@chamber.fi
www.helsinki.chamber.fi