KAUPPAKAMARI

Yritysten

RIKOSTURVALLISUUS 2020

Joulukuu 2020

Helsingin seudun kauppakamari
Kalevankatu 12
00100 HELSINKI

ESIPUHE

Yritysturvallisuuteen liittyvien selvitysten tavoitteena on saada tietoa erikokoisten ja eri toimialalla toimivien yritysten turvallisuuden tilanteesta. Selvitykset auttavat sekä yritysturvallisuuden nykytilan kartoittamisessa että yritysten riskienhallinnan tukemisessa.

Selvityksen tulokset antavat yritysjohtajille eväitä toimivaan riskienhallintaan. Selvityksen avulla voi vertailla, millaisia uhkia yrityksiin kohdistuu, mitä riskienhallinnan keinoja eri toimialoilla toimivat yritykset käyttävät ja kehittää tämän tiedon avulla oman liiketoiminnan turvallisuutta.

Joulukuussa 2020

Helsingin seudun kauppakamari

Panu Vesterinen
selvityksen kirjoittaja

SISÄLLYS

1 JOHDANTO

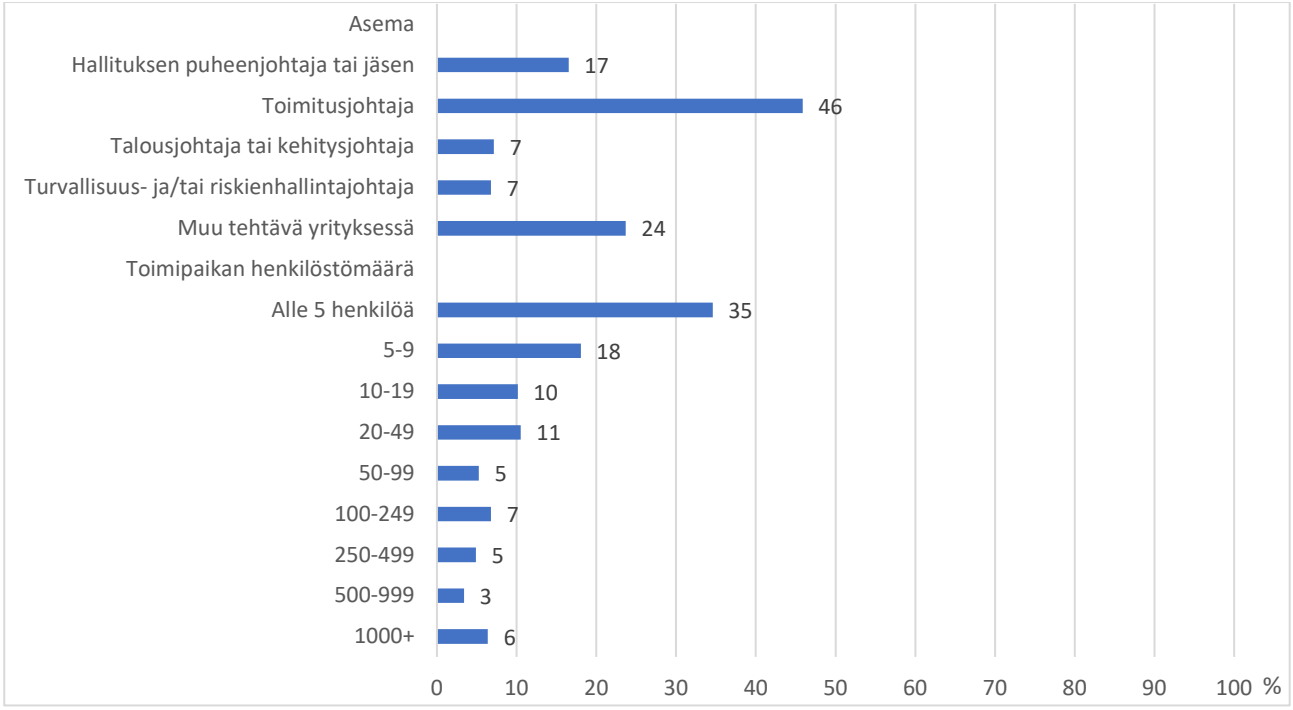
Tämän selvityksen tavoitteena on tutkia, mikä on yritysturvallisuuden tila on, millaisia uhkia eri toimialoilla toimiviin yrityksiin kohdistuu ja miten yritykset ovat varautuneita niihin. Selvitys kuvaa myös sellaisia yrityksiin kohdistuvia rikoksia ja väärinkäytöksiä, jotka usein jäävät tilastoimattomaksi piilorikollisuudeksi.

Tutkimustuloksista yritykset saavat käsityksen omaa toimialaa uhkaavista riskeistä ja muiden yritysten käyttämistä riskienhallintakeinoista. Selvitys on osa Helsingin seudun kauppakamarin edunvalvontaa. Kauppakamarilla on yli 7000 jäsentä. Kauppakamarit edistävät eri tavoin yritysten toimintaedellytyksiä.

Tutkimuksen toteuttaminen ja vastaajien taustatiedot

Yritysten rikosturvallisuus 2020 selvitys kattaa kaikki toimialat ja yrityskoot. Selvitys perustuu 266 yrityksen vastauksiin. Kyselyn toteutti Taloustutkimus yhteistyössä Helsingin seudun kauppakamarin kanssa. Selvityksen on laatinut Panu Vesterinen Helsingin seudun kauppakamarista.

Vastanneista yrityksistä 41 prosenttia edusta palveluita, 24 prosenttia teollisuutta, 13 prosenttia kauppaa, ja 6 prosenttia rakentamista. Vastaajista 21 prosenttia ilmoitti jonkin muun toimialan kuin yllä mainitun.



Selvityksen vastaajista suurin osa (46 %) on yritysten toimitusjohtajia. Hallitusjäseniä on 17 prosenttia vastaajista. Talousjohtajia tai kehitysjohtajia on seitsemän prosenttia vastaajista ja turvallisuus- ja riskienhallintajohtajia myös seitsemän prosenttia.

Selvityksessä käytetään nettoprosenttiosuutta ja saldolukua. Nettoprosentti ilmaisee, kuinka suuri osa vastaajista on ilmoittanut, että ainakin yksi mainituista turvallisuusriskeistä on toteutunut. Riskienhallintaa kuvaavissa kaavioissa osuus ilmaisee vastaavasti sen, kuinka monella vastaajalla on käytössä ainakin yksi kaaviossa esitellyistä riskienhallintakeinoista.
Yritysrikosten määrän kehitystä kuvaavissa taulukoissa käytetään saldolukua. Saldoluku on rikosten lisääntymistä kokeneiden yritysten osuuden ja vähentymistä ilmoittaneiden yritysten osuuden erotus.

2 YRITYSRIKOSTEN MÄÄRÄN KEHITYS

Yrityskyselyihin perustuvien tutkimusten tavoitteena on tuoda tietoa myös niistä yrityksiin kohdistuvista toteutuneista riskeistä, jotka muuten jäisivät piilorikollisuudeksi. Tilastokeskuksen mukaan piilorikollisuuteen lasketaan rikokset, jotka eivät tule poliisin tietoon ja joita siten ei rikoksina rekisteröidä. Yritysrikosten määrän kehitystä on vaikea arvioida pelkästään poliisin tilastojen perusteella.

Piilorikollisuuden suuri osuus yritysrikoksista johtuu pääasiassa kahdesta tekijästä: rikosten ilmoittamishalukkuudesta ja tilastointikäytännöistä. Yritykset eivät läheskään aina ilmoita rikos- tai väärinkäytösepäilyistä poliisille. Helsingin seudun kauppakamarin 2019 tehdyssä tiedon suojaamiseen keskittyvässä kyselyssä ilmeni, että enemmistö yrityksistä on jättänyt rikosilmoituksen tekemättä. Yritysrikollisuuden kokonaiskuvan hahmottamista vaikeuttaa edelleen se, ettei poliisin tietokannassa eritellä yrityksiin kohdistuvia rikoksia.

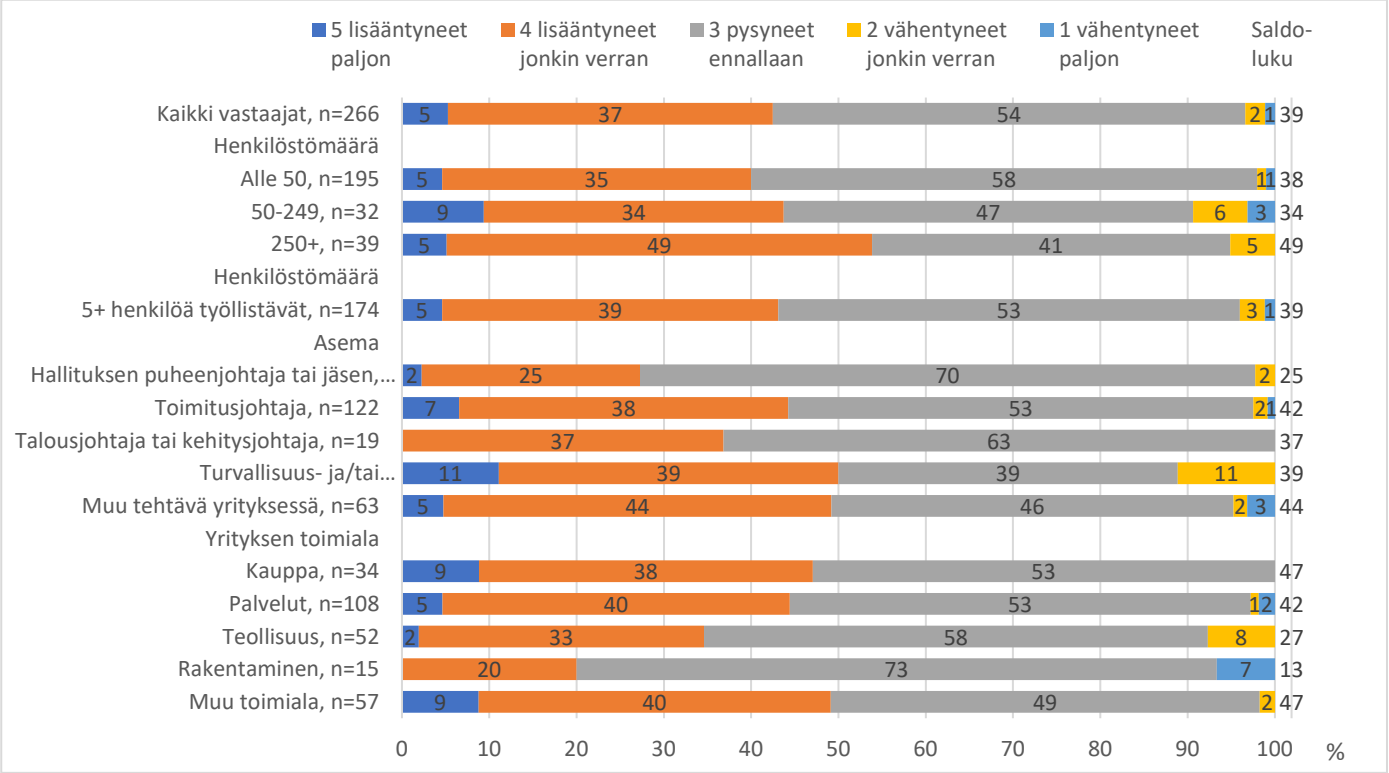
”Oikeusjärjestelmän hitaus, käräjäoikeuksien heikko kyky perehtyä asioihin, viranomaisten haluttomuus tehdä päätöksiä joilla vaikutettaisiin toimintaympäristöön. Yhtiö tekee jatkuvaa riskianalyysia, joten turvallisuudessa on aina puutteita, jos näitä ei katsottaisi olevan eikä pystyttäisi havainnoimaan, voidaan lähtökohtaisesti katsoa turvallisuustilanteen romahtaneen pahasti.”

”Poliisin tulo kesti 1h30 minuuttia.”

”Koska varkaan tunnistus videolta oli 99% syyttäjä päätti jättää syyttämättä."

”Vaikeuttamisella pystytään kiristämään; oikeuskäsittelyn prosessit ovat niin hitaita, suomalaisen käräjäoikeuden kyky perehtyä monimutkaiseksi tehtyyn todisteluaineistoon on niin heikko ja valituskäytäntö mahdollistaa minkä tahansa asian venyttämisen vuosien mittaiseksi. Yrityksellä on kiusaus ja helpompi maksaa huomattaviakin "sovintosummia" oikeudenkäyntien, asianajon, oikeudessa odottavan asian sijaan.”

Ovatko yritykseen kohdistuvat rikosriskit ja väärinkäytökset viimeisen kolmen vuoden aikana…



Vastanneet yritykset arvioivat yleisesti yritykseen kohdistuneiden erilaisten rikosten ja väärinkäytösten lisääntyneen kehitystä viimeisen kolmen vuoden aikana. Kaikista vastaajista 42 prosenttia kertoi niiden lisääntyneen vähintään jonkin verran. **Trendi on ollut samansuuntainen viimeisen viidentoista vuoden ajan.** Kaupan alalla 47 prosenttia ja palvelualalla 45 prosenttia ilmoitti lisääntymisestä. Teollisuudessa (35 %) ja rakennusalalla (20 %) määrä oli hieman vähäisempi.

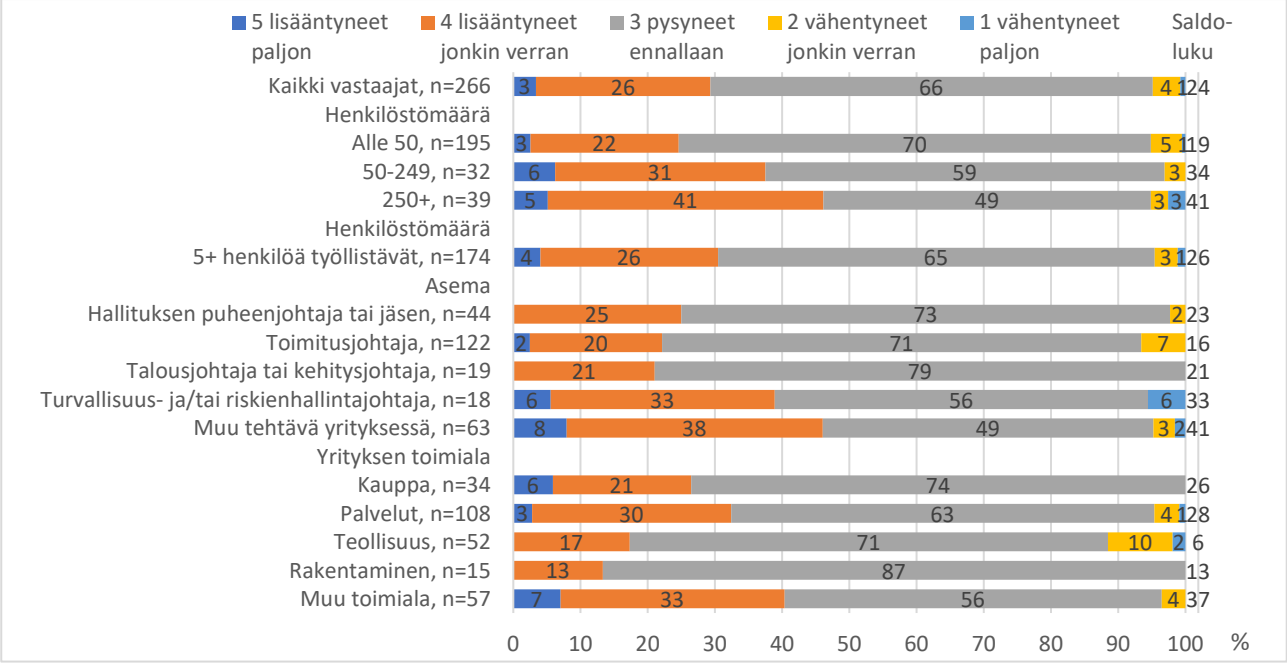
Kokoluokan mukaan jaoteltuna yli puolet (54 %) suurista vastaajayrityksistä, keskisuurista 43 % prosenttia ja pienistä 40 prosenttia vastasi tilanteen huonontuneen.

Saldoluvut kertovat osaltaan tilanteen huonontuneen, kaikkien vastaajayritysten saldoluku on 39. Vastaajien kokoluokan mukaan suurten vastaajayritysten 49, keskisuurten 34 ja pienten 38. Toimialoista suurin saldoluku 47, oli kaupan alalla. Se tarkoittaa että kaupan alalla tilannetta huonontuneena pitäviä yrityksiä on 47 prosenttiyksikköä enemmän kuin niitä, joiden mielestä tilanne on parantunut.

3 IHMISET YRITYSRIKOSTEN KOHTEINA JA TEKIJÖINÄ

Kaikista vastanneista yrityksistä 31 prosenttia oli kokenut henkilöstöön liittyviä turvallisuusriskejä viimeisen kolmen vuoden aikana. Yleisimpiä turvallisuusriskejä ovat työntekijän uhkailu tai häirintä töissä sekä työntekijän syyllistyminen rikokseen tai väärinkäytökseen yritystä kohtaan. Yrityksen henkilöstöön liittyvät riskit yleistyvät yrityksen kasvaessa. Suurilla yrityksillä on enemmän henkilökuntaa ja yleensä myös toimipisteitä kuin pienemmillä. Siksi niiden henkilöstöön kohdistuneet uhat ovat huomattavasti yleisempiä kuin pienempien yritysten.

Yritysten henkilöriskien kehitys viimeisen kolmen vuoden aikana



”Pidimme tiloissamme juhlat, joihin osallistui yhtiön henkilöstön lisäksi asiakkaita ja osakkaita. Hallinnon huoneen ovia ei saa lukkoon, mutta ne olivat suljettuna - oletimme sen riittävän kertomaan vieraille, että tilaan ei saa mennä. Illan mittaan vieraat levittäytyivät huoneeseen istumaan sulusta huolimatta ja muutama päivä myöhemmin huomasimme huoneessa olleen (pienen) käteiskassan kadonneen.”

”Toimitiloissa ulkopuoliset palveluntarjoajat ovat tietoturvariski; esim. siivous, koska kaikki eivät tunnu ymmärtävän niin yksinkertaista asiaa, ettei ovia saa jättää auki, jos poistuu hetkeksi paikalta.”

”Ulkopuolinen henkilö pääsi yrityksen tiloihin tekeytymällä työntekijäksi.”

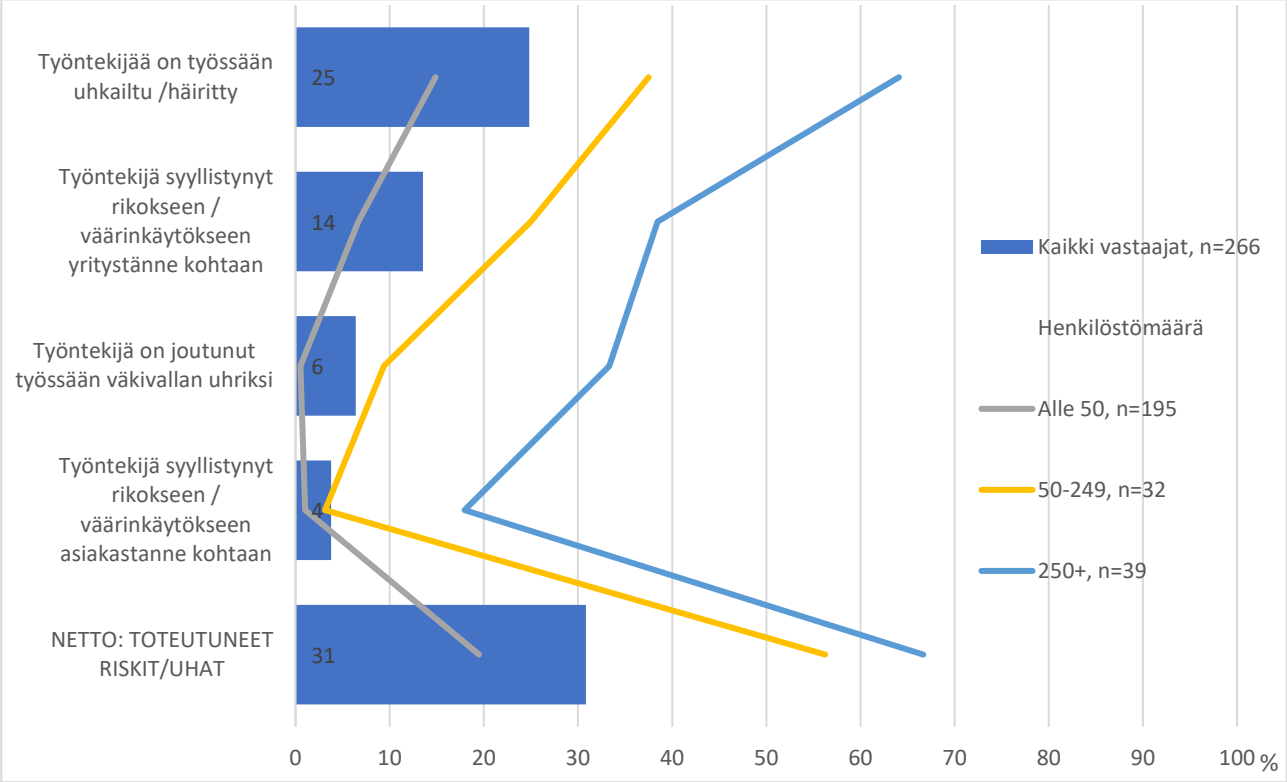
Vastanneet yritykset arvioivat henkilöstöön kohdistuneiden rikosten ja väärinkäytösten kehitystä viimeisen kolmen vuoden aikana. Kolmasosa kaikista vastaajista (29 %) kertoi niiden lisääntyneen vähintään jonkin verran. **Trendi on ollut samansuuntainen viidentoista vuoden ajan.** Palvelualalla 33 prosenttia ja kaupan alalla 27 prosenttia vastasi näin. Teollisuudessa (17 %) ja rakennusalalla (13 %) määrä oli hieman pienempi.

Lähes puolet (46 %) suurista vastaajayrityksistä, keskisuurista yli kolmasosa (37 %) ja pienistä neljäsosa (25 %) vastasi tilanteen huonontuneen.

Saldoluku kertoo että 24 prosenttia suurempi määrä vastaajista kokee tilanteen huonontuneen kuin olevan parempi kuin aiemmin. Kokoluokan mukaiset saldoluvut kertovat tilanteen huonontuneen seuraavasti: suurien 41 keskisuurten 34 ja pienten 19.

Yrityksen henkilöstöön kohdistuvat turvallisuusriskit

Toteutuneet riskit/uhat

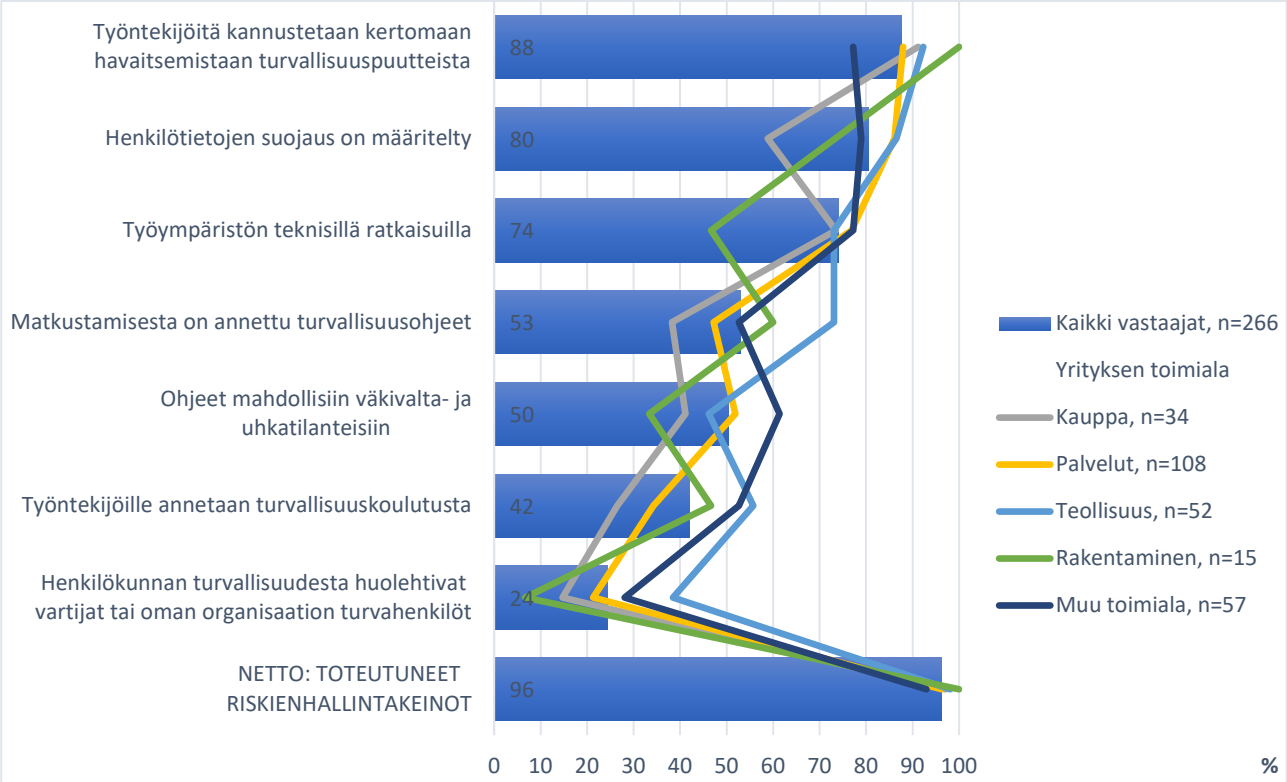


1. **Häirintä tai uhkailu**
   Kaksi kolmasosaa suurista vastaajayrityksistä (64 %) ja neljäsosa kaikista vastaajista (25 %) kertoi työntekijöiden joutuneen häirinnän tai uhkailun kohteeksi.

2. **Työntekijän rikos tai väärinkäytös**
   Suurista vastaajayrityksistä 38 prosenttia ja keskisuurista 25 prosenttia taas kertoi työntekijän syyllistyneen rikokseen tai väärinkäytökseen työnantajaansa kohtaan. Kaikista vastaajista 14 prosenttia oli joutunut kokenut saman tilanteen.

3. **Työntekijään kohdistunut väkivalta**
   Kolmasosa suurista vastaajayrityksistä (33 %) kertoi työntekijään kohdistuneesta väkivallasta.

Miten varautua uhkatilanteisiin?



”Huoltojen / remonttien aikana on syntynyt aukkoja fyysiseen turvallisuuteen, koulutuksista huolimatta henkilöstö toimii joskus (harvoin tosin!) ohjeiden vastaisesti.”

”Turvallisuusselvitykset; vastaukset tulevat melkoisella viiveellä ja henkilö on voinut olla tehtävässään jo jonkin aikaa, kunnes tieto saadaan.”

Vastaajat kertoivat yrityksen tavoista suojata henkilöstöä väkivallalta ja uhkatilanteilta. Seuraavilla keinoilla voidaan parantaa yrityksen työntekijöiden turvallisuutta:

1. **Työntekijöitä kannustetaan kertomaan turvallisuuspuutteista** (88 %)
   Henkilöstön tekemät havainnot ovat tehokkaimpia tapoja saada tieto puutteista yrityksen vastuuhenkilöiden tietoisuuteen. Tiedon saaminen havaituista puutteista ohjaa yrityksen turvallisuustyötä oikeisiin kohtiin. Työntekijä on yleensä huomattavasti parempi oman työympäristönsä turvallisuusriskien asiantuntija kuin yrityksen vastuuhenkilö, joka ei työskentele samassa työpisteessä.

   Yleisesti lähes kaikissa yrityksistä työntekijää kannustetaan kertomaan havaitsemistaan turvallisuuspuutteista. Rakennusalalla kaikki vastaajat, teollisuudessa 92 prosenttia, kaupan alalla 91 prosenttia ja palvelualalla 88 prosenttia kertoivat kannustavansa työntekijöitään kertomaan havainnoistaan. Tulokset kertovat siitä, että yritykset ymmärtävät työntekijöiden havaintojen arvon ja tehokkuuden turvallisuusresurssien suuntaamisessa.

2. **Henkilötietojen suojaus on määritelty** (80 %)
   Yritysten on suojattava sekä työntekijöiden että asiakkaidensa henkilötietoja. Henkilötietojen suojaamisen osalta merkittävä 17 prosenttiyksikön nousu (vuoden 2017 63%) tämän vuotiseen kertoo Tietosuojadirektiivin voimaantulon 2018 myötä lisääntyneestä tietoisuudesta henkilötietojen käsittelyssä. Suuret yritykset ilmoittivat lähes poikkeuksetta, että niissä henkilötietojen suojaus on määritelty. Osuudet olivat heikoimmat pienissä yrityksissä (77 %) ja kaupan alalla (59 %).

3. **Työympäristön tekniset ratkaisut** (74 %
   Lain mukaan yrityksen pitää huolehtia työntekijöidensä turvallisuudesta. Teknisiä ratkaisuja ovat esimerkiksi kameravalvonta ja erilaiset henkilöhälyttimet. Kyselyyn vastanneista yrityksistä 74 prosenttia ilmoitti käyttävänsä teknisiä ratkaisuja. Yleisintä tämä oli palvelualalla ja ”Muiden alojen” vastaajien keskuudessa (77%) ja vähiten niitä käytettiin rakennusalalla (47%). Rakennusalan osalta työmaat rajaavat käytännön mahdollisuuksia käyttää teknisiä järjestelmiä tähän tarkoitukseen.

4. **Ohjeet väkivalta- ja uhkatilanteiden** (50%) **ja turvallisuuskoulutus** (42 %)
   Vain puolella kaikista kyselyyn vastanneista yrityksistä on ohjeet mahdollisiin uhka- ja väkivaltatilanteisiin. Eri aloilla ohjeita väkivalta- ja uhkatilanteisiin käytettiin seuraavasti: ”Muiden alojen” vastaajat 61 prosenttia, teollisuudessa 52 prosenttia, palvelualalla 46 prosenttia ja kaupan alalla 41 prosenttia vastaajista.

   Turvallisuuskoulutusta järjesti alle puolet kaikista (42 %) vastaajista. Kouluttaminen on kuitenkin tehokkain tapa jalkauttaa erilaiset ohjeet ja toimintamallit työntekijöille. Eri aloilla henkilökuntaa koulutettiin seuraavasti: teollisuudessa 56 prosenttia, ”Muiden alojen” vastaajat 53 prosenttia, rakennusalalla 46 prosenttia, palvelualalla 34 prosenttia ja kaupan alalla 26 prosenttia vastaajista.

5. **Vartijoiden tai oman turvallisuushenkilökunnan käyttäminen** (24 %)
   Neljäsosa kaikista vastaajista käytti palveluntarjoajan tai omia ammattilaisia henkilöstönsä turvaamiseen. Vartijoiden käytön tarvetta rajaa yrityksen toiminnan luonne, on myös paljon yrityksiä joilla ei ole tarvetta käyttää erikseen vartiointipalveluja esimerkiksi sen vuoksi, että ne toimivat toimistokompleksissa tai toimivat rakennustyömailla. Eri aloilla vartiointia käytettiin seuraavasti: teollisuudessa 38 prosenttia, ”muita aloja” edustavat vastaajat 28 prosenttia, palvelualalla 21 prosenttia ja kaupan alalla 15 prosenttia vastaajista.

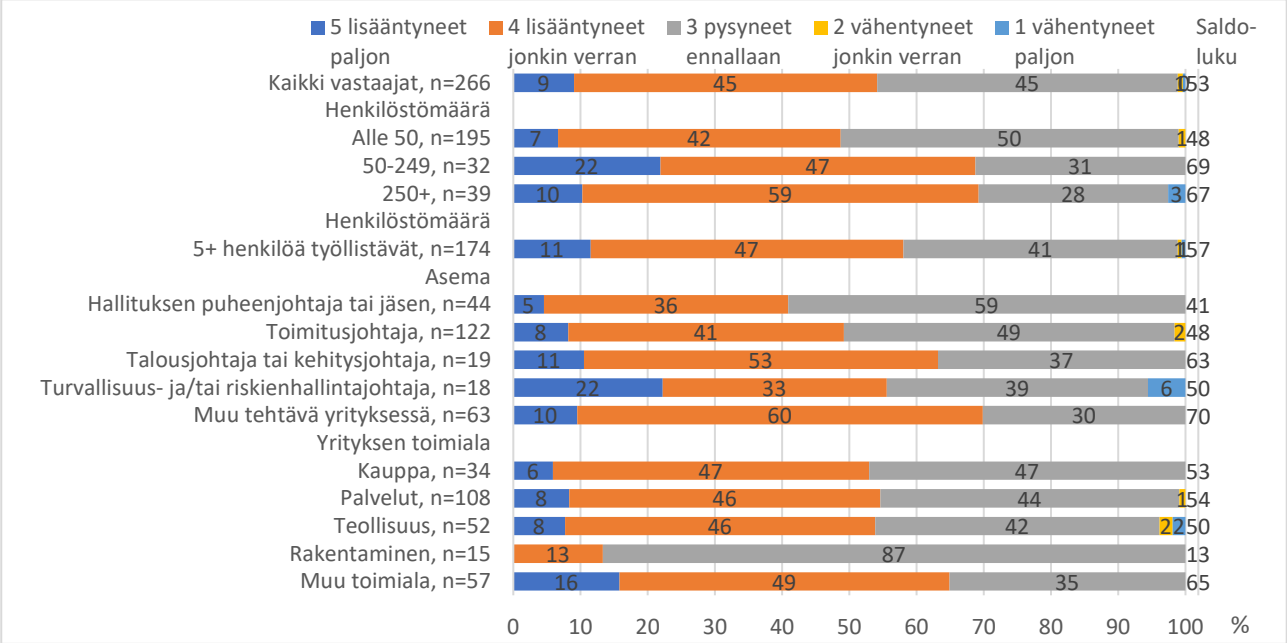
4 TIETOON KOHDISTUVAT RIKOKSET JA VÄÄRINKÄYTÖKSET

Kaikista vastanneista yrityksistä 34 prosenttia oli kokenut erilaisia tietoon kohdistuneita rikoksia tai tahallisia väärinkäytöksiä viimeisen kolmen vuoden aikana. Vastaajista 54 (2017: 44) prosenttia arvioi tietoturvallisuusriskien lisääntyneen paljon tai jonkin verran. Vuoden 2017 selvityksestä on tapahtunut 10 prosenttiyksikön muutos huonompaan suuntaan. Yleisimmät tietoon liittyvät rikokset ja väärinkäytökset ovat yritystiedon luvaton urkkiminen/ vakoilu, tietoverkkoon murtautumiset, kriittisten yritysasioiden kertominen luvatta kolmannelle osapuolelle ja tietojen luvaton kopiointi ennen siirtymistä pois yrityksen palveluksesta.

”Jokunen ovela sähköpostiviesti tutusta lähteestä on tullut, mutta virussuoja on toiminut. Myöskin yrityksen "toimitusjohtajalta tullut maksupyyntö" on onnistunut aiheuttamaan hämmennystä.”

”Toimistoon on murtauduttu ja yrityksen tietoja sisältäviä kovalevyjä varastettu.”

Yritysten tietoon liittyvien turvallisuusriskien kehitys

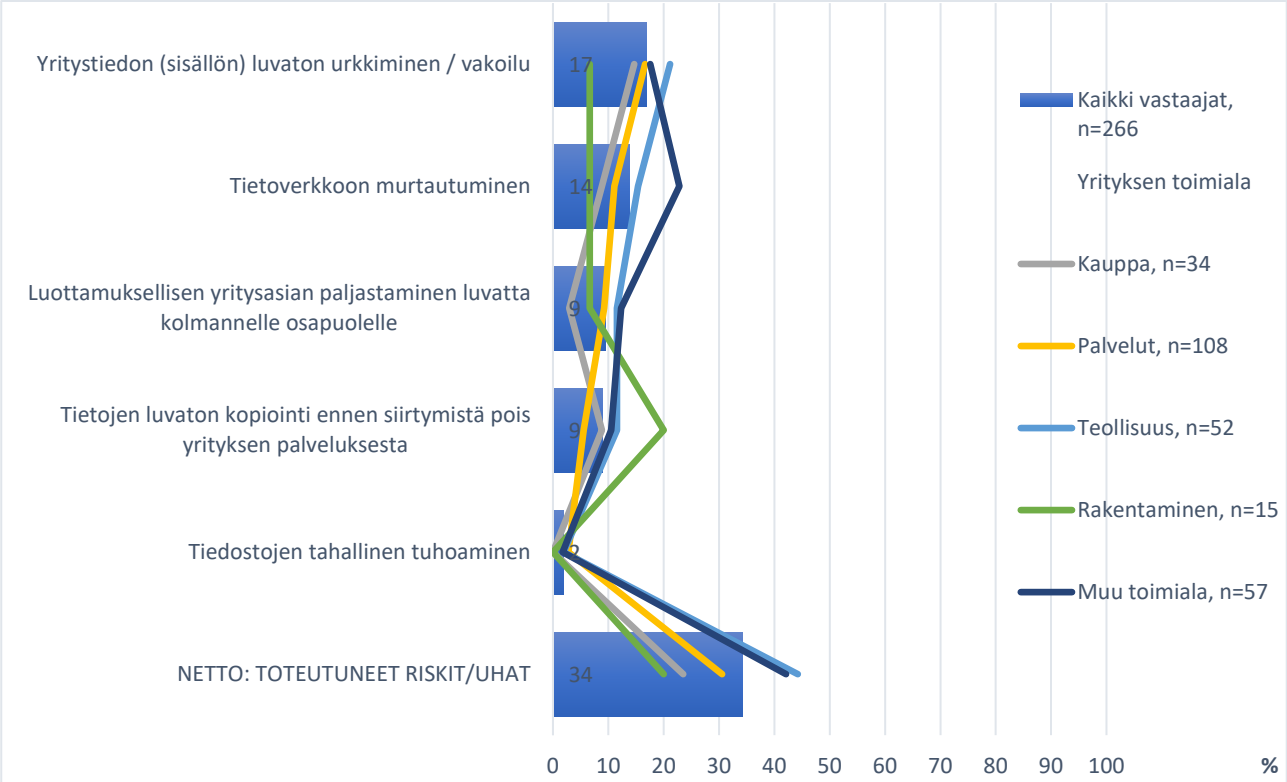


Saldoluku 53 kertoo karulla tavalla sen, että tilanteen aiempaa huonompana näkevien yritysten ”ylivoima” on 54 prosenttia vastaan tilannetta aiempaa parempana pitävien 1 prosentti. **Yritysten kanta on selvä, yritysten tietoon kohdistuvat riskit ovat lisääntyneet.** Vuonna 2017 saldoluku oli 42 ja 2012 se oli 34. Trendi on varsin yksiselitteinen ja osoittaa tarvetta kehittää yritysten tietoturvaa.

”Asiakas vieraili tuotantotilassa ja kuvasi kamerakännykällä seinällä olevia asiakastilauspapereita.”

”Alihankkijan tuottamaan nettisivustoon hakkeroitiin ja sitä kautta yritettiin päästä käsiksi rekisteröityneiden käyttäjien sähköpostiosoitteisiin ja salasanoihin.”

Yritysten tietoriskit viimeisen kolmen vuoden aikana



Yleisimmät tietoriskit yrityksissä

Yritysten kokemien tietoturvaloukkausten kärjessä olivat yritystiedon luvaton urkkiminen tai vakoilu, tietoverkkoon murtautumiset ja muut sisäiset tietoon liittyvät väärinkäytökset.

”Turvalliset, keskitetysti hallitut päätelaitteet, turvatut yhteydet yrityksen omaan verkkoon, ohjeistus henkilöstölle etätyön- ja matkatyön riskeistä. Järjestelmien ja laitteiden jatkuva tekninen valvonta.”

1. Yritystiedon luvaton urkkiminen tai vakoilu

Kaikista vastaajayrityksistä lähes joka viides (17 %) kertoi joutuneensa urkkimisen tai vakoilun kohteeksi. Vakoilua on vaikea tunnistaa ja siksi kysymys jo viisitoista vuotta sitten muotoiltiin näin. Kasvua vuoden 2017 selvityksestä on 9 prosenttiyksikköä.

Teollisuuden vastaajayrityksistä 21 prosenttia, palvelualan ja ”muiden alojen” yrityksillä 18 prosenttia ja kaupan alan vastaajista 15 prosenttia vastasi urkkimista tai vakoilua tapahtuneen. Suurista vastaajayrityksistä 31 prosenttia, keskisuurista 25 prosenttia ja pienistä 13 prosenttia oli kertomansa mukaan joutunut urkinnan tai vakoilun kohteeksi.

Selityksenä kasvulle voi olla yritysten tietoisuuden kasvu, yhä useampi yritys ymmärtää että tietoa voi olla mielenkiinnon kohteena ja myös tapahtuneita tekoja osataan tunnistaa aiempaa useammin, niin tietoverkkojen kuin reaalimaailmankin puolella.

”Aineistoja ei kuljeteta paperisessa muodossa mihinkään, vaan kaikki etänä käsiteltävä aineisto on sähköisessä muodossa.”

2. Tietoverkkoon murtautuminen

Tietoverkkoon murtautumisen motiiveja on monia Usein syynä saattaa olla tekijän halu päästä luvattomasti käsiksi johonkin tietoon, tehdä lunnasohjelmahyökkäyksen tai kokeilla omaa hakkerointitaitoaan. Oli syy mikä tahansa, kyse on aina rikoksesta. Toimialoista yleisintä se oli ”muiden alojen” yrityksien keskuudessa (23 %).

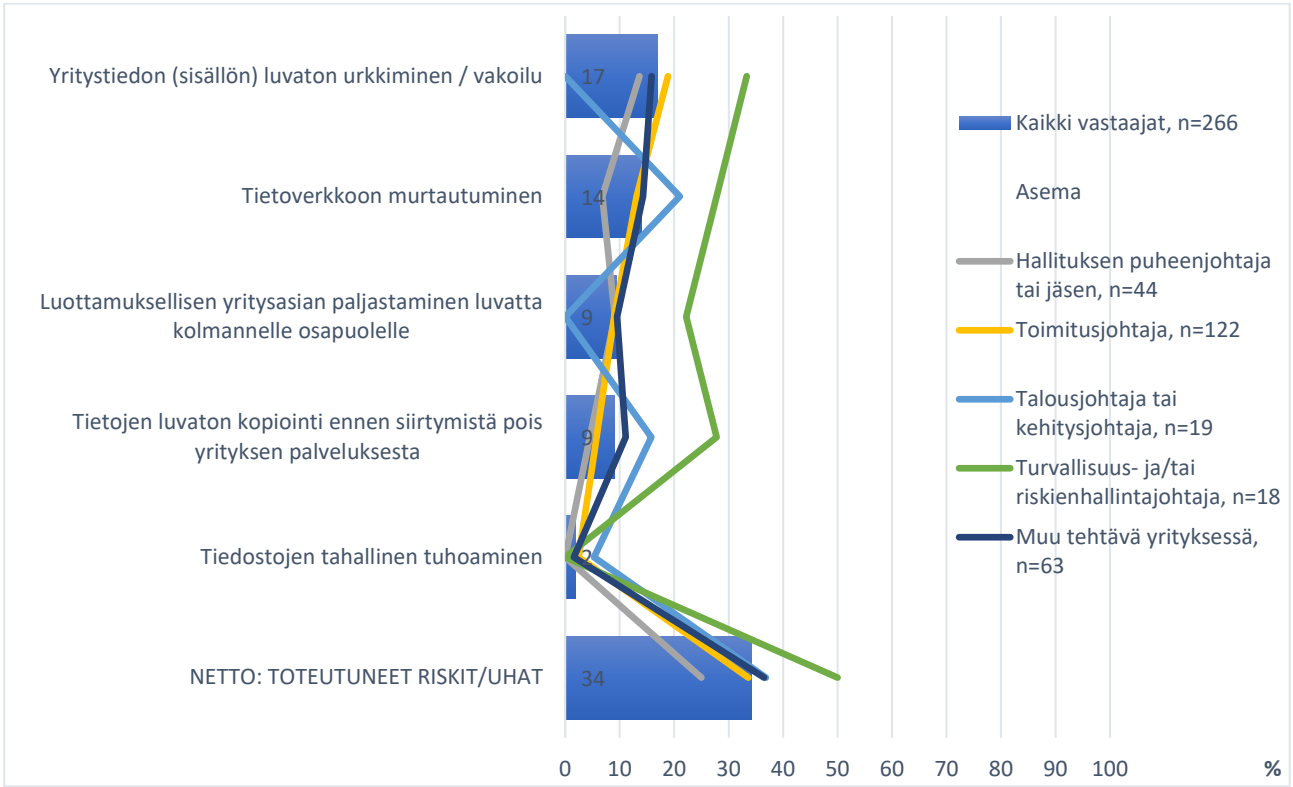
Kaikista vastaajayrityksistä 14 prosenttia kertoi joutuneensa tietomurron kohteeksi. Suurista vastaajayrityksistä 15 prosenttia, keskisuurista 11 prosenttia ja pienistä 9 prosenttia kertoi olleensa tietomurron kohteena. **Todellinen luku on huomattavasti suurempi, sillä ei ole kovinkaan yleistä että yritykset huomaavat tai osaavat tunnistaa tietomurron.**

3. Luottamuksellisen yritysasian paljastaminen luvatta ulkopuoliselle

Kaikista vastaajista joka kymmenes yritys kertoo luottamuksellisen tiedon luvattomasta paljastamisesta ulkopuoliselle. Suurista vastaajayrityksistä 26 prosenttia ja teollisuuden vastaajayrityksistä 12 prosenttia on joutunut luvattoman tiedon paljastamisen kohteeksi.

Luvaton yritystiedon paljastaminen voi tapahtua tahallisesti tai vahingossa. Se voi lipsahtaa keskustelussa tai kirjallisesti. **Tilanteesta riippuen kyseessä voi myös olla rikos, kuten yrityssalaisuuden rikkominen.** Luvaton paljastaminen tulee yrityksen tietoon täysin sattumanvaraisesti, joten voidaan arvioida että tämänkin kysymyksen kohdalla tapausten todellinen lukumäärä on huomattavasti suurempi.

”Tärkeä tieto liikkuu vain koneen tai muistitikun mukana.”



Yleisimmät riskienhallintakeinot tiedon suojaamiseksi

Yrityksen tietotaito tai muu omaisuus, joka voisi olla laittoman tiedustelun tai yritysvakoilun kohteena

Yrityksistä vain puolet (49 %) tunnistaa, että niillä on tietotaitoa tai muuta omaisuutta, joka saattaisi olla laittoman tiedustelun tai yritysvakoilun kohteena. Viidentoista vuoden aikana ei ole tapahtunut merkittävää kehitystä, vaan yhä **merkittävä osa yrityksistä ei tunnista niillä olevan tietoja, joita ulkopuolinen tunkeutuja tai vaikkapa yrityksen oma työntekijä voisi viedä.** Teollisuudessa on eniten (71 %) yrityksiä, jotka tunnistavat tiedon, joka saattaisi olla laittoman tiedustelun tai yritysvakoilun kohteena.

Ammattiryhmistä toimitusjohtajat (39 %) tunnisti yrityksen ulkopuolisia kiinnostavan yrityksen tiedon**. Jokaisella yrityksellä kuitenkin on jotain tietoa, joka voisi kiinnostaa ulkopuolisia tahoja.** Yksi selitys sille etteivät yritykset miellä niillä olevan vaikkapa kilpailijaa kiinnostavaa tietoa, on ettei yritysvakoilua ilmiönä ja toimintana tunneta. Sen vuoksi oletus siitä mikä tietoa ulkopuolinen voisi hyödyntää omaksi edukseen ja ehkä yrityksen vahingoksi jää huolestuttavalla tavalla vajaaksi. Kilpailija voi hyödyntää esimerkiksi asiakasrekisteriä, alihankkijatietoja, markkinointisuunnitelmia ja yritysostoaikeita omaksi edukseen. Monella yrityksellä on tällaisia tietoja. **Jos yritys ei tunnista omaa suojattavaa tietoa, on sen vaikea suojata sitä tehokkaasti.**

”Valvotut VPN-yhteydet ja ohjeistus tietoturvan suhteen.”
”

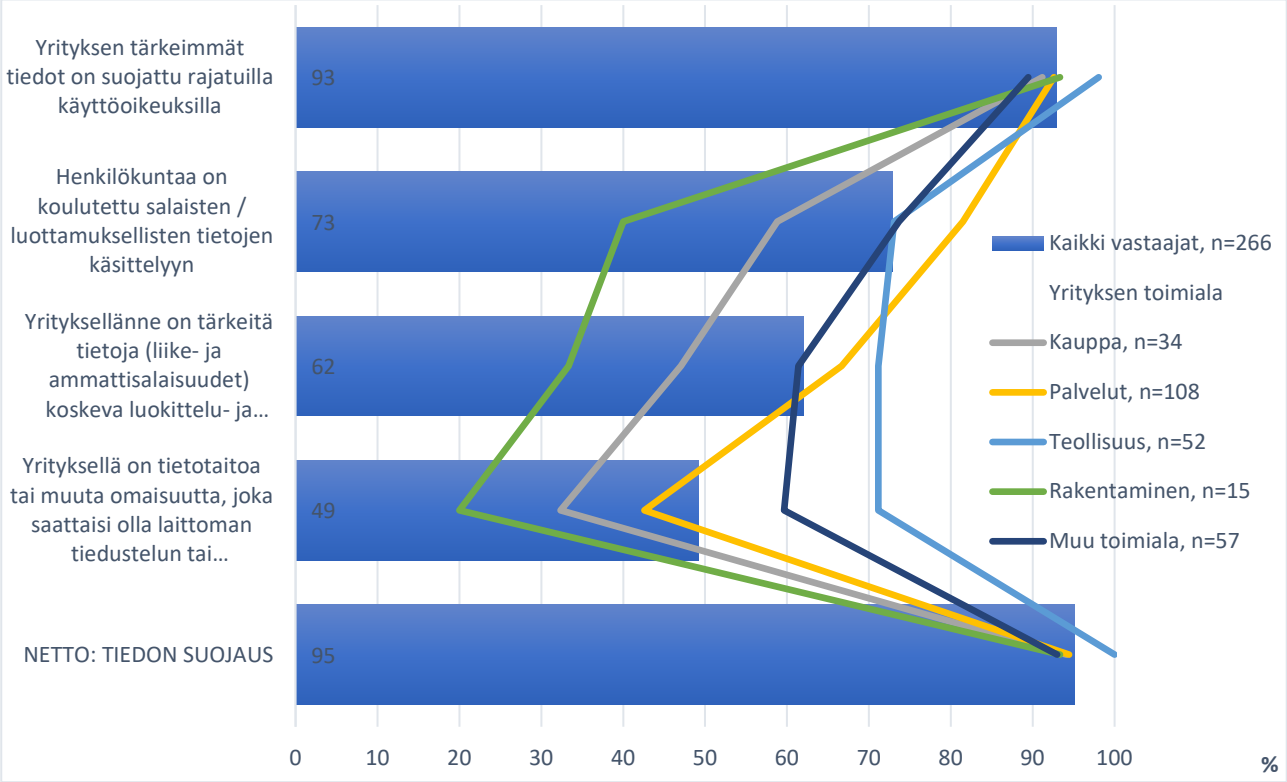
”Henkilöstöä on koulutettu tarkempaan tietoturvallisuuteen, myös työympäristön (koti) suhteen.”

”Sähköpostiin "murtauduttu" suojauksista huolimatta.”

”Henkilöstö kadottanut asiakasmateriaalia, ts. toiminut ohjeiden vastaisesti ja huolimattomasti.”

Tietoon liittyvät turvallisuusriskit

Käytetyt riskinhallintakeinot



1. **Rajatut käyttöoikeudet**

Yritys voi turvata tiedon luottamuksellisuutta, eheyttä ja saatavuutta rajaamalla tiedon tai tietojärjestelmän käyttöoikeuksia. Se on yksinkertaisimpia tapoja osoittaa ettei kyseinen tieto ole tarkoitettu kaikkien saataville. Sillä osoitetaan työntekijöille, että kyseistä tietoa halutaan suojata.

Vastaajayrityksistä 93 prosenttia kertoi suojaavansa tärkeimmät tiedot rajatuilla käyttöoikeuksilla. Toimialoista tämä oli yleisintä teollisuudessa. Ammattiryhmistä kaikki vastanneet turvallisuusjohtajat ja talousjohtajat kertoivat yrityksen suojaavan tietoa näin.

2. **Henkilökunta koulutetaan salaisten/ luottamuksellisten tietojen käsittelyyn**

Koulutuksen antama osaaminen voi parhaimmillaan estää luottamuksellisen tiedon päätymisen vahingossa vääriin käsiin. Siksi työnantajan on syytä kouluttaa työntekijät salaisen tai luottamuksellisen tiedon asianmukaiseen käsittelyyn. Koulutus parantaa työntekijöiden turvallisuusosaamista ja vähentää yrityksen tai asiakkaiden tietoihin kohdistuvia uhkia.

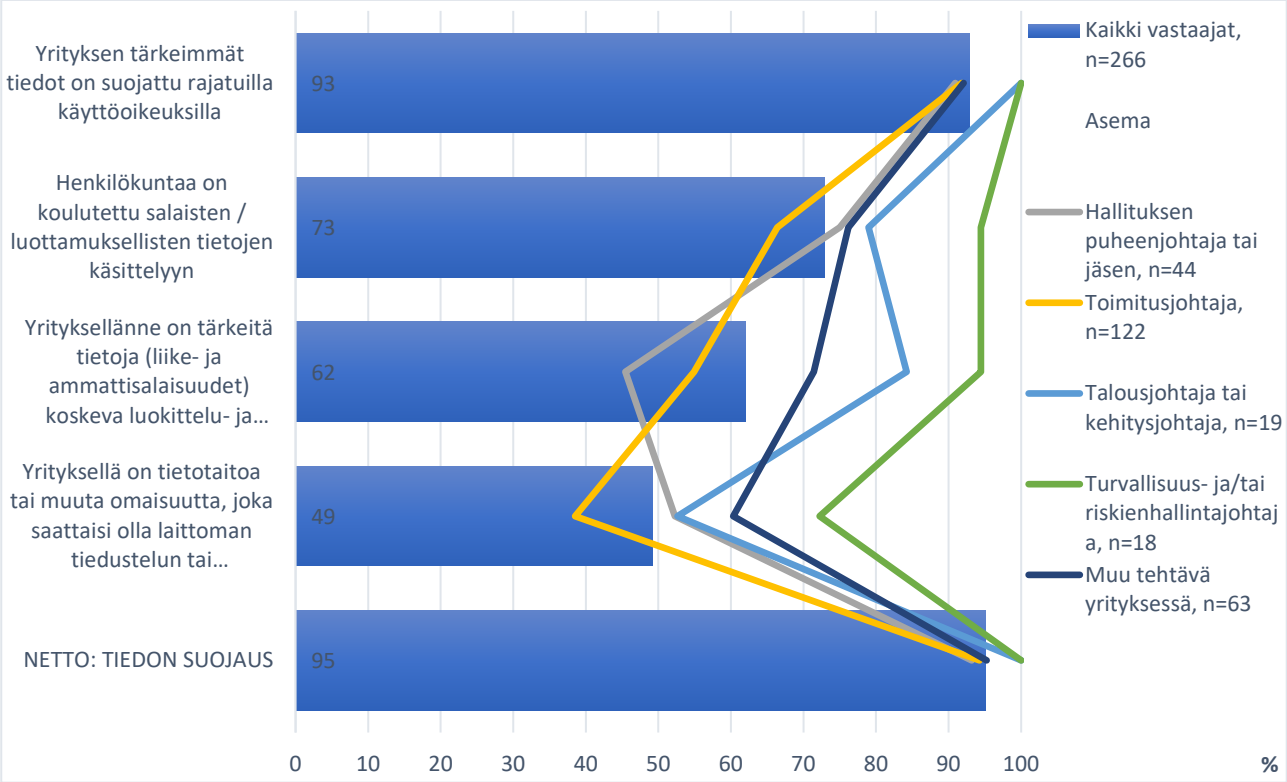
Kaikista vastaajayrityksistä 73 prosenttia kouluttaa henkilökuntaansa salaisten tai luottamuksellisten tietojen käsittelyyn. Kokoluokan mukaan suurissa yrityksissä kouluttaminen salaisten tai luottamuksellisten tietojen käsittelyyn oli yleisintä (82 %) ja myös pienistä yrityksistä 69 prosenttia koulutti salaisten tai luottamuksellisten tietojen käsittelyyn.

Toimialoista yleisintä kouluttaminen salaisten tai luottamuksellisten tietojen käsittelyyn on palvelualalla (81 %). Teollisuuden vastaajista 73 prosenttia, kaupan alan yrityksistä 59 prosenttia ja rakennusalan yrityksistä 40 prosenttia käyttää koulutuksia keinona vähentää riskiä. Huolestuttavaa on, että yli neljäsosa (27 %) prosenttia kaikista vastaajista ei kouluta työntekijöitään tiedon käsittelyyn. Joka neljännessä yrityksessä ei todennäköisesti osata käsitellä omia tai muiden salaisia tai luottamuksellisia tietoja turvallisesti.

3. Ohjeet salaisten tai luottamuksellisten tietojen käsittelystä

Ohjeet liike- ja ammattisalaisuuksien käsittelystä ovat välttämättömiä, jotta yritys voi suojata tietojaan ja kouluttaa henkilökuntaansa toimimaan oikein. Työntekijöille opetetuilla ohjeilla on myös helppo osoittaa mahdollisten rikkomusten jälkikäteisessä selvittelyssä tietoa käsitellyn väärällä tavalla. Kaksi kolmasosaa kaikista vastaajayrityksistä (62 %) oli laatinut ohjeen liike- ja ammattisalaisuuksien käsittelystä.

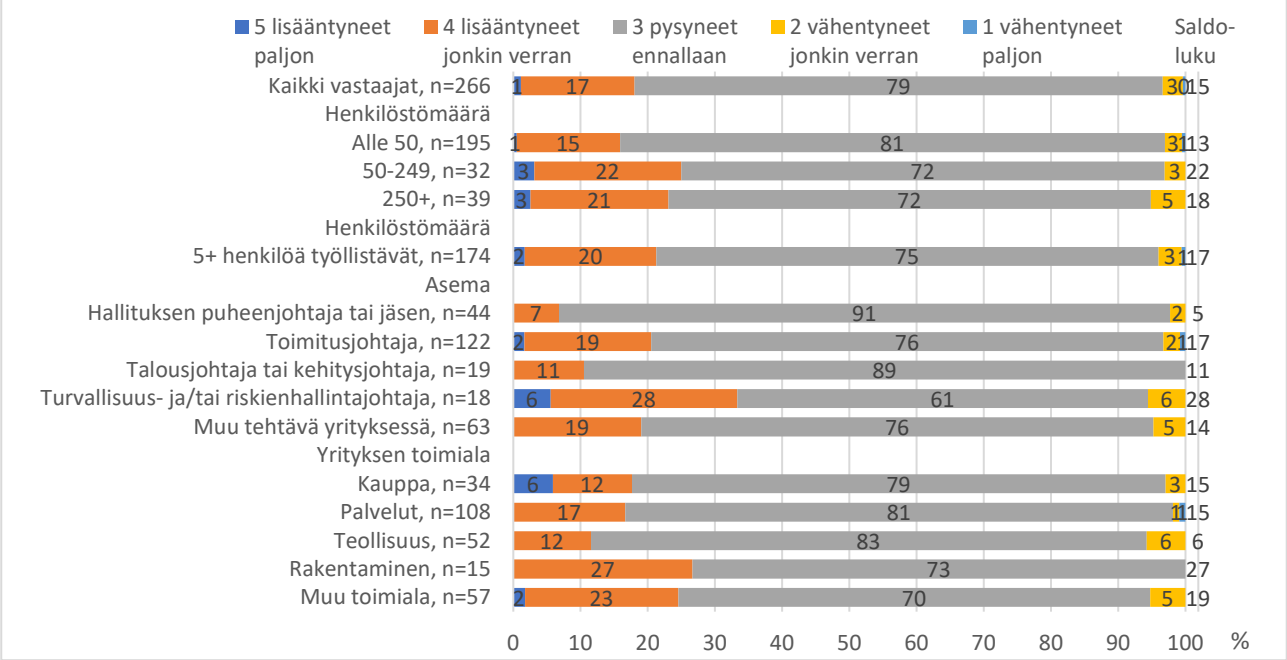
Suurista vastaajayrityksistä 85 prosentilla on ohjeet näiden tietojen käsittelyyn. Teollisuudessa 71 prosenttia, palvelualalla 67 prosenttia, kaupan alalla 32 prosenttia ja rakennusalan yrityksistä 20 prosenttia käyttää ohjeita suojatakseen tietojaan.



5 OMAISUUTEEN KOHDISTUVAT RIKOKSET JA VÄÄRINKÄYTÖKSET

Kaikkiaan 32 prosenttia kaikista vastaajayrityksistä on kokenut yrityksen omaisuuteen kohdistuneita rikoksia tai väärinkäytöksiä viimeisen kolmen vuoden aikana. Suurimmalla osalla vastaajayrityksistä (79 %) omaisuuteen kohdistuvat turvallisuusriskit ovat pysyneet ennallaan viimeisen kolmen vuoden aikana. Kokonaiskuvan kannalta on pidettävä mielessä se, että turvallisuusriskit eivät ole näiden vastaajien osalta pienentyneet. Joka viidennessä (18 %) yrityksessä omaisuuteen kohdistuvat turvallisuusriskit ovat lisääntyneet paljon tai jonkin verran. Yhteensä 97 prosenttia vastaajista kokee omaisuuteen kohdistuvien rikosten määrän pysyneen samana tai lisääntyneen.

Yritysten omaisuusriskien kehitys viimeisen kolmen vuoden aikana



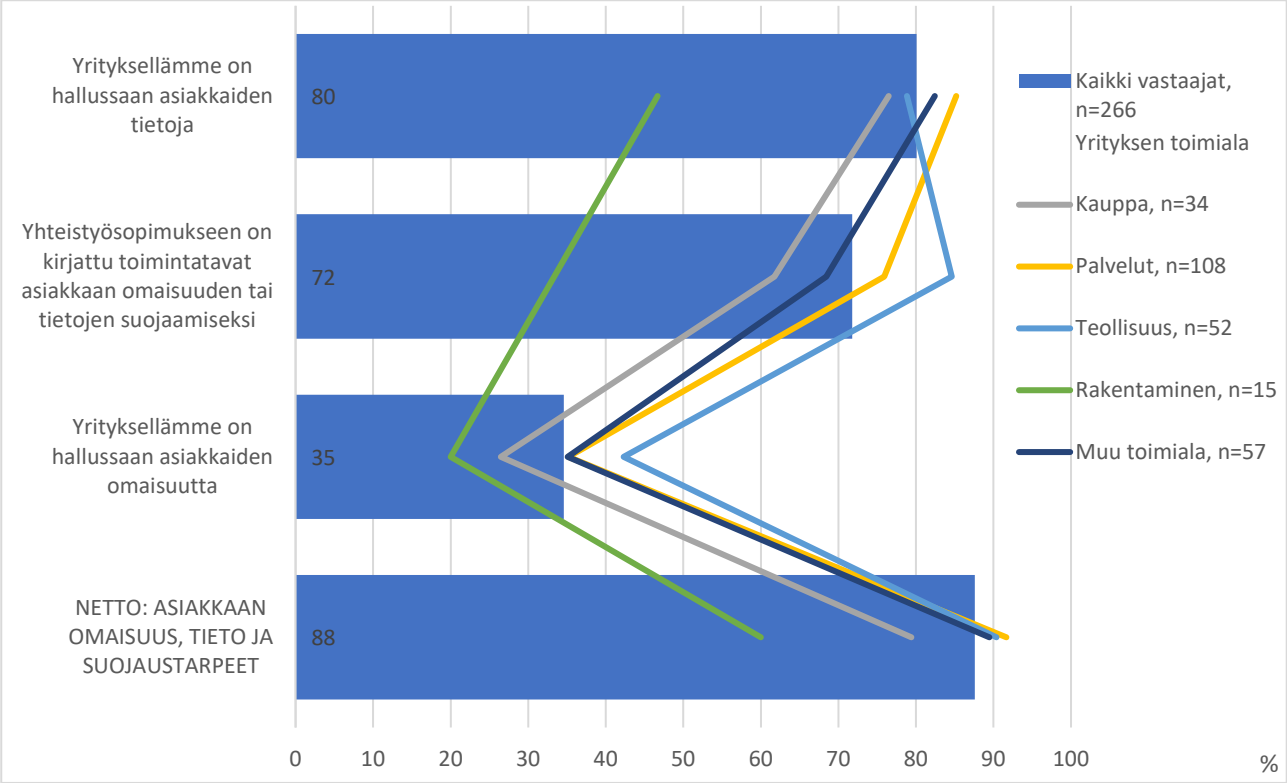
”Hälytysjärjestelmän puutteellinen toiminta ja vartiointiyrityksen puutteellinen toiminta.”

Yritysten hallussa oleva asiakkaiden tieto ja omaisuus sekä sopimukset

Asiakkaiden tietoja on suurella osalla (80 %) kaikista yrityksistä. Palvelualan yrityksistä 85 prosentilla, ”muiden alojen” yrityksistä 82 prosentilla , teollisuuden yrityksistä 79 prosentilla ja kaupan alan yrityksistä 76 prosentilla on hallussaan asiakkaiden tietoja.

Kolmasosalla (35 %) kaikista vastaajayrityksistä on hallussaan asiakkaiden omaisuutta. Teollisuudessa 42 prosentilla, palvelualalla ja ”muiden alojen” yrityksistä 35 prosentilla ja kaupan alalla 26 prosentilla on hallussaan asiakkaan omaisuutta.

Omaisuutta tai tietoja luovutettaessa osapuolet usein kirjaavat yhteistyösopimukseen tai sen liitteeseen toimintatavat asiakkaan omaisuuden tai tietojen suojaamisesta. Kaikista yrityksistä 72 prosentilla on sopimukseen kirjattu toimintatavat tietojen suojaamiseksi. Yleisintä toimintatapojen kirjaaminen omaisuuden tai tietojen suojaamiseksi on teollisuudessa (85 %), palvelualalla (76 %), ”muiden alojen” yrityksillä (68 %) ja kaupan alalla (62 %) on ja harvinaisinta rakennusalan (33 %) yrityksissä.



Yrityksiin kohdistuvien varkauksien, murtojen ja ilkivallan yleisyys

Kaikista vastaajayrityksistä joka neljänneltä (24 %) oli varastettu omaisuutta viimeisen kolmen vuoden aikana. Rakennusalan yrityksistä kaksi kolmasosaa (67 %) oli ollut varkauden kohteena. Teollisuudessa ja kaupan alalla 23 prosenttia oli joutunut varkauden kohteeksi. Vähiten varkauksia oli palvelualalla (17 %). Työmaita on vaikea valvoa tehokkaasti ja siksi varkaudet ovat yleisiä rakennusalalla.

Kaikista vastanneista yrityksistä joka seitsemäs (16 %) oli joutunut murron kohteeksi viimeisen kolmen vuoden aikana. Kaupan alalla 9 prosentilla oli ollut murtoja toimi- tai tuotantotiloihin. Teollisuudessa 19 prosenttia ja palvelualalla 12 prosenttia vastaajayrityksistä oli joutunut murron kohteeksi.

Kaikista vastaajayrityksistä 15 prosenttia oli joutunut toimi- tai tuotantotiloihin kohdistuvan ilkivallan kohteeksi. Ilkivalta toimi- tai tuotantotiloihin oli yleisintä rakennusalalla (20 %) Harvinaisinta se oli teollisuudessa (13 %), kaupan alalla (12 %) ja palvelualalla (10 %).

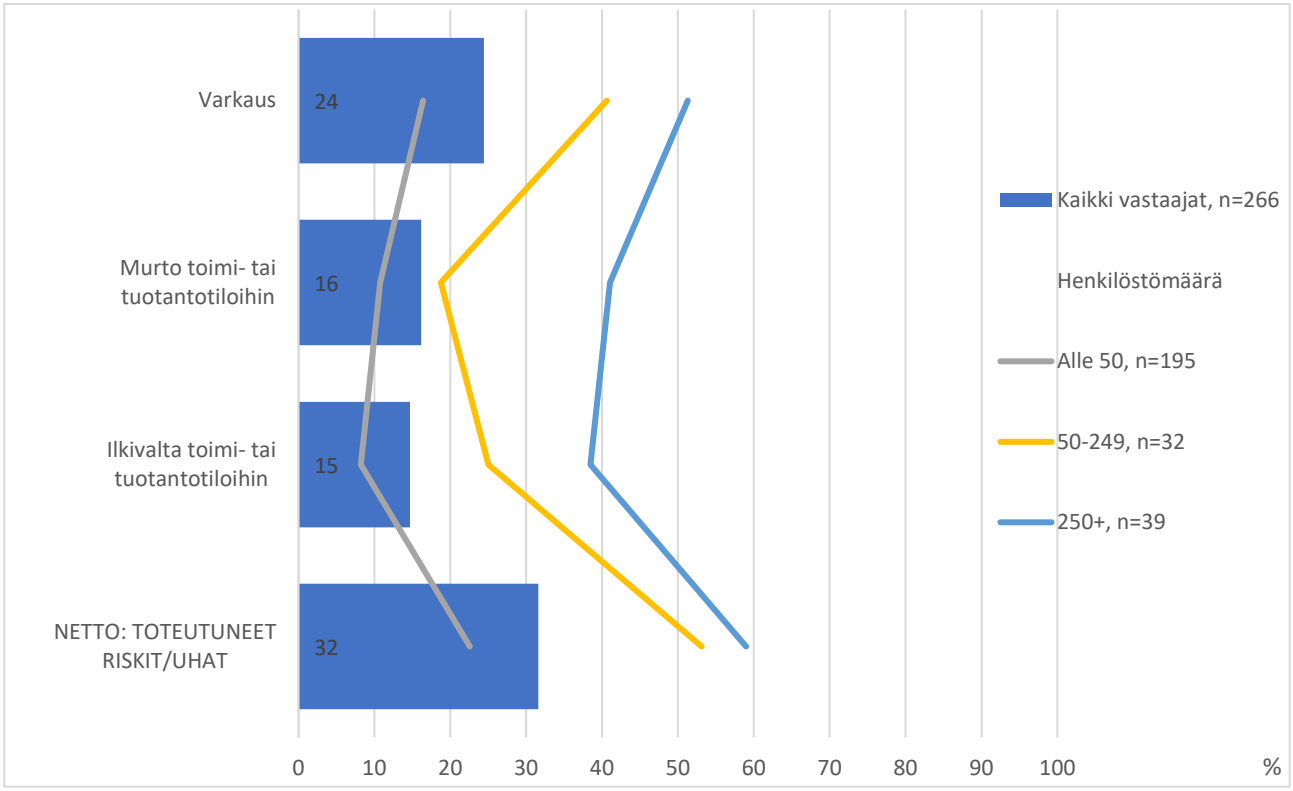
”Alueelle ja toimitiloihin päästy liian helposti sisään ns. kadulta, kukaan ei kysynyt henkilökorttia.”

”Työmaiden valvonta omaisuusrikoksiin nähden.”

”Tuotantolaitosalueen valvonta ollut puutteellinen, minkä seurauksena varkaat ovat päässeet suhteellisen vapaasti alueille.”

”Aidatulle ja suljetulle piha-alueellemme murtauduttiin leikkaamalla aitaan reikä ja vietiin arvokas laite pihalta. Kameravalvonta olisi silloin ollut paikallaan.”

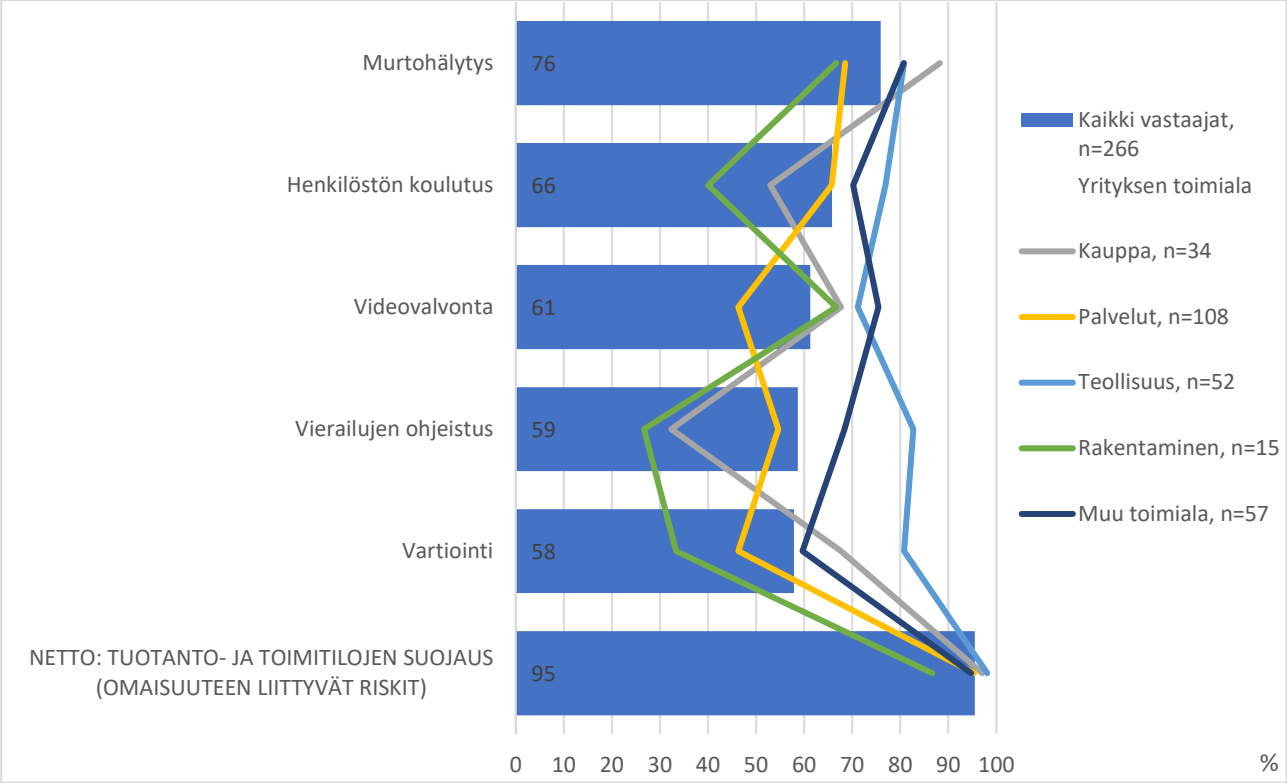
Omaisuuteen liittyvät riskit
Toteutuneet riskit ja uhat



Yleisimmät riskienhallintakeinot tuotannon ja toimitilojen suojaamiseksi

Monet yritysturvallisuuden osa-alueet ovat yhteydessä toisiinsa ja parantamalla toimitilaturvallisuuden tasoa yritys parantaa samalla esimerkiksi tietoturvallisuuden tasoa. Tietämätön tai välinpitämätön henkilökunta voi osaltaan päästää tiloihin asiattomia tahoja ja tällöin moni toimitilaturvallisuuden toimenpide menettää merkityksensä. Koulutuksella on suuri merkitys myös toimitilaturvallisuuden tehokkuuden osalta.

Käytetyt riskienhallintakeinot



”Toimistokiinteistössä sijaitsevan toimitilamme oven sähkölukko aukesi sähkökatkon aikana. Samainen ovi lukittui helposti auki asentoon eli 90 asteen kulmaan. Riskit on poistettu, sillä kiinteistön omistaja vaihtoi omalla kustannuksellaan sekä oven että lukitusmekanismin erilaiseksi.”

”Toimistolle murtauduttiin ja sieltä varastettiin paljon kalustoa ja tietoteknisiä välineitä.”

”Yhteen aikaisempaan toimipaikkaan muuttaessa ei oltu ehditty asentamaan vielä valvontakameroita ja hälytyslaitteita ja oli ensimmäinen yö muuton jälkeen, niin juuri sinä yönä murtauduttiin toimipaikkaan. Varkaat jäivät onneksi naapurikiinteistössä kiinni ja kaikki puuttuvat tavarat saatiin takaisin.”

1. **Yleisin tapa varautua on murtohälytys- / rikosilmoitinjärjestelmä** (76 %).
   Murtohälytysjärjestelmän käyttö on yleisintä kaupan alalla (88 %), seuraavina tulevat teollisuus (81 %) ja ”muu toimiala” (81 %) ja palvelut (69 %).

2. **Toiseksi yleisintä on kouluttaa henkilöstöä** (66 %).
   Yleisintä kouluttaminen on teollisuudessa (77 %), seuraavaksi yleisintä se oli niiden vastaajien keskuudessa, jotka olivat ilmoittaneet toimialakseen ”Muu toimiala”, näistä vastaajista valtaosa (70 %) koulutti henkilökuntaa. Kaksi kolmasosaa palvelualalla (66 %) ja puolet kaupan alalla (53 %) käyttivät kouluttamista keinona parantaa turvallisuutta. Henkilöstön koulutus omaisuuden suojaamiseksi oli vähäisintä rakennusalalla (40 %).

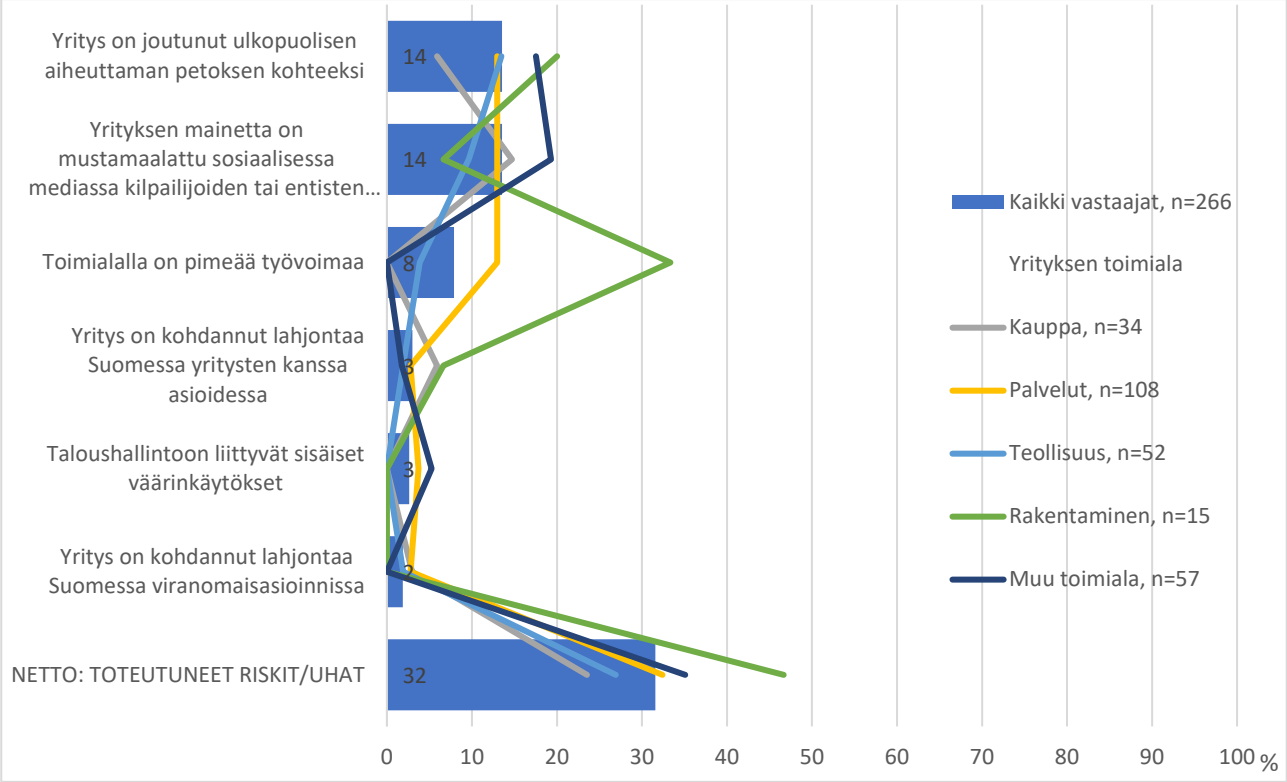
3. **Videovalvontaa käyttää kuusi kymmenestä** (61 %)
   Yleisintä videovalvonta on niiden vastaajien keskuudessa, jotka olivat ilmoittaneet toimialakseen ”Muu toimiala”, näistä vastaajista 75 prosenttia käyttää videovalvontaa, seuraavaksi yleisintä se on teollisuudessa (71 %), rakennusalalla ja kaupan alalla (67 %). Videovalvonta on harvinaisinta palvelualalla (46 %).

4. **Yli puolet (59 %) ohjeistaa vierailukäytännöt ja käyttää vartiointipalveluja (58 %)**
   Vierailujen ohjeistusta käytetään eniten teollisuudessa (83 %) ”muilla aloilla” (68 %) ja palvelualalla (55 %). Vartiointipalvelujen käyttö on yleisintä teollisuudessa (81 %), kaupan alalla (68 %), ”muilla aloilla” (60 %) ja palvelualalla (46 %).

6 TOIMINTAAN KOHDISTUVAT RIKOKSET JA VÄÄRINKÄYTÖKSET

Helsingin seudun kauppakamarin selvityksen vastaajat tarkastelivat aihealuetta perättömän tiedon levittämisen, pimeän työvoiman, lahjonnan ja taloushallintoon liittyvien sisäisten väärinkäytösten sekä ulkopuolisten henkilöiden tekemien erilaisten petosten kannalta. Kaikista vastaajista 32 prosenttiin oli kohdistunut jokin toiminnan riskeistä.

Yrityksen toimintaan liittyvät riskit viimeisen kolmen vuoden aikana



”Luottamus asiakkaaseen, joka toteutti tilauspetoksen.”

”Hakkeri ottanut sähköpostiosoitteen haltuunsa ja yritti saada kirjanpitäjän maksamaan tekaistun 67.000€ laskun nopeasti.”

”Maksuvälinepetos (kortti kopioitu ja varoja käytetty vajaa 4000€ edestä).”

Ulkopuolisen henkilön tekemät petokset

Kaikista vastaajayrityksistä 14 prosenttia ilmoitti joutuneensa ulkopuolisen aiheuttaman petoksen kohteeksi viimeisen kolmen vuoden aikana. Rakennusalan yrityksistä joka viides (20 %) ilmoitti tapahtuneesta petoksesta viimeisen kolmen vuoden aikana. Seuraavaksi yleisimpiä petokset olivat niiden vastaajien keskuudessa, jotka olivat ilmoittaneet toimialakseen ”Muu toimiala”, näistä vastaajista viidesosa (18 %) kertoi petoksen tapahtuneen. Hieman harvinaisempia petokset olivat teollisuudessa (14 %) ja palvelualalla (13 %).

Yrityksen maineen mustamaalaaminen sosiaalisessa mediassa

Sosiaalisessa mediassa leviävä perätön tieto aiheuttaa helposti haittaa kohteena olevan yrityksen liiketoiminnalle. Yleisintä perättömän tiedon levittäminen oli niiden vastaajien keskuudessa, jotka olivat ilmoittaneet toimialakseen ”Muu toimiala”, näistä vastaajista viidesosa (19 %) kertoi tulleensa mustamaalatuksi. Seuraavaksi yleisintä se oli kaupan alalla, jossa 15 prosenttia vastaajista kertoi yritykseensä kohdistuneesta mustamaalauksesta. Palvelualalla 13 prosenttia, teollisuudessa 10 prosenttia ja rakennusalalla 7 prosenttia vastaajista oli kokenut mustamaalausta. **Eri tavoin tapahtuva mustamaalaus on viidentoista vuoden aikana valitettavasti vakiintunut osaksi kaikkien toimialojen arkea**.

Pimeä työvoima toimialalla

Kaikista yrityksistä 8 prosenttia on kohdannut omalla toimialallaan pimeää työvoimaa. Yleisintä pimeä työvoima on rakennusalalla, jossa 33 prosenttia vastaajista oli kohdannut sitä. Seuraavaksi yleisintä se oli palvelualalla (13 %) ja teollisuudessa (4 %).

Vuoden 2017 yritysturvallisuuskyselyssä teollisuusyrityksistä kahdeksan prosenttia ja kaupan alan yrityksistä kuusi prosenttia raportoi pimeästä työvoimasta toimialalla. Palvelualalla pimeästä työvoimasta toimialalla raportoivien yritysten osuus on kuitenkin ollut aiempien vuosien selvityksissä selvässä kasvussa. Palvelualalla osuus oli 22 prosenttia vuoden 2017 mittauksessa, 18 prosenttia vuoden 2012 mittauksessa ja 12 prosenttia vuoden 2005 mittauksessa. Tässä selvityksessä palvelualalla pimeää työvoimaa kohdanneiden osuus oli 13 prosenttia. Harmaa taloutta on vuosien mittaan pyritty kitkemään lainsäädännöllä ja viranomaistoimin ja ne ovat todennäköinen syy ilmiön pienemiseen palvelualalla.

Lahjonta

Tässä selvityksessä tarkastellaan sekä viranomaisasioinnissa että yritysten välisessä yhteistyössä esiintyvää lahjontaa. Yritystoiminnassa ilmenevä lahjonta jää yleensä tilastoimattomaksi piilorikollisuudeksi. Selvityksessä lahjonnan yleisyyteen liittyvät luvut saattavat tuntua pieniltä, mutta kyse on kilpailua vääristävästä piilorikollisuuden ilmiöstä.

Viranomaisasioinnissa kohdattu lahjonta:

Kaikista vastaajayrityksistä kaksi prosenttia oli kohdannut lahjontaa viranomaistoiminnassa. Kaupan alan ja palvelualan yrityksistä kolme prosenttia oli kohdannut viranomaistoiminnassa lahjontaa. Rakennusalan yrityksistä ja teollisuusyrityksistä kaksi prosenttia oli kohdannut lahjontaa viranomaisasioinnissa.

Yritysten välisessä toiminnassa kohdattu lahjonta

Kaikista vastaajayrityksistä kolme prosenttia oli kohdannut lahjontaa yritystoiminnan parissa. Rakennusalan yrityksistä seitsemän prosenttia ja kaupan alan yrityksistä kuusi prosenttia oli kohdannut lahjontaa. Palvelualalla kolme ja teollisuusyrityksistä kaksi prosenttia oli kohdannut lahjontaa yritystoiminnassa.

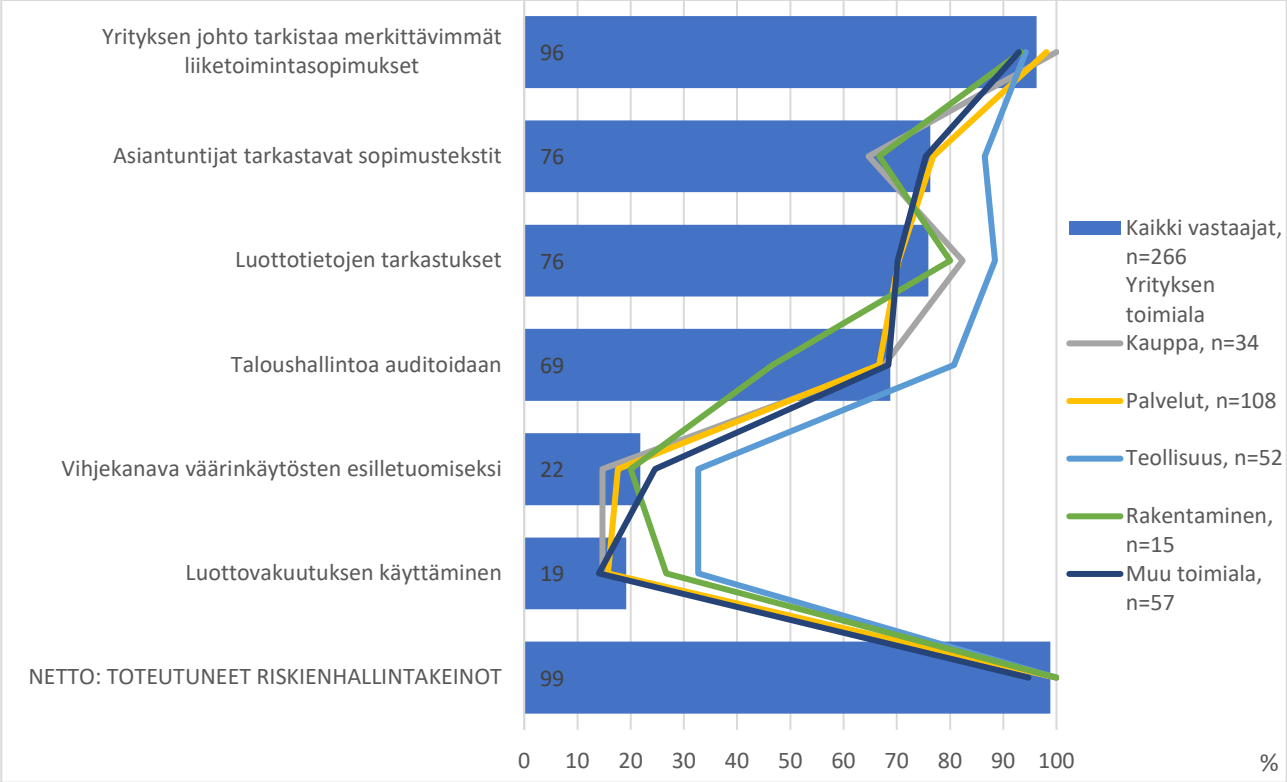
Taloushallintoon liittyvät sisäiset väärinkäytökset

Taloushallintoon liittyviä sisäisiä väärinkäytöksiä oli havainnut vain kolme prosenttia kaikista vastanneista. Toimialat, jolla väärinkäytöksiä oli havaittu, olivat ”muiden alojen” toimijat (5 %) ja palveluala

(4 %). Tämä ei kuitenkaan tarkoita ettei väärinkäytöksiä tapahdu muillakin toimialoilla ja huomattavasti enemmän kuin näiden vastausten perusteella voi päätellä.

Kyse on teoista, joita on vaikea havaita. Usein niitä tekevät henkilöt, joita ei osata edes epäillä teoista ja väärinkäytökset saattavat olla hyvin erilaisia riippuen siitä millä alalla yritys on ja mitä väärinkäytettävää omaisuutta tai palvelua yritys tarjoaa.

Yleisimmät riskienhallintakeinot toiminnan suojaamiseksi



1. **Lähes kaikissa yrityksissä johto tarkistaa merkittävimmät liiketoimintasopimukset** (96 %). Yli 90 prosentissa kaikista vastaajayrityksistä johto tarkastaa merkittävimmät liiketoimintasopimukset.

2. **Sopimukset tarkistetaan asiantuntijoiden toimesta (76 %)**
   Teollisuudessa 87 prosenttia vastaajista tarkastuttaa sopimukset asiantuntijoiden toimesta. Palvelualalla 77 prosenttia toimii näin. Rakennusalalla 67 prosenttia ja kaupan alalla 65 prosenttia vastaajista käyttää asiantuntijoita.

3. **Luottotietojen tarkistus turvaa toimintaa (76 %)**
   Teollisuudessa 88 prosenttia tarkastaa luottotietoja turvatakseen toimintansa kannattavuutta. Kaupan alalla 82 prosenttia, rakennusalalla 80 prosenttia ja palvelualalla 70 prosenttia vastaajayrityksistä tekee samoin.

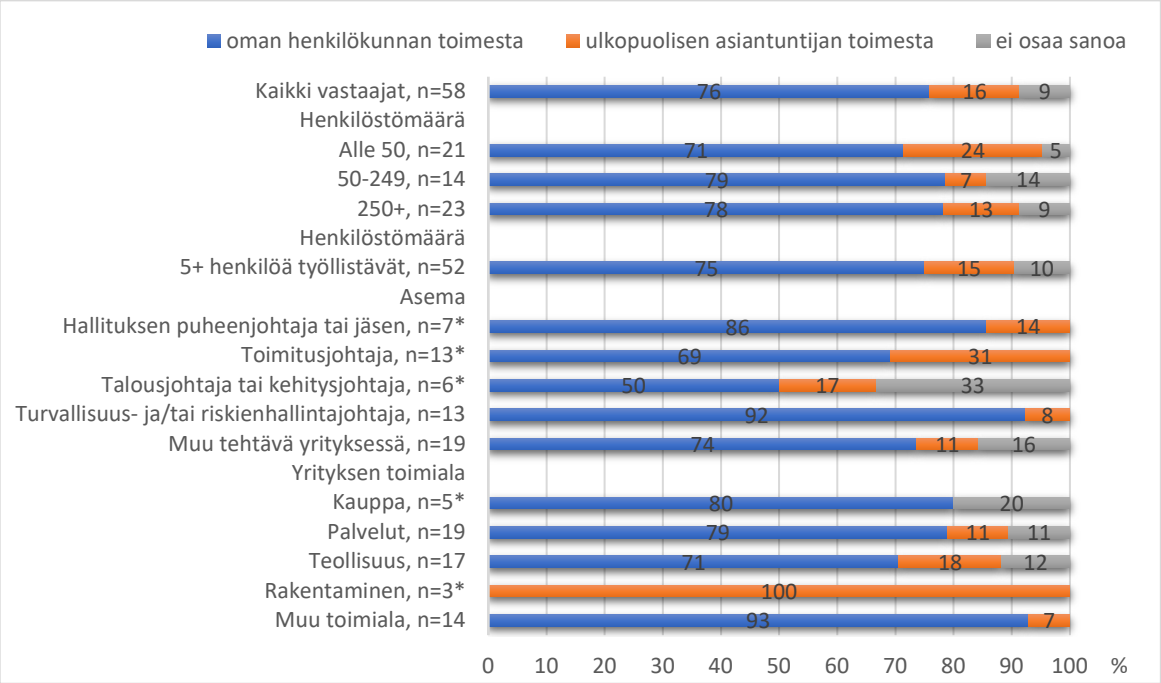
4. **Taloushallintoa auditoidaan (69 %)**
   Taloushallintoon liittyviä väärinkäytöksiä voidaan ehkäistä auditoimalla ja työtehtäviä eriyttämällä sekä käyttämällä ammattitaitoista tilintarkastusta ja sisäistä valvontaa. Auditointi on yleisintä teollisuudessa (81 %). Seuraavaksi yleisintä se on kaupan alalla ja ”muiden alojen” vastaajien keskuudessa (68 %) ja palvelualalla (67 %). Rakennusalalla alle puolet (47 %) auditoi taloushallintoa.

5. **Vihjekanava väärinkäytösten esilletuomisesta (22 %)**
   Vuoden 2021 lopussa Whistleblowing -direktiivi tulee velvoittamaan yli 50 henkeä työllistävät yritykset pitämään vihjekanavaa, jonka kautta työntekijät voivat tehdä ilmoituksia väärinkäytöksistä yrityksen toiminnassa. Alihankintaketjuissa suuret toimijat saattavat velvoittaa alihankkijansa järjestämään asian yrityskoosta riippumatta. Teollisuudessa 33 prosenttia vastaajista ylläpitää jo nyt vihjekanavaa. Seuraavaksi yleisintä se on ”muiden alojen” vastaajien keskuudessa (25 %), rakennusalalla (20 %), palvelualalla (16 %) ja kaupan alalla (15 %).

6. **Luottovakuutuksia käytetään saatavien turvaamiseksi (19 %)**
   Luottovakuutus tukee yrityksen riskienhallintaa ja sen avulla yritys voi suojata myyntisaatavansa asiakkaiden maksukyvyttömyyden ja -haluttomuuden varalta. Yleisintä luottovakuutuksen käyttäminen on teollisuudessa (33 %) ja rakennusalalla (27 %). Palvelualalla (16 %) ja kaupan alalla (15 %) se on hieman harvinaisempaa.

Yritys on varautunut toimintaan kohdistuviin rikosriskeihin vihjekanavalla

Saatuanne tiedon toiminta anne liittyvästä epäillystä väärinkäytöksestä, tutkitteko sen...



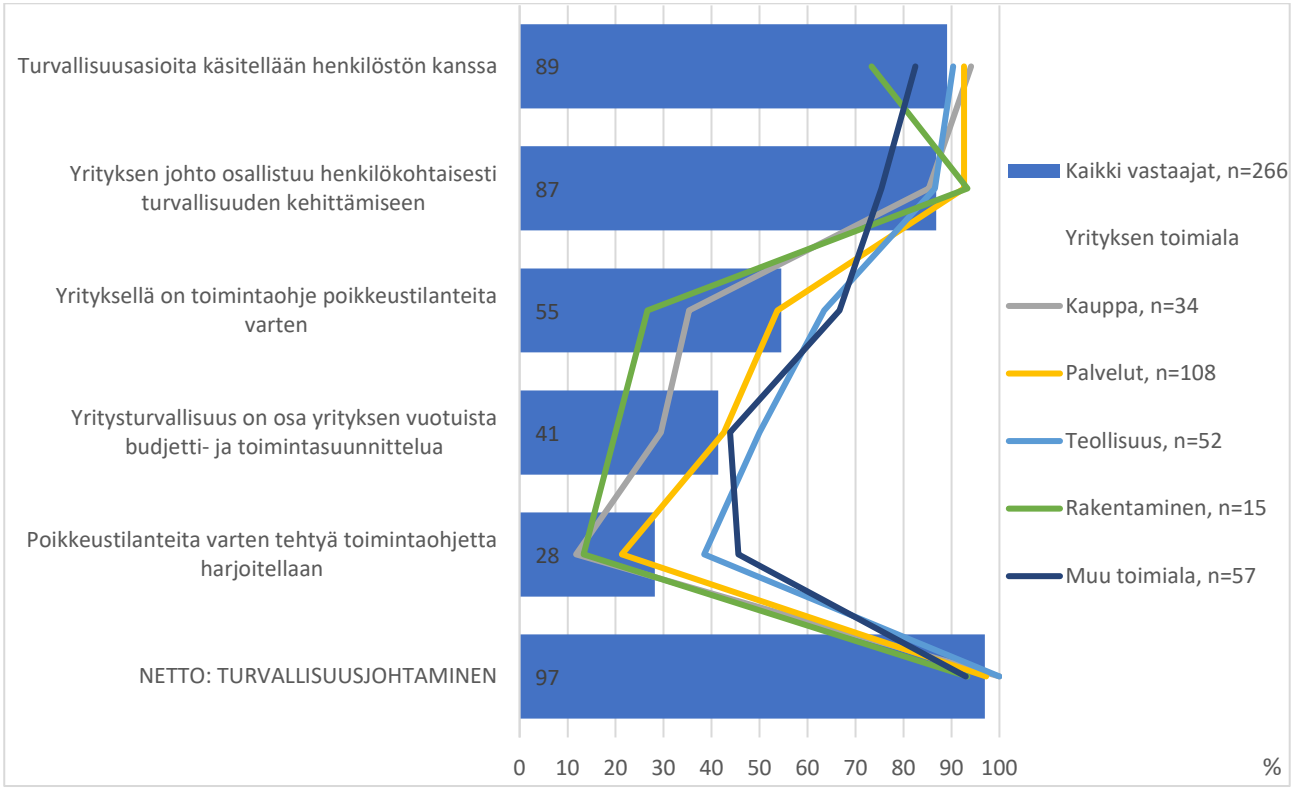
Yrityksen saatua ilmoituksen vihjekanavan kautta on sen selvitettävä asia. Joulukuussa 2021 voimaantuleva Whistleblowing -direktiivi velvoittaa yritystä reagoimaan seitsemän päivän kuluessa ilmoittamalla vihjeenantajalle saaneensa ilmoituksen ja aloittavansa selvittelyn. Kolmen kuukauden kuluessa yrityksen on kerrottava millaiseen tulokseen selvitys on johtanut.

Yritys voi tehdä selvitystyön itse tai käyttää ulkopuolista asiantuntijaa. Tärkeintä on, että selvityksen tekijät ovat ammattimaisia ja tietävät miten tutkintaa tehdään. Mikäli väärinkäytös osoittautuu epäillyksi rikokseksi, yrityksen on käytettävä palveluntarjoajaa, jolla on turvallisuusalan elinkeinolupa. Muutoin rikoksen selvittelypalvelua tarjoava taho syyllistyy itse rikokseen selvittäessään rikosta ilman tarvittavia lakisääteisiä lupia. Kaikista vastaajayrityksistä valtaosa, 71 prosenttia, selvittää tällä hetkellä väärinkäytökset itse. Tämä osuus tullee pienenemään edellä mainitun direktiivin tultua voimaan. Vastaajien kokoluokka ei aiheuta suurta vaihtelua osuuteen, pienistä 71 prosenttia, keskisuurista 79 prosenttia ja suurista 78 prosenttia selvittää väärinkäytökset itse.

7 TURVALLISUUSJOHTAMINEN

Turvallisuusjohtamisesta

Turvallisuusjohtamisen avulla yritys kehittää turvallisuuttaan johdonmukaisesti. Turvallisuus kuuluu kuitenkin yrityksen kaikkien työntekijöiden vastuulle ja on osa töiden jokapäiväistä laatua. Lähes kaikkien turvallisuusjohtamisen osa-alueiden osalta on tapahtunut näkyvää myönteistä kehitystä kun vastauksia verrataan tämän vuosina 2017, 2012, 2008 ja 2005 tehtyjen selvitysten tuloksiin. Tämä kertoo positiivisella tavalla turvallisuuden ankkuroitumisesta osaksi yritysten toimintaa ja johtamista.



Turvallisuusjohtaminen

Johdon osallistuminen ja turvallisuusasioiden käsittely henkilökunnan kanssa

”Toimitusjohtaja soveltaa myös turvallisuuteen liittyvissä asioissa omia sääntöjä, ei viranomaisten suosituksia.”

Yhdeksän kymmenestä vastaajayrityksestä (87 %) kertoi johdon osallistuvan turvallisuuden kehittämiseen. Eri toimialoilla johto osallistui turvallisuuden kehittämiseen seuraavasti: palveluala 93 prosenttia ja rakentaminen 93 prosenttia, teollisuus 87 prosenttia ja kaupan ala 86 prosenttia. Johdon esimerkki turvallisuuden osalta on hyvin tärkeää, sillä mikäli johto ei osoita mielenkiintoa ja esimerkkiä turvallisuuden noudattamisessa ja huomioimisessa jokapäiväisessä työssä eivät alaisetkaan yleensä suhtaudu siihen vakavasti.

Käsittelemällä turvallisuusasioita henkilökunnan kanssa saadaan työntekijät aktivoitua turvallisuusasioihin ja ymmärtämään roolinsa osana yrityksen turvallisuutta. Turvallisuusasioiden käsittely osana liiketoiminnan kokouksia, kuten kuukausipalavereissa ja projektikokouksissa lisää valppautta

turvallisuuden suhteen. Eri toimialoilla turvallisuutta käsiteltiin yhdessä henkilökunnan kanssa seuraavasti: palveluala 93 prosenttia ja rakentaminen 73 prosenttia, teollisuus 90 prosenttia ja kaupan ala 95 prosenttia.

Kirjallinen toimintaohje poikkeustilanteisiin ja sen harjoitteleminen

Jatkuvuutta uhkaavan tilanteen käynnistyessä ensimmäisten toimenpiteiden joukossa on käynnistää poikkeustilanteen toimintaohjeiden mukainen toiminta kutsumalla poikkeustilanteiden johtoryhmä koolle. Etukäteen tehtyjen suunnitelmien ja ohjeiden toimivuutta voi testata helpoiten harjoittelemalla eri tilanteita neuvotteluhuoneharjoituksina.

Yli puolella vastanneista yrityksistä (55 %) on poikkeustilanteen toimintaohje. Eri toimialoilla oli toimintaohje poikkeustilanteita varten seuraavasti: ”muiden alojen” vastaajat 67 prosenttia, teollisuus 63 prosenttia, palveluala 54 prosenttia, kaupan ala 35 prosenttia, ja rakennusala 27 prosenttia.

Poikkeustilanneohjetta on harjoitellut 28 prosenttia vastaajista. Poikkeustilannetta oli harjoiteltu ahkerimmin ”muiden alojen” vastaajien keskuudessa teollisuudessa, jossa 46 prosenttia oli harjoitellut toimintaa. Seuraavaksi yleisintä harjoittelu oli teollisuudessa (38 %) ja palvelualalla (21 %). Rakennusalalla (13 %) ja kaupan alalla (12 %) harjoittelu oli harvinaisempaa. On yhä monia yrityksiä, jotka eivät testaa tekemiensä suunnitelmien toimivuutta lainkaan.

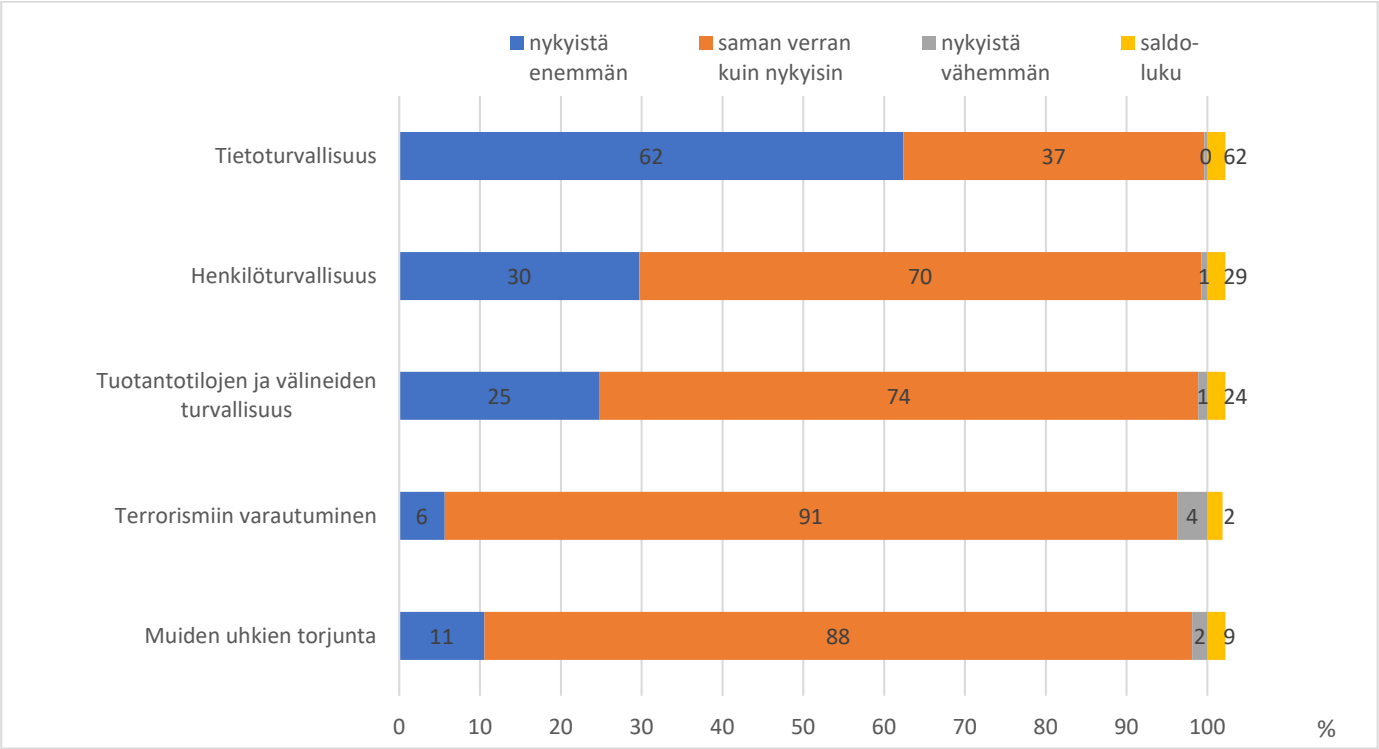
Yritysturvallisuus osana vuotuista budjetti- ja toimintasuunnittelua

On vaikea nähdä yrityksen kehittävän yritysturvallisuutta pitkäjänteisesti jos yritys ei liitä yritysturvallisuutta osaksi yrityksen muuta vuotuista toiminnan suunnittelu- ja rahoitusprosessia. Toiminta ja resurssien suuntaaminen on tällöin helposti lähes sattumanvaraista ja tehotonta. Ohjaavina tekijöinä ovat helposti tapahtuneet poikkeamat ja vahingot eikä ennalta estävään työhön välttämättä panosteta lainkaan.

Kaikista vastanneista yrityksistä 41 prosenttia oli kytkenyt yritysturvallisuuden osaksi vuotuista suunnittelua. Eri toimialoilla osuudet vaihtelivat seuraavasti: teollisuus (50 %), ”muiden alojen” vastaajat (44 %), palveluala (43 %), kaupan ala (29 %) ja rakennusala (20 %).

8 TURVALLISUUSPANOSTUKSET JATKOSSA

Mitä turvallisuuden osa-aluetta yritykset tulevat painottamaan jatkossa?



Kyselyyn vastanneet yritykset arvioivat tulevaisuuden painopisteitä turvallisuuden kehittämisessä. Yritysturvallisuuden kehittämisessä seuraavia osa-alueita tullaan painottamaan aiempaa enemmän:

1. Tietoturvallisuus 62 prosenttia kaikista vastaajista
2. Henkilöturvallisuus, 30 prosenttia kaikista vastaajista
3. Tuotantotilojen ja –välineiden turvallisuus, 25 prosenttia kaikista vastaajista

Kuten aikaisemmissa kyselyissä myös tässä kyselyssä turvallisuuden kehittäminen painottuu tietoturvallisuuteen. Yritykset tiedostavat liiketoimintansa olevan tietojärjestelmistä riippuvaista. Kaksi kolmasosaa (62 %) kaikista vastaajayrityksistä vastasi, että tietoturvallisuuteen panostetaan yrityksessä jatkossa nykyistä enemmän. Kolmasosa (37 %) pitää panostukset nykyisellä tasolla.

Henkilökunnan turvallisuudesta huolehtiminen on osa vastuullisen työnantajan toimintaa. Lähes kaikki yritykset pitävät panostuksensa vähintään entisellä tasolla. Seitsemän kymmenestä (70 %) yrityksestä aikoo panostaa henkilöturvallisuuteen saman verran kuin nykyisin ja kolmasosa (30 %) nykyistä enemmän.

Yritykset osaavat huomioida omaisuuteen kohdistuvan rikollisuuden uhan toiminnalleen ja varautua siihen. Tuotantotilojen turvallisuus pysyy keskeisellä sijalla turvallisuuden kehittämisessä. Kolmasosa (33 %) kaikista yrityksistä aikoo lisätä siihen resursseja ja kaksi kolmasosaa (66 %) aikoo jatkaa samalla tasolla. Osuus on hieman keskimääräistä alempi (30 %) pienissä yrityksissä ja keskimääräistä suurempi (42–43 %) keskisuurissa ja suurissa yrityksissä. Tuotantotilojen turvallisuuteen panostaa nykyistä enemmän 42 prosenttia rakennusalan yrityksistä, 38 prosenttia teollisuusyrityksistä, 32 prosenttia palvelualan yrityksistä ja 23 prosenttia kaupan alan yrityksistä.

Kaikista yrityksistä kuusi prosenttia vastasi, että yritys aikoo varautua nykyistä enemmän terrorismiin tulevaisuudessa. Terrorismista on viimeisten vuosien aikana tullut riski, jonka vaikutukset voivat kohdistua yritykseen kansainvälisen toiminnan ja liikematkustamisen lisäksi myös kotimaan toiminnoissa.

Kymmenesosa (11 %) yrityksistä ilmoitti varautuvansa entistä enemmän turvallisuuden kehittämisessä muihin turvallisuuden kehittämisen osa-alueisiin.

9 KORONAN VAIKUTUKSET LIIKETOIMINNAN JATKUVUUDENHALLINTAAN

Jatkuvuussuunnittelun merkitys yrityksen toiminnalle

Jatkuvuussuunnittelun tavoitteena on turvata liiketoiminnan nopea käynnistäminen häiriöiden ja poikkeustilanteiden jälkeen ja vähentää niistä aiheutuvia haitallisia vaikutuksia. Jatkuvuussuunnittelulla varaudutaan mahdollisiin ongelmatilanteisiin kuten tietojen tai toimitilojen osittaiseen tai täydelliseen tuhoutumiseen tai avainhenkilöiden yllättävään menettämiseen. Toiminnan jatkuvuuden varmistamisessa keskeisessä asemassa ovat luotettavat yhteistyökumppanit, järjestelmien varmentaminen ja varajärjestelmät.

Tosiasia on, että koronapandemian tapainen uhka jatkuvuudelle pitää sisällään tekijöitä, joihin yritykset eivät voi etukäteen tai laisinkaan varautua jatkuvuussuunnittelun keinoin. Jos asiakkaat eivät saa matkustaa tai heitä kehotetaan olemaan matkustamatta, ei tällaiseen valtiovallan toimeen voi varautua etukäteen. Jos taas toiminta laillisesti suljetaan valtiovallan toimesta, ei tähänkään ole minkäänlaisia työkaluja käytettävissä. Pandemian tuoma lomautus ja työttömyys rajaa kotitalouksien käytössä olevaa varallisuutta ja tällä on vaikutusta kulutukseen ja kun se osuu yritykseen, ei sillä tässäkään tilanteessa ole mahdollisuuksia etukäteiseen varautumiseen.

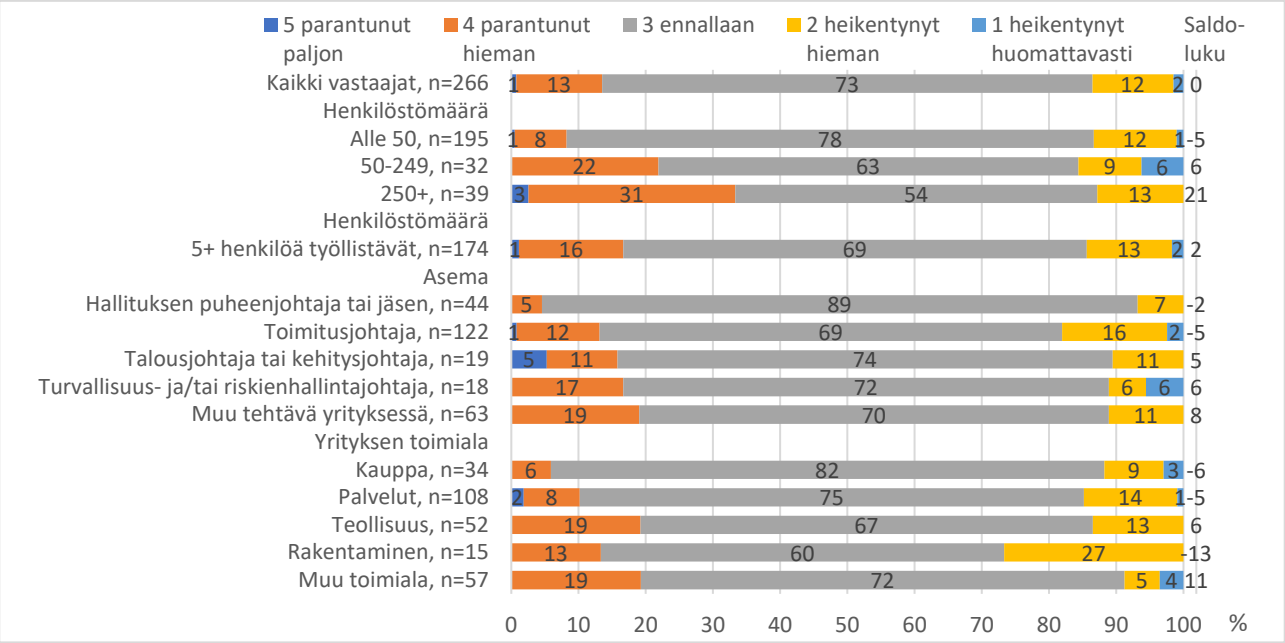
”Meidän osaltamme huolto on vähentynyt Suomessa ja vienti on sakannut pahasti.”

”Kysynnän ja liikevaihdon romahtaminen.”

”Viivästykset toimittajien tuotteissa koronasta johtuen.”

Turvallisuustilanteen kehitys koronan aikana

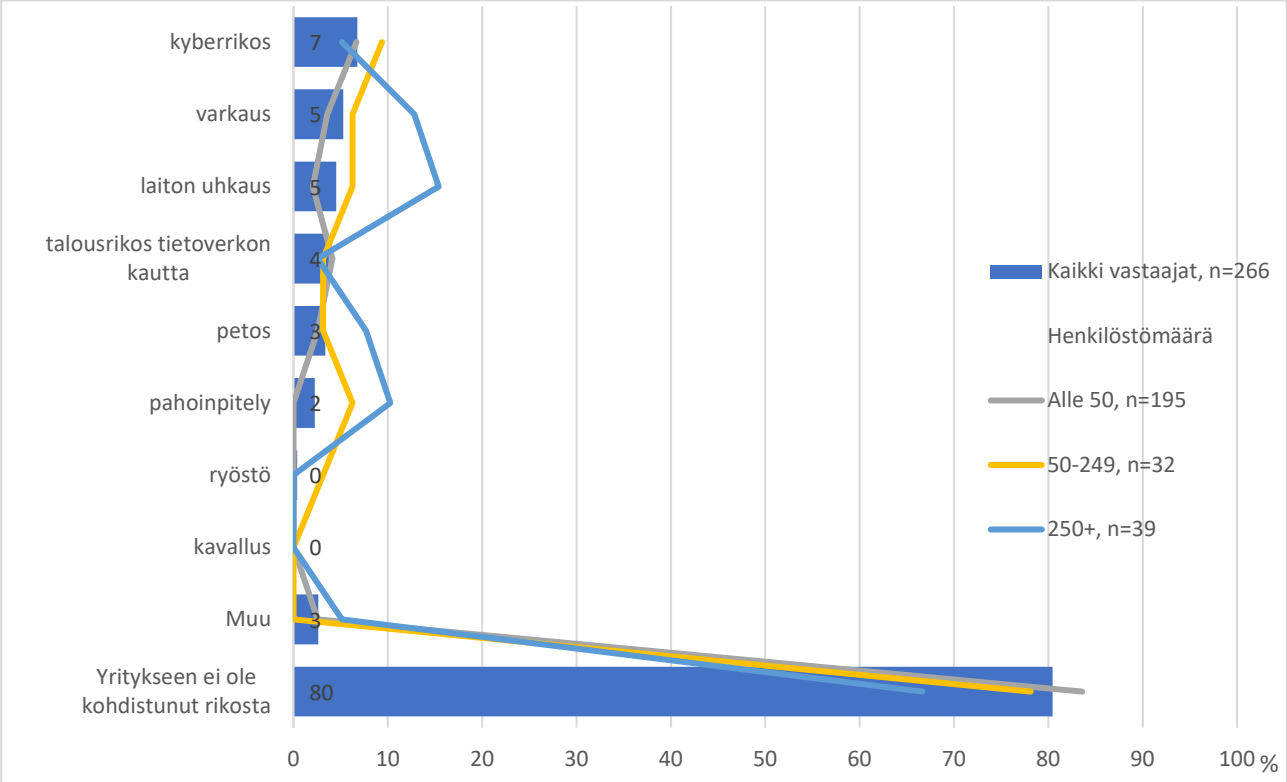
Onko yrityksenne turvallisuustilanne koronan aikana...



Kysyttäessä koronan vaikutuksista yritysten turvallisuustilanteeseen, 14 prosenttia kaikista vastaajista vastasi tilanteen heikentyneen vähintään hieman. Suurista ja pienistä vastaajista 13 prosenttia ja keskisuurista 14 prosenttia koki huonontuneen.

Valtaosa kaikista vastaajista (73 %) ei havainnut tilanteen muuttuneen huonommaksi tai parantuneen. Suurista vastaajista 34 prosenttia ja keskisuurista 22 prosenttia koki turvallisuustilanteen parantuneen. Syytä voi arvailla, mutta eräs selittävä tekijä voi olla etätyön lisääntyminen. Sitä kautta henkilöihin kohdistuvat ja henkilöistä johtuvat turvallisuusriskit ovat vähentyneet.

Korona-aikana yritykseen/työntekijöihin kohdistuneet rikokset

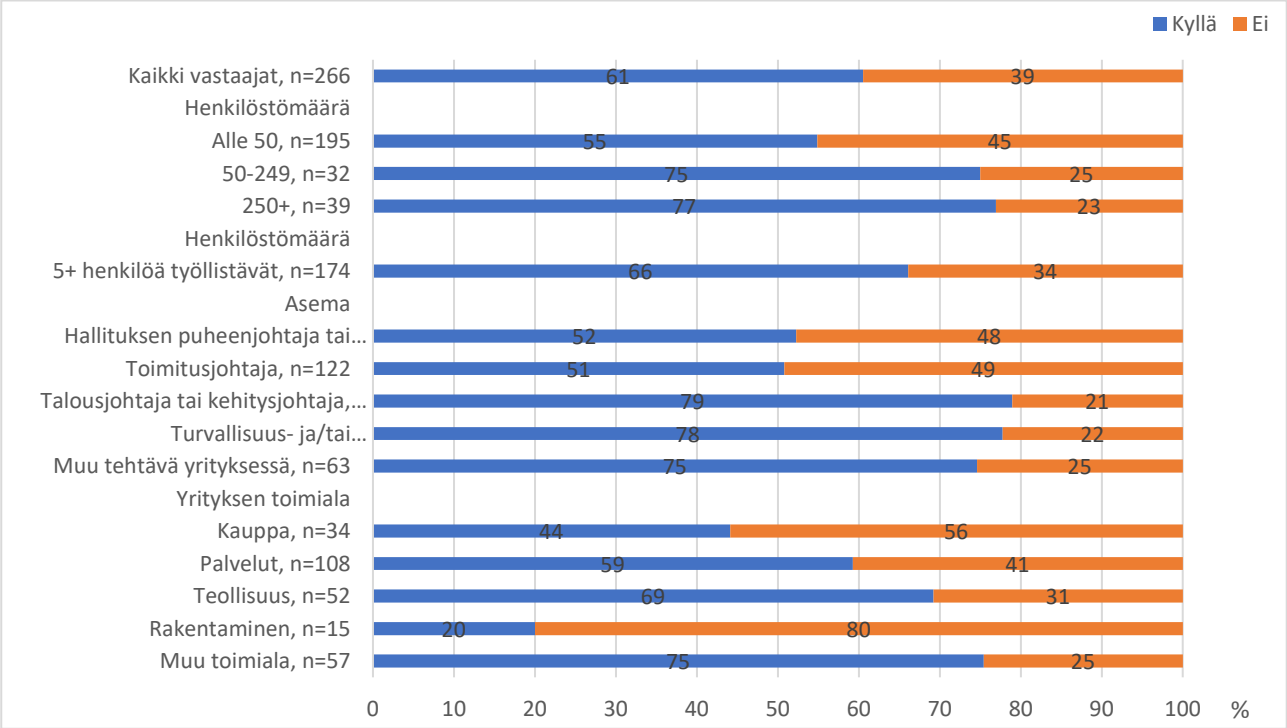


Yrityksiltä kysyttiin yritykseen ja sen työntekijöihin kohdistuneista rikoksista, jotta selvitykseen saadaan kuva siitä, millaisia rikoksia korona-aikaan tapahtuu ja onko niissä jotain korona-ajalle ominaista suuntausta. Yleisin vastaus (80 %) oli, yritykseen tai sen työntekijöihin ole korona-aikana kohdistunut rikosta. Suurien vastaajayritysten keskuudessa nousivat varkaudet, laittomat uhkaukset ja pahoinpitelyt muita vastaajia selkeämmin esille.

1. Kyberrikokset oli yleisin korona-ajan rikos. Kaikista vastaajista seisemän prosenttia vastasi **kyberrikoksen** kohdistuneen yritykseen. Katsottaessa eri ammattiryhmien vastauksia, turvallisuus- ja riskienhallintajohtajien keskuudessa niitä pidetiin kaikkein yleisimpänä rikosten ryhmänä,
2. Toiseksi yleisimmät rikokset vastaajien keskuudessa olivat **varkaudet ja laittomat uhkaukset**, kaikista vastaajista viisi prosenttia kertoi varkauden tai laittoman uhkauksen kohdistuneen yritykseen tai sen työntekijöihin. Suurista vastaajista 13 prosenttia vastasi varkauden ja 15 prosenttia laittoman uhkauksen kohdistuneen yritykseen tai sen työntekijöihin.
3. Seuraavaksi yleisimpänä rikoksena erottautui talousrikos tietoverkon **kautta tehtynä. Erilaiset verkon kautta tehdyt petokset ovat viime vuosina lisääntyneet**, joten on luonnollista että ne ovat näkyvillä myös tässä selvityksessä. Kaikista vastaajista neljä prosenttia kertoi tällaisen rikoksen tapahtumisesta.

Yritystoiminnan jatkuvuutta korona-aikana tukevat toimenpiteet

Onko vastaaja panostanut etätyön tietoturvallisuuteen?



Tänä vuonna etätyö yleistyi Suomessa eniten koko Euroopassa. Se on osoitus suomalaisen tietoliikenneinfran kapasiteetista ja työntekijöiden sopeutumiskyvystä. Kaikista vastaajista 39 prosenttia ei kuitenkaan ollut panostanut etätyön turvallisuuteen. Yllättävää on että suurista vastaajista 23 prosenttia ja keskisuurista 24 prosenttia olivat laiminlyöneet etätyön turvallisuuteen. Näillä vastaajilla on eniten työntekijöitä ja sen myötä määrällisesti eniten etätyön tekijöitä. Jokainen uusi etätyöyhteys on käytännössä uusi mahdollinen hyökkäyskanava yrityksen tietoverkkoon.

”Työntekijöillä oikeus käyttää vain yrityksen tietokonetta, kaikissa siirrettävissä laitteissa on salasanat.”

”Suojatut serveriyhteydet”

”Pöytäkoneiden kryptaus (koska vietiin kotiin etäkonttorille), tiheämpiä salasanan vaihtoja.”

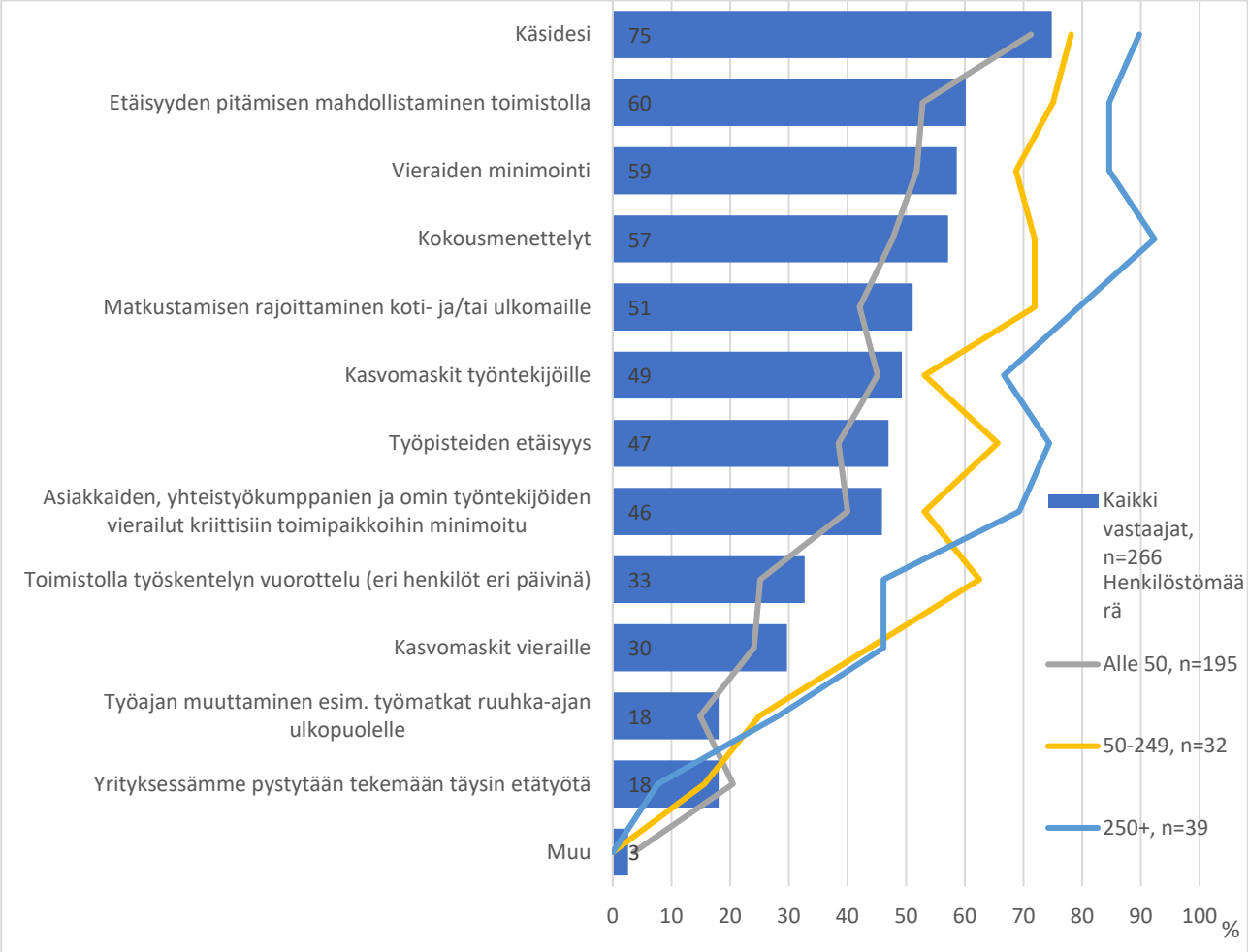
”Käytettävät laitteet, tietokoneet ja puhelimet ovat etähallinnan piirissä, kaikki data kulkee salattuna jo työntekijän koneelta lähtien, säännöllinen henkilöllisyyden lisävarmennus kirjauduttaessa. Lisäksi etäyhteys kuvan kanssa varmistaa kirjautuneen henkilöllisyyden lähes päivittäin.”

”Työtiedostoihin pääsee käsiksi vain suojatun VPN-yhteyden kautta. Kaikki henkilökunnan jäsenet ovat suorittaneet etätyöaikana cyber-turvallisuuskoulutuksen. Meillä on yleiset tietoturvaohjeet, jotka sisältävät myös ohjeet etätyöskentelyä varten.”

”Tietokoneilla, palvelimilla ja pilvessä tapahtuvasta liikenteestä kerätään yhteen paikkaan lokit ja analysoidaan SIEM-järjestelmällä. Epäilyttävät poikkeamat aiheuttavat automaattisia kirjautumiskieltoja ja muita toimenpiteitä. Lisätty tietoturvakoulutusten määrää ja tehostettu sisäistä uutisointia Kyberturvallisuuskeskuksen tiedotteista ja havainnoista. Jatkuvuus turvattu varajärjestelmillä ja varmuuskopioilla.”

”Tietokoneelle ei tallenneta mitään vaan kaikki tieto on pilvipalveluissa tai etäpalvelimilla. Tietokoneen katoaminen tai varastaminen ei aiheuta tietojen katoamista koneen mukana. Palomuurit ja muutenkin tietoturvallisuus yhtä hyvät myös kotona.”

Mikäli yrityksessänne ei täysin voida tehdä etätyötä, miten olette varautuneet koronaan ja varmistamaan liiketoiminnan jatkuvuuden?



Havaintoja yritysten käyttämistä keinoista torjua ja pienentää koronatartunnan vaaraa.

Vastaukset on annettu lokakuussa, jolloin koronan toinen aalto on ollut käynnissä. Kysymykset on laadittu tarkastuslistan tyyliin, kun ne käy läpi, saa hyvän kuvan siitä mitä kannattaisi tehdä ja mitä on tehty. Lähes viidesosa (18 %) kaikista vastaajayrityksistä voi tehdä täysin etätyötä. Suurista vastaajayrityksistä tämä on mahdollista vain kahdeksalla prosentilla.

1. Kolme neljäsosaa kaikista vastaajista kertoi **että ne käyttävät käsidesiä** torjuntakeinona.

2. Kaikista vastaajista 70 prosenttia **oli varannut kasvomaskeja** vierailijoille.

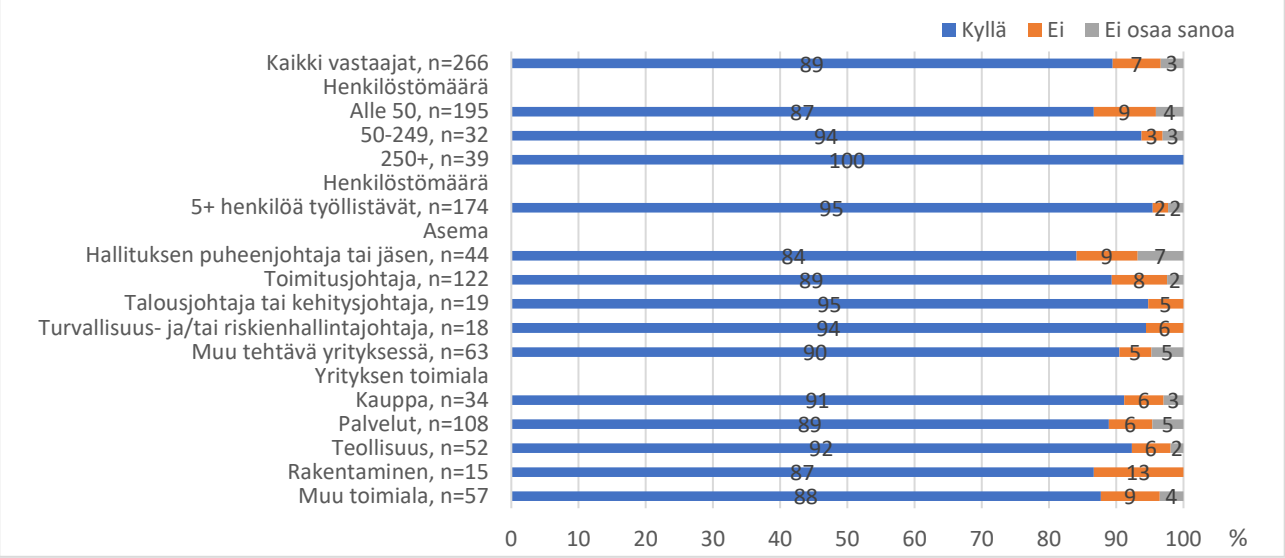
3. Viidesosa (18 %) kaikista vastaajista oli muuttanut työaikoja niin, että **työmatkat voidaan tehdä ruuhka-aikojen ulkopuolella.**

4. Kolmasosa (33 %) *on* **luonut työntekijöistä rotaatioryhmiä,** jotka työskentelevät toimistolla esimerkiksi eri päivinä.

5. Puolet (49 %) vastaajista on hankkinut **kasvomaskeja työntekijöille.**

Onko yrityksenne turvallisuustilanne koronan aikana...

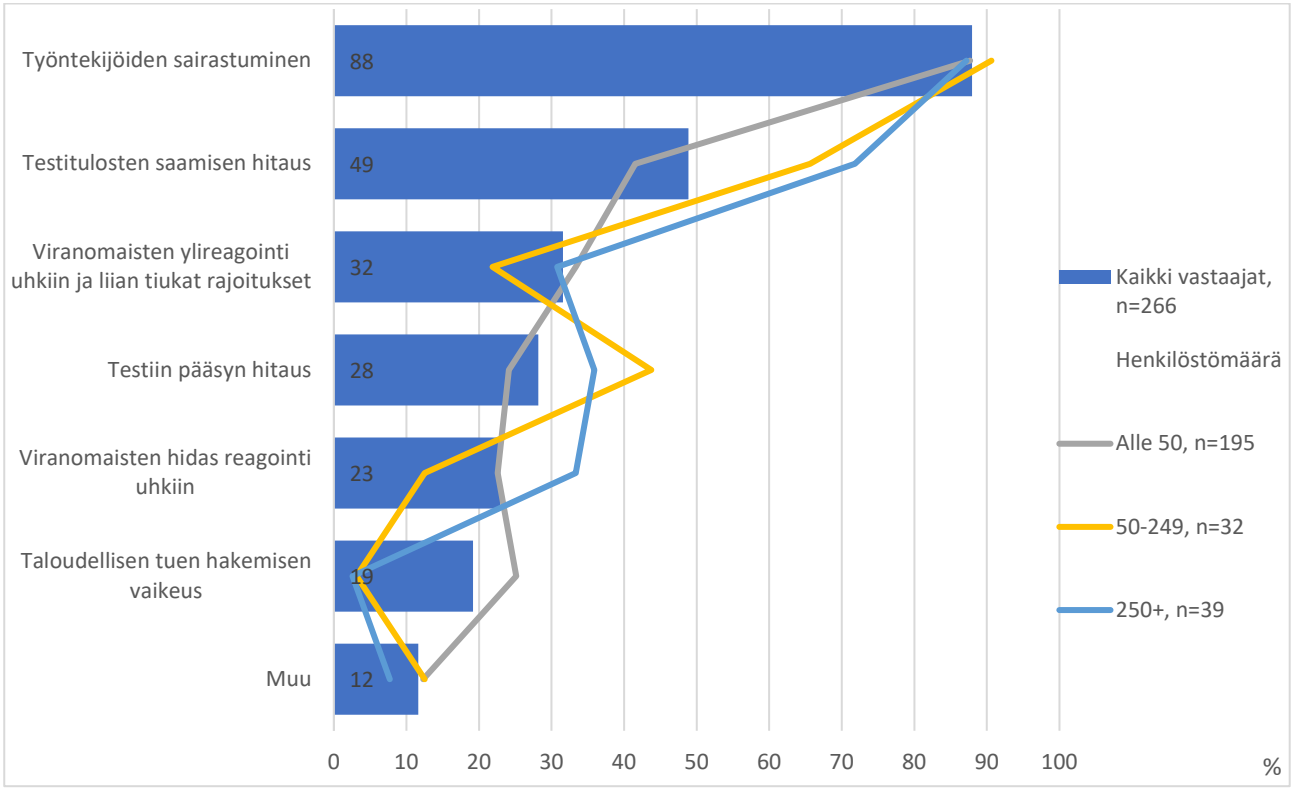
Onko yrityksessä selkeät ohjeet sairastumisen varalta



Kysyttäessä yrityksen selkeistä ohjeista sairastumisen varalle, 89 prosenttia vastaajista kertoi niillä olevan sellaiset. Koronan myötä tämän ohjeistuksen tarpeellisuutta ei tarvitse enää perustella. Arvioitaessa kaikkien eri vastausluokkien vaihteluväliä 81 -100 prosenttia, ei tilanteessa ole havaittavissa erityisiä huolenaiheita.

Koronan aiheuttamat uhat yritysten jatkuvuudelle

Mikä koronatilanteessa uhkaa eniten jatkuvuutta?



”Koronatilanteen taloudelliset vaikutukset asiakasyrityksiimme.”

”Asiakasyritysten rajoitukset, emme pääse tekemään työtämme.”

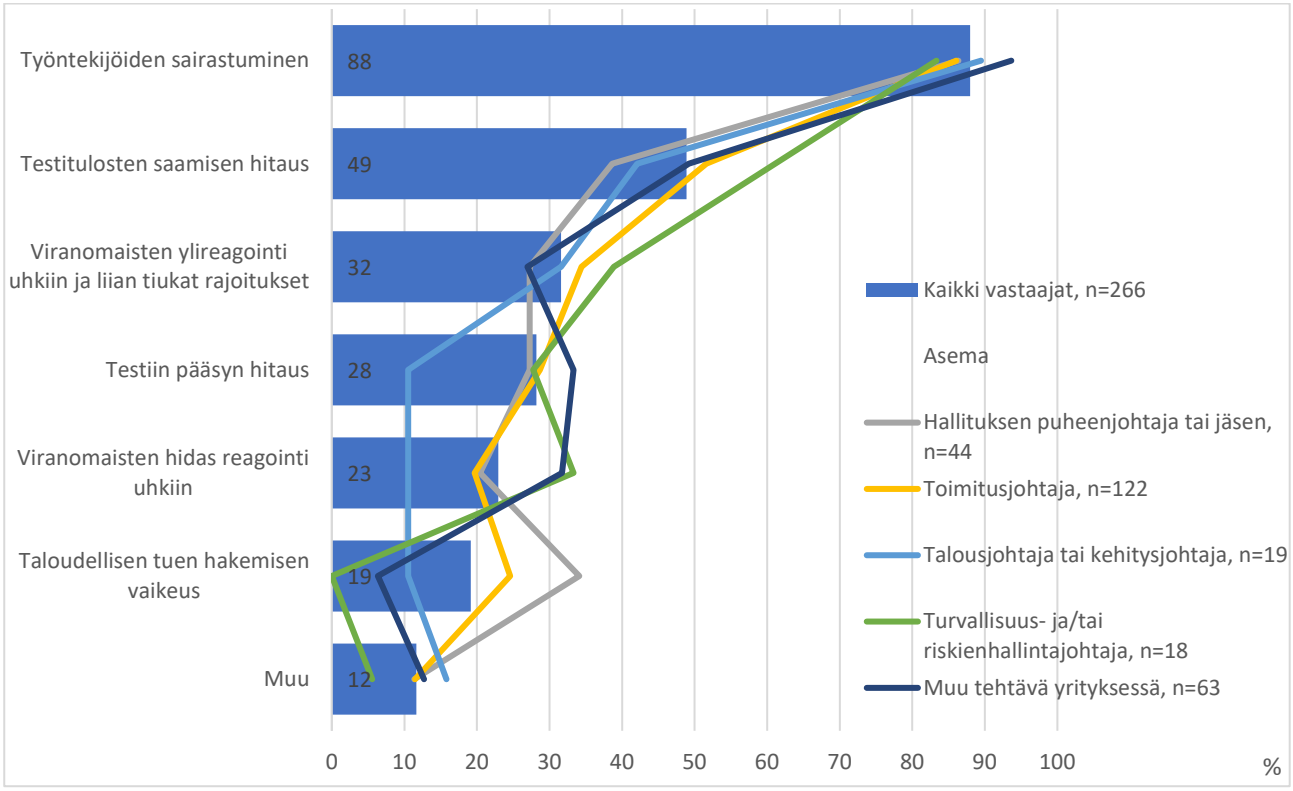
”Viranomaisohjeiden yleinen tulkinta alalla työelämässä.

”Ennalta-arvaamattomat vaikutukset yrityksen asiakkaiden talouteen, "investointi-lama.”

Kaikista vastaajista valtaosa (88 %) piti työntekijän sairastumista suurimpana uhkana yrityksen jatkuvuudelle. Pandemia uhkana yrityksen jatkuvuudelle kohdistuu yritykseen yksilön terveyden kautta, joten on luonnollista sen olevan uhkien kärkipäässä. Seuraavaksi suurimpana uhkana (49 %) pidettiin testitulosten saamisen hitautta. Kirjoitettaessa selvitystä (marraskuu 2020) tämä tilanne on julkisudessa olevien tietojen perusteella kuitenkin parantunut syys-lokakuusta, jolloin vastauksia annettiin.

Kolmanneksi suurin uhka (32 %) yritysten mielestä oli viranomaisten ylireagointi ja liian tiukat rajoitukset. Neljänneksi yleisin (28 %) uhka oli testeihin pääsyn hitaus, mutta tämänkin osalta tilanne on parantunut huomattavasti vastausten antamisajankohdasta.

Taloudellisen tuen hakemisen vaikeutta piti uhkana viidesosa (19 %) kaikista vastaajista. Pienien vastaajayritysten keskuudessa 25 prosenttia koki näin ja ammattiryhmien keskuudessa hallitusten puheenjohtajien ja jäsenien (34 %) ja toimitusjohtajien (24 %) keskuudessa vastattiin näin.



"Yksi osasto suljettiin karanteeniin, koska ei pystytty jäljittämään altistumisia tarkkaan."

"Työntekijöiden perheiden koronan aiheuttama karanteeni."

"Vientiyrityksenä myyntimme kärsii matkustamisen mahdottomuudesta ja messujen peruuttamisesta."

"Kysynnän romahtaminen viranomaisten sulkutoimenpiteiden ja etätyön voimakkaan kasvun ansiosta."

"Viranomaispäätösten vaikutus liiketoimintaan:"

Kaikista vastaajista 88 prosenttia on huomioinut työntekijän sairastumisen tai karanteeniin joutumisen aiheuttaman riskin. Tartuntojen lisääntyessä maassamme, tulevat myös karanteenit lisääntymään. Mikäli karanteeniin joutuvat henkilöt ovat läsnätyöntekijöitä ja tartunnan saanut on tehnyt töitä heidän kanssaan, voi yritys kohdata kovia haasteita etsiessään korvaavia työntekijöitä, jos se ei ole tehnyt työntekijöistä eri päivinä tai vuorokauden aikoina työskenteleviä rotaatioryhmiä.

Kaikista vastaajista 43 prosenttia kertoi varautuneensa asiakkaiden sairastumiseen tai karanteeniin joutumiseen. Mahdollisuudet varautumiseen ovat rajallisia, mutta esimerkkinä verkkokaupan ja asiakkaalle toimittamisen lisääminen vähentävät haitallisia vaikutuksia liiketoiminnalle. Oman henkilökunnan suojaaminen maskeilla ja käsidesien tarjolla pitäminen vähentävät tartuntariskiä.

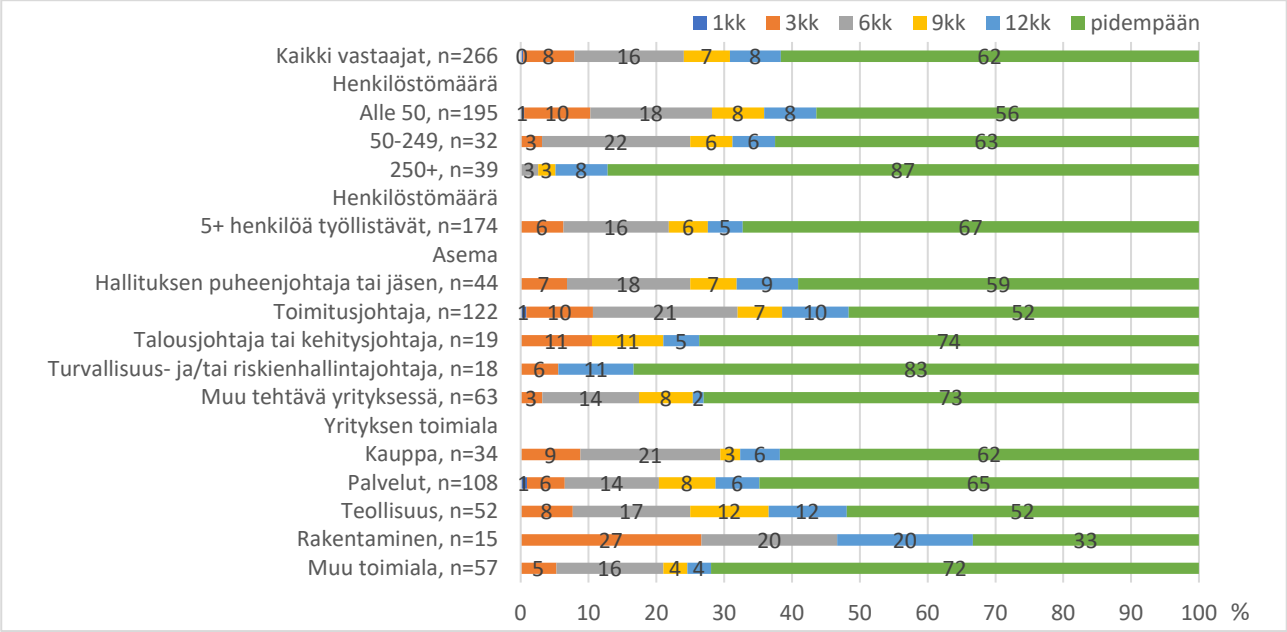
Lähiomaisten sairastumiseen tai karanteeniin joutumiseen oli varautunut 39 prosenttia vastaajista. Tässä yksinkertaisin varautumisen tapa on mahdollistaa etätyö. Alihankkijoiden sairastumisen tai karanteeniin joutumisen oli huomioinut 36 prosenttia vastaajista.

Huomion arvoista on, että suuri määrä yrityksiä ei ole huomioinut sairastumisen tai karanteeniin joutumisen aiheuttamaa riskiä liiketoiminnalle:

- asiakkaiden osalta 57 prosenttia
- lähiomaisten osalta 61 prosenttia
- alihankkijoiden osalta 64 prosenttia

Mikäli tartuntamäärät tulevat lisääntymään merkittävästi, tulee sairastumisten ja karanteeniin joutumisten vaikutus liikatoiminnalle lisääntymään. Yhdistettynä taloustilanteen aiheuttamaan konkurssiriskiin, voi tällä on vakavia seurauksia yrityksen toiminnan jatkuvuudelle.

Miten pitkään yrityksen toiminnan jatkuvuus/resilienssi kestää pandemian jatkumista



”Kriittisillä aloilla toimivien asiakkaiden konkurssi.”

”Avustusten epäoikeudenmukaisuus, koska yritystukea sai vain verohallinnon toimialaluokittelun mukaisesti, joten monet tilanteesta paljon kärsineet eivät voineet tukea hakea mistään.”

Tätä kysymystä arvioitaessa on pidettävä mielessä, että vastaukset on annettu syys-lokakuussa. Kaikista vastaajista neljäsosa (24 %) ilmoitti pandemian jatkuessa tällaisena yrityksen jatkuvuuden/resilienssin päättyvän maksimissaan kuuden kuukauden kuluessa. Tämä tarkoittaa että merkittävä määrä yrityksiä on ajautunut konkurssiin maalis-huhtikuuhun 2021 mennessä. Kesään 2021 mennessä tämä määrä on jo yhteensä 31 prosenttia.

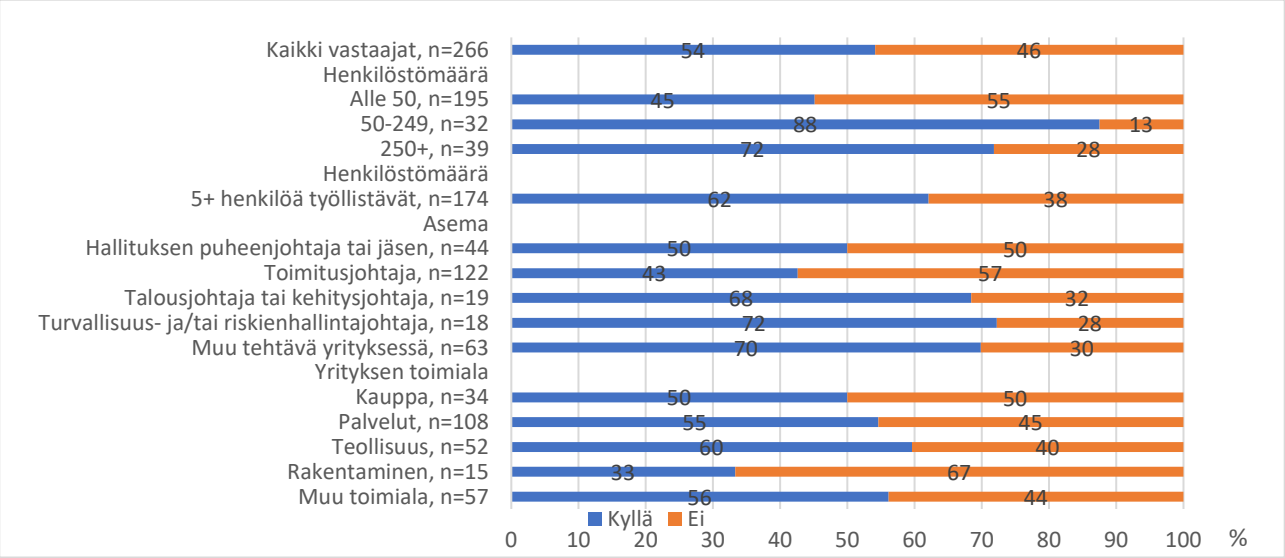
Toimitusjohtajista 32 prosenttia vastasi jatkuvuuden kestävän maalis-huhtikuuhun 2021 ja 42 prosenttia kesään 2021 saakka. Hallituksen puheenjohtajista ja jäsenistä 25 prosenttia vastasi jatkuvuuden kestävän maalis-huhtikuuhun 2021 ja 32 prosenttia kesään 2021 saakka.

Kaupan alalla liiketoiminnan jatkuvuus loppu 30 prosentilla maalis-huhtikuuhun mennessä. Teollisuudessa käy samoin 25 prosentille vastaajista ja palvelualalla 21 prosentille vastaajista.

Kun pandemia ei selvästikään ole väistymässä, tarve taloudelliselle tuelle on selvä. Tätä arvioitaessa kannattaa huomioida, että taloudellisen tuen hakemisen vaikeutta piti uhkana liiketoiminnan jatkuvuudelle 34 prosenttia hallitusten puheenjohtajista ja jäsenistä ja 24 prosenttia toimitusjohtajista. Tuen hakemisen tulee olla helppoa ja nopeaa.

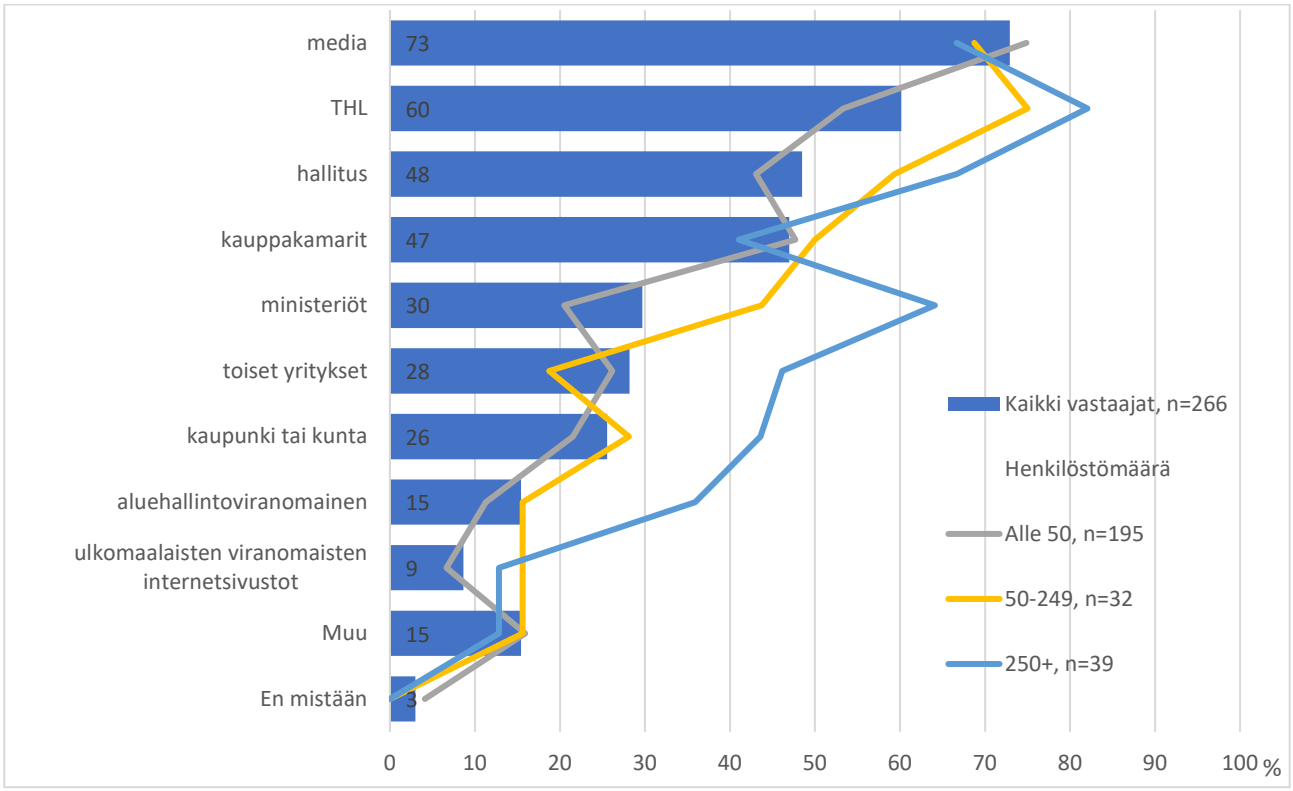
Tiedonsaanti koronaan liittyen

Onko yritys saanut hallitukselta ja viranomaisilta niin selkeää tietoa, jonka nojalla on voinut asianmukaisesti varautua koronaan ja turvata liiketoiminnan jatkuvuuden?



Tiedon saaminen erityisesti pandemian osalta on tärkeää. Tilannetta ei helpota tarjolla oleva disinformaatio ja massat tavoittava oletuksiin perustuva some-viestintä. Vain hieman yli puolet (54 %) kaikista vastaajista kertoo saaneensa selkeää tietoa, jota voinut käyttää koronaan varautumiseen ja liiketoiminnan jatkuvuuden turvaamiseen. Tilanne on huonoin (45 %) pienten vastaajien keskuudessa. Oli syy mikä tahansa, suuri määrä yrityksistä ei ole saanut tarvittavaa tietoa.

Mistä yritys on saanut tietoa koronan vaikutuksista yritystoimintaan



”Viranomaisohjeiden yleinen tulkinta alalla työelämässä epäselvää.”

Tiedon luotettavuuden merkitys on ensisijaisen tärkeää etenkin kriisitilanteessa. Yritysten saatavilla tulisi olla selkeää viranomaistietoa, joka ei ole ristiriidassa muun viranomaisviestinnän kanssa,. Tässä kysymyksessä ei kysytty mistä luotettavaa ja hyvälaatuista tietoa on saatu, vaan sitä mistä yleensä tietoa on saatu ja käytännössä myös haettu.

Kaikista vastaajista 73 prosenttia oli saanut tietoa koronan vaikutuksista liiketoimintaan median kautta. Media on luonnollinen tiedonlähde, mutta kaikki sen välittämä tieto ei ole viranomaisviestintää.

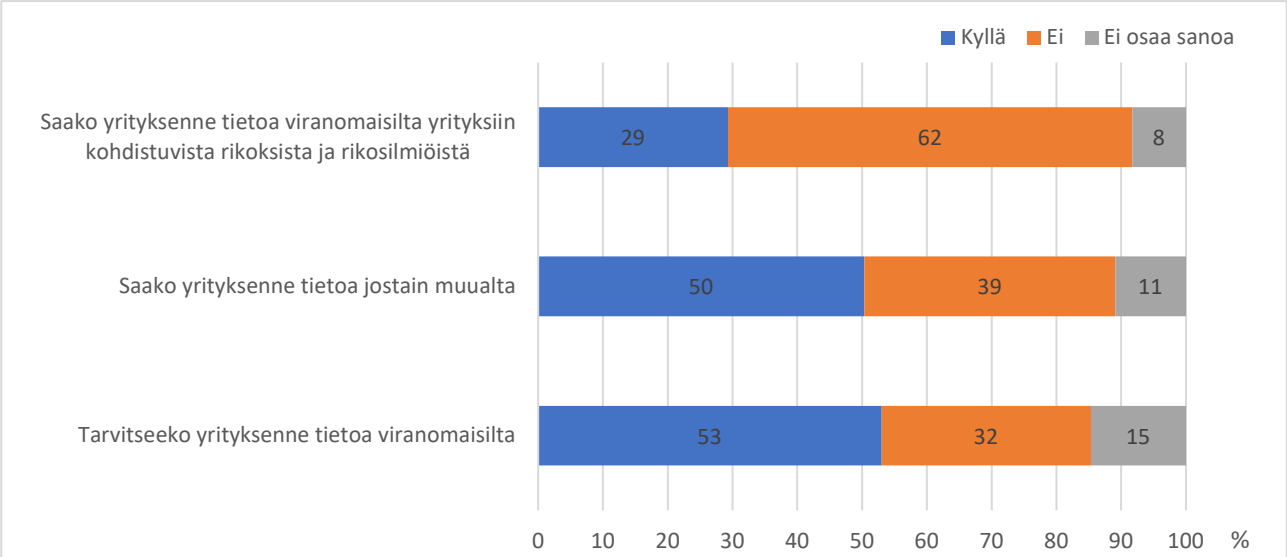
Kaikista vastaajista 60 prosentin tiedonlähteenä on ollut THL. Suurten vastaajien keskuudessa jopa 82 prosenttia on saanut tietoa sieltä.

Kaikista vastaajista lähes puolen (48 %) tiedon lähteenä on ollut hallitus. Kaksi kolmasosaa (67 %) suurista vastaajista on saanut tiedon hallituksen viestinnästä.

Kaikista vastaajista 47 prosenttia on saanut tietoa kauppakamareilta. Ministeriöt ovat olleet kolmasosan (30 %) tiedon lähteenä. Suurista vastaajista kaksi kolmasosaa (64 %) on saanut tietoa ministeriöiden viestinnästä.

10 TIEDONSAANTI RIKOSILMIÖISTÄ

Yritysten rikosriskeihin liittyvä tiedonsaanti ja tarve saada tietoa



Kaikista vastanneista yrityksistä lähes kolmasosa (29 %) sai tietoa rikoksista ja rikosilmiöistä viranomaisilta. Suurin osa (62 %) vastaajasta ilmoitti, ettei ole saanut tietoa viranomaisilta rikoksista ja rikosilmiöistä.

Puolet kaikista kyselyyn vastanneista yrityksistä (50 %) oli saanut tietoa rikosilmiöistä muuta kautta. Merkittävä osa (39 %) vastaajista ei ollut kuitenkaan saanut tietoa muistakaan lähteistä.

Vastanneilta yrityksiltä kysyttiin, onko yrityksellä tarvetta saada viranomaisilta tietoa rikoksista ja rikosilmiöistä. Yli puolet kaikista yrityksistä (53 %) ilmoitti tarvitsevansa tietoa viranomaisilta. Vain kolmasosa (32 %) kaikista vastaajista ei tarvinnut tietoa viranomaisilta.

11 TARKISTUSLISTAT RISKIENHALLINNAN TUKENA

1. Ihmisiin liittyviin rikosriskeihin ja väärinkäytöksiin varautuminen

- Työväkivallan vähentäminen: työtilan järjestelyt ja tekniset suojaus- ja hälytysjärjestelmät, henkilökunnan koulutus ja ohjeistus väkivaltatilanteiden hallitsemiseksi ja välttämiseksi, turvalliset toimintatavat, riskien tunnistaminen ja riskinäkökulmien huomioonottaminen, uhkatilanteen jälkiselvittely ja uhrin auttaminen
- Turvallisuusasiat osaksi perehdyttämiskoulutusta
- Työntekijöiden turvallisuuskoulutus
- Turvallisuuskulttuurin luominen ja ylläpitäminen
- Työntekijöiden kannustaminen kertomaan havaitsemistaan turvallisuuspuutteista
- Avainhenkilöille on varamiesjärjestelmä
- Henkilötietojen suojaus
- Kriisiviestintäsuunnitelma
- Matkustamisen turvallisuusohjeet

- Taustaselvitykset (ml. referenssien tarkistaminen) työntekijöistä
- Taustaselvitykset avainhenkilöistä
- Yhteistyökumppanien luotettavuusselvitykset
- Asiakkaiden luottokelpoisuusselvitykset
- Alihankkijoiden referenssien tarkastaminen
- Kaikki sopimukset kirjallisina
- Avainhenkilöiden salassapitositoumus
- Kilpailukieltosopimus tarvittaessa (lain rajoitukset)
- Tehtävienmukaiset pääsy- ja kulkuoikeudet

2. Tietoon liittyviin rikosriskeihin ja väärinkäytöksiin varautuminen

- Tiedon tekniset suojauskeinot (palomuuri, virustorjunta, ajantasainen käyttöjärjestelmä, varmuuskopiointi, palvelimet)
- Tietojen luokittelu
- Liike- ja ammattisalaisuuksia koskeva luokittelu- ja käsittelyohje
- Henkilökunnan koulutus salaisten / luottamuksellisten tietojen käsittelyyn
- Ohjeet viranomaisten ja yhteistyökumppanien luovuttamille luottamuksellisille asiakirjoille ja tiedoille
- Varautuminen siihen, että yritys voi olla yritysvakoilun kohteena

3. Tuotanto- ja toimitilojen suojaaminen

- Eriytetyt tuotanto-, toimisto – ja tuotekehitystilat
- Murtohälytys
- Kulunvalvonta
- Videovalvonta
- Vierailujen ohjeistus
- Vartiointi
- Henkilöstön koulutus
- Valvontajärjestelmien säännöllinen toimivuustestaus
- Varalaitteet keskeisten tuotantoprosessien turvaamiseksi

4. Irtaimen omaisuuden suojaus

- Omaisuusrekisteri
- Turvamerkintä
- Kameravalvonta
- Lukitusmekanismi (esimerkiksi pulttaus, vaijeri)
- Säilytys erillisessä lukitussa tilassa tai kassakaapissa
- Kuljetusohjeet

5. Toimintaan kohdistuvat rikokset ja väärinkäytökset

- Kirjalliset sopimukset yhteistyötahojen kanssa, yhteistyökumppanin luotettavuuden arvioiminen
- Asiantuntijat tarkastavat sopimustekstit
- Asiantuntijoiden laatimat sopimuspohjat
- Yrityksen johto tarkistaa merkittävimmät liiketoimintasopimukset
- Epätavallisen hävikin seuranta ja hävikin syiden selvittäminen
- Talousrikoksien torjunta: vaarallisten työyhdistelmien välttäminen, ammattitaitoinen tilintarkastus, sisäinen valvonta ja tarkastus, eettiset ohjeet, auditointi sekä luotettavat työntekijät

6. Yrityksen turvallisuusjohtaminen

- Yrityksen johto osallistuu henkilökohtaisesti turvallisuuden kehittämiseen
- Turvallisuusasioita käsitellään henkilöstön kanssa
- Työntekijät voivat vaikuttaa turvallisuutta koskevaan päätöksentekoon
- Yrityksen eri osastot/toimialat tekevät yhteistyötä turvallisuusasioissa
- Yrityksen riskien säännöllinen arvioiminen riskikartoituksen avulla, toimenpiteet riskien vähentämiseksi ja toimenpiteiden seuranta.
- Yrityksellä on toimintaohje poikkeustilanteita varten
- Yritysturvallisuus on osa yrityksen vuotuista strategiasuunnittelua ja budjetti- ja toimintasuunnittelua
- Turvallisuus on osa yrityksen toiminta- tai laatujärjestelmää

7. Jatkuvuussuunnittelu

- Kaikissa tilanteissa ylläpidettävät kriittiset toiminnot on tunnistettu sekä dokumentoitu kirjallisesti.
- Asiakassopimusten näkökulmasta vähintään kriittisille palveluille/toiminnoille on määritelty suurin sallittu keskeytysaika.
- Mahdolliset liiketoimintaa vakavasti haittaavat tilanteet on tunnistettu ja niiden vaikutukset liiketoiminnalle on arvioitu koko organisaatiossa yhdenmukaisella tavalla.
- Liiketoiminnan jatkuvuuden kehittämistoimet on määritelty ja ne ovat selkeästi vastuutettu sekä niiden toteutusta seurataan.
- Liiketoiminnalle kriittiset ulkoiset palvelu- ja hyödyketoimittajat on tunnistettu ja heidän kanssa on sopimuksissa kuvattu häiriötilanteisiin varautumisen vaatimukset.
- Yrityksellä on ohjeistettu jatkuvuudenhallinnan prosessi / toimintamalli ja ajantasainen jatkuvuussuunnitelma.
- Käytettävissä on selkeä ohjeistettu toimintamalli vakavien häiriötilanteiden johtamiseksi ja hallitsemiseksi.
- Yrityksellä on käytössään kriisiviestintäohje ja ohje on henkilöstön tiedossa.
- Tietojen käyttö häiriötilanteissa on varmistettu säännöllisesti otettavilla varmistus- ja palautusmenettelyillä.
- Tietojärjestelmien käyttö häiriötilanteissa on varmistettu riittävällä palvelukapasiteetilla ja tietoliikenneyhteyksillä.
- Koulutus ja harjoittelu liiketoiminnan häiriöiden varalle on suunnitelmallista ja säännöllistä.
- Varautumisen ja jatkuvuudenhallinnan prosessia / toimintamallia on arvioitu (esim. osana laadunvalvontaa, turvallisuusauditointia, tms järjestelmää).

12 JOHTOPÄÄTÖKSET

Yrityksiin kohdistuvat rikokset ja väärinkäytökset eivät ole vähentyneet – tietoa tarvitaan

Kaikista vastaajayrityksistä 42 prosenttia arvioi, että rikosten ja väärinkäytösten määrä on kasvanut viimeisen kolmen vuoden aikana. Vuosien aikana etenkin suurissa yrityksissä kasvua on tapahtunut paljon. Kun vuonna 2012 lisääntyneistä rikoksista raportoi 34 prosenttia, nyt osuus oli peräti 54 prosenttia. Negatiivinen kehitys on jatkunut jo 15 vuoden ajan, kun ilmiötä on tutkittu kauppakamarien toimesta.

Vaikka viranomaisten tilastoinnin perusteella rikokset yleisesti ovat olleet laskusuunnassa, yrityksiin kohdistuva rikollisuus ei ole vähenemässä. Tilastoista tämä ei kuitenkaan näy ja yksi syy voi olla se, että yritykset eivät enää tee rikosilmoituksia, koska oletuksen on ettei esitutkinta ei johda mihinkään tai se keskeytetään. Tätä oletusta tukee se, että julkisuudessa esitetyt tilastot ja tiedot rikosten selvittämisprosenteista eivät luo luottamusta siihen, että rikosilmoituksen teko kannattaisi. Toinen syy voi olla se, että polisiin rikosilmoitusjärjestelmässä ei saada poimittua yrityksiin kohdistuvien rikosten määriä, vaan jaottelu on vain rikosperusteinen.

Toisaalta yli puolet (53 %) yrityksistä kertoo tarvitsevan turvallisuuteen liittyvää tietoa viranomaisilta. Yritysten on jatkettava ja lisättävä turvallisuutensa kehittämistä ja samanaikaisesti tiedonjakoa viranomaisilta kaivataan tämän työn tueksi.

Yritysten havaitsema yritysvakoilu ja tiedon urkinta lisääntynyt merkittävästi – tietoturvallisuuteen panostetaan

Suurissa yrityksissä 31 prosenttia ja teollisuudessa 21 prosenttia vastaajista kertoi, että näin oli tapahtunut. Vuonna 2017 vain kahdeksan prosenttia vastaajista kertoi yrityksiinsä kohdistuneesta yritysvakoilusta tai tiedon urkkimisesta. Tunnistettu laiton kiinnostus yritysten tietoon on kolmessa vuodessa kaksinkertaistunut.

Kasvusta huolimatta kyse on piilorikollisuudesta, josta suurin osa jää yrityksiltä huomaamatta. Todellinen tapausten määrä on suurempi. Vain puolet (49 %) yrityksistä tunnistaa niillä olevan tietoa, joka voisi kiinnostaa kilpailijoita yritysvakoilun kautta tai olla laittoman tiedustelun kohteena. Yleisimmin tämä rikollista kiinnostava tieto-omaisuus tunnistetaan teollisuuden piirissä (71 %).

Yritykset elävät tiedosta, on se sitten tuotekehitystietoa tai yritysostosuunnitelmiin liittyvää tietoa. Tiedon suojaamisen saralla on yhä paljon parannettavaa alkaen tietoisuuden kehittämisestä. Positiivista kuitenkin on, että yritykset tiedostavat liiketoimintansa olevan tiedosta ja tietojärjestelmistä riippuvaista. Kaksi kolmasosaa (62 %) kaikista vastaajayrityksistä vastasi panostavansa tulevaisuudessa tietoturvallisuuteen enemmän kuin aiemmin.

Kaikki tietoriskit yleistyneet, kerrannaisvaikutukset ankaria

Yritykset arvioivat myös, että yleisesti tietoriskien tilanne on viimeisten kolmen vuoden aikana huonontunut yrityksissä. Näin kertoo yli puolet (54 %) kaikista vastaajista. Yli kaksi kolmasosaa suurissa ja keskisuurissa vastaajayrityksistä (69 %) koki tilanteen tietoriskien osalta huonontuneen.

Vuonna 2017 selvityksessä 42 prosenttia kaikista vastaajista kertoi tietoriskien osalta tilanteen huonontuneen aiemmasta. Kolmen vuoden aikana tilanne on huonontunut 12 prosenttiyksikköä.

Suomi on viimeiset vuosikymmenet ollut ylpeä koulutuksen tasosta, tutkimus- ja kehitystyöstä, suomalaisen työn laadusta ja maailmalla on tunnettuja suomalaisia ”high tech” -yrityksiä. Kaikki nämä suomalaiset ylpeydenaiheet ovat rikollisten silmissä ensiluokkaisia mielenkiinnon kohteita.

Miten paljon suomalaiselta yrityksiltä viedään laadukasta tietoa kilpailijoiden hyödynnettäväksi? Arviot vaihtelevat sadoista miljoonista miljardiin vuositasolla. Tätä summaa arvioitaessa kannattaa mieltää, että sen kattamiseksi tarvitaan kate-euroja. Mikäli vahinko on 100 miljoonaa ja alan keskikate 20%, on alan uhreiksi joutuneiden yritysten tehtävä lisää liikevaihtoa 500 miljoonan edestä. Ja vasta sen jälkeen on päästy matemaattisesti menetyksen nollaamiseen. Kerrannaisvaikutukset yritysvakoilusta ovat huomattavasti ankarammat kuin yleisesti tunnutaan ymmärtävän. Siksi vakoilun torjuntaan ja tiedon suojaamiseen olisi panostettava huomattavasti enemmän kuin aiemmin. Jos tieto on uusi öljy, voi suojaamaton lähde kuivua luvattoman pumppauksen seurauksena.

Yrityksen maineen mustamaalaus tullut osaksi arkea, kolmasosa suurista ollut kohteena

Eri tavoin tapahtuva mustamaalaus on viidentoista vuoden aikana valitettavasti vakiintunut osaksi kaikkien toimialojen arkea. Kaikista yrityksistä 14 prosenttia kertoi joutuneensa mustamaalatuksi sosiaalisessa mediassa. Suurista yrityksistä 36 prosenttia oli tullut mustamaalatuksi. Sosiaalisen median käyttämisen yleistyttyä, kynnys mustamaalaukselle on varsin alhaalla. Paras vastakeino yritykselle on asiallinen viestintä ja tämä edellyttää toimivien ja selkeiden viestintäsuunnitelmien olemassaoloa.

Yleisintä perättömän tiedon levittäminen on niiden vastaajien keskuudessa, jotka olivat ilmoittaneet toimialakseen ”Muu toimiala”. Näistä vastaajista viidesosa (19 %) kertoi tulleensa mustamaalatuksi. Seuraavaksi yleisintä se oli kaupan alalla, jossa 15 prosenttia vastaajista kertoi yritykseensä kohdistuneesta mustamaalauksesta. Palvelualalla 13 prosenttia, teollisuudessa 10 prosenttia ja rakennusalalla 7 prosenttia vastaajista oli kokenut mustamaalausta.

Ulkopuolisen henkilön tekemät petokset – neljäsosa suurista uhrina

Kaikista vastaajayrityksistä 14 prosenttia ilmoitti joutuneensa ulkopuolisen aiheuttaman petoksen kohteeksi viimeisen kolmen vuoden aikana. Suurista yrityksistä 23 prosenttia oli päätynyt huijatuksi tavalla tai toisella. Erilaiset sähköpostia hyödyntävät huijaukset, kuten toimitusjohtajahuijaukset, ovat lisääntyneet viime aikoina. Varautuminen huijauksien torjuntaan ei ole vaikeaa, mutta se vaatii henkilökunnalta valppautta ja rohkeutta epäillä ja kyseenalaistaa erilaisia normaalilta liiketoiminnalta näyttäviä huijausyrityksiä. Henkilökunnan koulutus ja uhkatietoisuus ovat avainasemassa petosten torjunnassa.

Rakennusalan yrityksistä joka viides (20 %) ilmoitti tapahtuneesta petoksesta viimeisen kolmen vuoden aikana. Seuraavaksi yleisimpiä petokset olivat niiden vastaajien keskuudessa, jotka olivat ilmoittaneet toimialakseen ”Muu toimiala”, näistä vastaajista viidesosa (18 %) kertoi petoksen tapahtuneen. Hieman harvinaisempia petokset olivat teollisuudessa (14 %) ja palvelualalla (13 %).

Viidesosa yrityksistä kertoo omaisuuteen kohdistuvien rikosriskien kasvaneen

Kolmasosa kaikista vastaajayrityksistä on kokenut viimeisen kolmen vuoden aikana yrityksen omaisuuteen kohdistuneita rikoksia tai väärinkäytöksiä. Varkauksia oli kokenut neljäsosa yrityksistä ja yli puolet suurista yrityksistä. Suurien yritysten tilannetta selittää se, että niissä yleensä on toiminnan laajuuden vuoksi rikollisille enemmän hyödynnettäviä kohteita.

Suurimmalla osalla vastaajayrityksistä (79 %) omaisuuteen kohdistuvat turvallisuusriskit ovat pysyneet ennallaan viimeisen kolmen vuoden aikana. Kokonaiskuvan kannalta on pidettävä mielessä se, että turvallisuusriskit eivät ole näidenkään osalta pienentyneet.

Joka viidennessä yrityksessä omaisuuteen kohdistuvat turvallisuusriskit ovat lisääntyneet paljon tai jonkin verran. Lähes kaikki (97 %) vastaajat kokevat omaisuuteen kohdistuvien rikosten määrän pysyneen vähintään samana kuin aiemmin tai lisääntyneen.

Työntekijöiden tekemät rikokset ja väärinkäytökset vaikeita torjua

Työnantajan tulee lähtökohtaisesti luottaa työntekijöihin ja antaa heille oikeat työkalut ja liikkumavaraa työn tulokselliseen hoitamiseen. Luottamus ja liikkumavara antavat työntekijälle mahdollisuuden toimia pitkän aikaa epärehellisesti työnantajan tietämättä. Jos kaikkea toimintaa valvotaan, muuttuu toiminta byrokraattiseksi eikä yritys voi toimia niin. Tämä antaa epärehelliselle työntekijälle mahdollisuuksia väärinkäytöksiin ja kiinnijäämisen todennäköisyys voi olla hyvin pieni.

Suurista vastaajayrityksistä 38 prosenttia ja keskisuurista 25 prosenttia kertoi työntekijän syyllistyneen rikokseen tai väärinkäytökseen työnantajaansa kohtaan. Kaikista vastaajista 14 prosenttia oli joutunut työntekijänsä uhriksi.

Väärinkäytösten tutkiminen omatoimisesti vielä tällä hetkellä yleistä

Joulukuussa 2021 voimaantuleva Whistleblowing -direktiivi lisää painetta ammattimaisen tutkinnan osaamiselle. Se velvoittaa yritystä reagoimaan seitsemän päivän kuluessa ilmoittamalla vihjeenantajalle vastaanottaneensa vihjeen ja aloittavansa selvittelyn. Kolmen kuukauden kuluessa yrityksen on kerrottava ilmoittajalle, mitä asian suhteen on tehty ja mitä on selvinnyt.

Kaikista vastaajayrityksistä valtaosa, 76 prosenttia, selvittää vielä väärinkäytökset itse, kun taas ulkopuolisia asiantuntijoita (16 %) käyttää selvä vähemmistö. Vastaajien kokoluokka ei aiheuta suurta vaihtelua omatoimisesti väärinkäytöksiä selvittävien osuuteen, pienistä 71 prosenttia, keskisuurista 79 prosenttia ja suurista 78 prosenttia selvittää väärinkäytökset itse.

Koulutus – yksinkertainen on tehokasta ja yleistä yritysten keskuudessa

On sitten kyse omaisuuden, tiedon tai henkilökunnan suojaamisesta, koulutus on tehokkaimpia tapoja varautua uhkia vastaan. Koulutettu henkilökunta osaa toimia oikein ja toisaalta työnantaja voi edellyttää työntekijöille koulutettujen toimintatapojen noudattamista työntekijöiltä. Koulutettu työntekijä voi olla huomattavasti valppaampi tunnistamaan riskejä ja toimimaan oikein eri tilanteissa.

Kaksi kolmasosaa vastaajista kouluttaa työntekijöitä toimitilojen ja omaisuuden suojaamiseen liittyvissä asioissa. Alle puolet (42 %) kaikista yrityksistä kouluttaa työntekijöitä erilaisiin uhkatilanteisin ja enemmistö (73 %) antaa koulutusta salaisten tai luottamuksellisten tietojen oikeaan käsittelyyn.

Pandemian jatkuminen katkaisee monen yrityksen jatkuvuuden ja etätyön turvallisuus huolettaa

Pandemian aikana yritykset ovat ottaneet laajasti käyttöön erilaisia toimenpiteitä, joilla pyritään torjumaan ja vähentämään tartuntoja ja varmistamaan toiminnan jatkuminen. Siitä huolimatta neljäsosa (24 %) vastanneista yrityksistä kertoo jatkuvuuden edellytysten loppuvan maalis-huhtikuussa 2021. Kesään 2021 mennessä jatkuvuuden edellytysten loppumisesta vastanneiden osuus kasvaa kolmasosaan (31 %).

Pandemia on lisännyt etätyötä ja nostanut etäyön tietoturvallisuuden huolen aiheeksi. Selvityksen mukaan jopa 39 prosenttia vastanneista yrityksistä kertoo, etteivät ne ole panostaneet etätyön turvallisuuteen riittävästi. Tämä antaa paljon mahdollisuuksia niille, jotka haluavat hyödyntää etätyön yleistymistä rikollisiin tarkoituksiin.

LÄHTEITÄ JA LISÄTIETOA

Finlex.fi. Sivustolla on Suomen sähköinen säädöskokoelma.

ICC Finland ja Keskuskauppakamari (2016). Tietoturvaopas yrityksille. ICC Cyber security guide for business.

Finassiala.fi ja vahingontorjunta.fi sivuilla on ohjeita muun muassa omaisuuden suojaamisesta. Sivustoilla on myös tilastoja poliisin tietoon tulleesta omaisuusrikollisuudesta.

Helsingin seudun kauppakamari (2019). Yrityksiin kohdistuvat kyberuhat.

Huoltovarmuuskeskuksen sivuilla on välineitä yrityksen jatkuvuussuunnitteluun. https://www.huoltovarmuuskeskus.fi/tietoa-huoltovarmuudesta/jatkuvuudenhallinta/ .

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

Kilpailu- ja kuluttajavirasto (2017). Pieniin ja keskisuuriin yrityksiin kohdistuvat huijaukset. Kilpailu- ja kuluttajaviraston selvityksiä 2/2017.

Rikoksentorjunta.fi. Oikeusministeriön alaisen rikoksentorjuntaneuvoston sivuilla on tietoa rikoksentorjunnasta.

Tilastokeskuksen sivuilta löytyy tilastotietoa esimerkiksi rikollisuudesta ja rikostenselvittämisprosenteista. Http://www.stat.fi/ .

Vapaavuori, Tom (2016). Yrityssalaisuudet, liikesalaisuudet ja salassapitosopimukset.

YRITYSTEN RIKOSTURVALLISUUS 2020 – KYSYMYKSET

1. YRITYSRIKOSTEN MÄÄRÄN KEHITYS

Ovatko yritykseen kohdistuvat rikosriskit ja väärinkäytökset viimeisen kolmen vuoden aikana…

lisääntyneet paljon
lisääntyneet jonkin verran
pysyneet ennallaan
vähentyneet jonkin verran
vähentyneet paljon

2. IHMISIIN LIITTYVÄT RISKIT

Ovatko yrityksen <u>henkilöstöön</u> kohdistuvat turvallisuusriskit viimeisen kolmen vuoden aikana…

lisääntyneet paljon
lisääntyneet jonkin verran
pysyneet ennallaan
vähentyneet jonkin verran
vähentyneet paljon

<u>Toteutuneet riskit /uhat</u>

Onko yrityksessänne viimeisen kolmen vuoden aikana…

	Kyllä / Ei/ Ei osaa sanoa
työntekijä on joutunut työssään väkivallan uhriksi?	
työntekijää on työssään uhkailtu /häiritty?	
työntekijä syyllistynyt rikokseen / väärinkäytökseen yritystänne kohtaan?	
työntekijä syyllistynyt rikokseen / väärinkäytökseen asiakastanne kohtaan?	

<u>Riskienhallintakeinot</u>

Miten yrityksenne on varautunut ihmisiin kohdistuviin rikosriskeihin työtehtävissä?

	Kyllä / Ei/ Ei osaa sanoa
Työympäristön teknisillä ratkaisuilla	
Ohjeet mahdollisiin väkivalta- ja uhkatilanteisiin	
Henkilötietojen suojaus on määritelty	
Matkustamisesta on annettu turvallisuusohjeet	
Työntekijöille annetaan turvallisuuskoulutusta	
Työntekijöitä kannustetaan kertomaan havaitsemistaan turvallisuuspuutteista	
Henkilökunnan turvallisuudesta huolehtivat vartijat tai oman organisaation turvahenkilöt	

3. TIETOON LIITTYVÄT RISKIT

Ovatko yrityksen tietoon kohdistuvat turvallisuusriskit viimeisen kolmen vuoden aikana…

lisääntyneet paljon
lisääntyneet jonkin verran
pysyneet ennallaan
vähentyneet jonkin verran
vähentyneet paljon

Toteutuneet riskit /uhat

Onko yrityksenne tietoon kohdistunut seuraavia rikoksia tai tahallisia väärinkäytöksiä viimeisen kolmen vuoden aikana?

Kyllä / Ei/ Ei osaa sanoa
Luottamuksellisen yritysasian paljastaminen luvatta kolmannelle osapuolelle
Yritystiedon (sisällön) luvaton urkkiminen / vakoilu
Tietojen luvaton kopiointi ennen siirtymistä pois yrityksen palveluksesta
Tietoverkkoon murtautuminen
Tiedostojen tahallinen tuhoaminen

Riskienhallintakeinot

Varautuminen tiedon väärinkäytöksiin (tiedon suojaus)

Kyllä / Ei/ Ei osaa sanoa
Onko yrityksellänne tärkeitä tietoja (liike- ja ammattisalaisuudet) koskeva luokittelu- ja käsittelyohje?
Onko yrityksen tärkeimmät tiedot suojattu rajatuilla käyttöoikeuksilla?
Onko henkilökuntaa koulutettu salaisten / luottamuksellisten tietojen käsittelyyn?
Onko yrityksellä tietotaitoa tai muuta omaisuutta, joka käsityksenne mukaan saattaisi olla laittoman tiedustelun tai yritysvakoilun kohteena?

4. TOIMINTAAN LIITTYVÄT RISKIT

Toteutuneet riskit /uhat

Onko yrityksenne toimintaan kohdistunut seuraavia rikoksia tai tahallisia väärinkäytöksiä viimeisen kolmen vuoden aikana?

Kyllä/ Ei /Ei osaa sanoa
Toimialalla on pimeää työvoimaa
Yritys on kohdannut lahjontaa Suomessa yritysten kanssa asioidessa
Yritys on kohdannut lahjontaa Suomessa viranomaisasioinnissa
Taloushallintoon liittyvät sisäiset väärinkäytökset
Yritys on joutunut ulkopuolisen aiheuttaman petoksen kohteeksi
Jos kyllä, mistä on ollut kyse (esim. maksuvälinepetos, tilauspetos, valelasku)
Onko yrityksenne mainetta mustamaalattu sosiaalisessa mediassa kilpailijoiden tai entisten työntekijöiden toimesta?

Riskienhallintakeinot

Miten yrityksenne on varautunut yrityksen toimintaan kohdistuviin rikosriskeihin työtehtävissä?

	Kyllä/ Ei /Ei osaa sanoa
Asiantuntijat tarkastavat sopimustekstit	
Yrityksen johto tarkistaa merkittävimmät liiketoimintasopimukset	
Taloushallintoa auditoidaan	
Luottotietojen tarkastukset	
Luottovakuutuksen käyttäminen	
Vihjekanava väärinkäytösten esilletuomiseksi	

Saatuanne tiedon toimintaanne liittyvästä epäillystä väärinkäytöksestä, tutkitteko sen

a) oman henkilökunnan toimesta
b) käytätte ulkopuolista asiantuntijaa
c) en osaa sanoa

Kuuluvatko yrityksen turvallisuusjohtamiseen seuraavat osat?

	Kyllä/ Ei /Ei osaa sanoa
Yrityksen johto osallistuu henkilökohtaisesti turvallisuuden kehittämiseen	
Turvallisuusasioita käsitellään henkilöstön kanssa	
Yritysturvallisuus on osa yrityksen vuotuista budjetti- ja toimintasuunnittelua	
Yrityksellä on toimintaohje poikkeustilanteita varten	
Poikkeustilanteita varten tehtyä toimintaohjetta harjoitellaan	

5. KORONAN VAIKUTUKSET LIIKETOIMINNAN JATKUVUUDENHALLINTAAN

1. Onko yrityksenne turvallisuustilanne koronan aikana

parantunut paljon/ parantunut hieman/ennallaan/ heikentynyt hieman/ heikentynyt huomattavasti

2. Jos korona-aikana yritykseenne tai työntekijöihinne on kohdistunut rikos, niin millainen rikos on ollut kyseessä?

- petos
- kyberrikos
- kavallus
- varkaus
- ryöstö
- pahoinpitely
- laiton uhkaus
- talousrikos tietoverkon kautta
- Muu mikä
- Yritykseen ei ole kohdistunut rikosta

3. Oletteko panostaneet etätyön tietoturvallisuuteen?
Kyllä/ei
Miten? (vapaa kysymys)

4. Mikäli yrityksessänne ei täysin voida tehdä etätyötä, miten olette varautuneet koronaan ja varmistamaan liiketoiminnan jatkuvuuden?

Etäisyyden pitämisen mahdollistaminen toimistolla
Työpisteiden etäisyys
Toimistolla työskentelyn vuorottelu (eri henkilöt eri päivinä)
Käsidesi
Kasvomaskit työntekijöille
Kasvomaskit vieraille
Työajan muuttaminen esim. työmatkat ruuhka-ajan ulkopuolelle
Kokousmenettelyt
Vieraiden minimointi
Asiakkaiden, yhteistyökumppanien ja omin työntekijöiden vierailut kriittisiin toimipaikkoihin minimoitu, (varasto, tuotanto myynti, asiakaspalvelu....)
Matkustamisen rajoittaminen koti- ja/tai ulkomaille
Muu, mikä?

5. Mikä koronatilanteessa uhkaa eniten jatkuvuutta? Valitse 3 suurinta
Työntekijöiden sairastuminen
Viranomaisten hidas reagointi uhkiin
Viranomaisten ylireagointi uhkiin ja liian tiukat rajoitukset
Testiin pääsyn hitaus
Testitulosten saamisen hitaus
Taloudellisen tuen hakemisen vaikeus
Muu, mikä?

7. Oletteko kartoittaneet toimintanne riskikohdat siltä osin miten eri tahojen koronasairastuminen tai karanteeni voi vaikuttaa toimintaanne?
-omat työntekijät
-alihankkijat
-asiakkaat
-työntekijöiden lähiomaiset

8. Onko yrityksessänne selkeät ohjeet sairastumisen varalta?

9. Miten pitkään yrityksenne toiminnan jatkuvuus/resilienssi kestää pandemian jatkumista?
1kk
3kk
6kk
9kk
12kk
pidempään

10. Onko yrityksenne saanut hallitukselta ja viranomaisilta niin selkeää tietoa, jonka nojalla olette voineet asianmukaisesti varautua koronaan ja turvata liiketoiminnan jatkuvuuden?

Kyllä/ei

11. Mistä olette saaneet tietoa koronan vaikutuksista yritystoimintaan?
- kauppakamarit
- hallitus
- ministeriöt
- THL
- kaupunki tai kunta
- aluehallintoviranomainen
- media
- ulkomaalaisten viranomaisten internetsivustot
- toiset yritykset
-muualta. mistä?

6. OMAISUUTEEN LIITTYVÄT RISKIT

Ovatko yrityksen <u>omaisuuteen</u> kohdistuvat turvallisuusriskit viimeisen kolmen vuoden aikana…

lisääntyneet paljon
lisääntyneet jonkin verran
pysyneet ennallaan
vähentyneet jonkin verran
vähentyneet paljon

Yrityksenne hallussa oleva asiakkaan omaisuus, tieto ja suojaustarpeet

	Kyllä/ Ei /Ei osaa sanoa
Yrityksellämme on hallussaan asiakkaiden omaisuutta	
Yrityksellämme on hallussaan asiakkaiden tietoja	
Yhteistyösopimukseen on kirjattu toimintatavat asiakkaan omaisuuden tai tietojen suojaamiseksi	

Toteutuneet riskit /uhat

Onko yrityksenne omaisuuteen kohdistunut seuraavia rikoksia tai väärinkäytöksiä viimeisen kolmen vuoden aikana?

	Kyllä/ Ei /Ei osaa sanoa
Murto toimi- tai tuotantotiloihin	
Ilkivalta toimi- tai tuotantotiloihin	
Varkaus	

Riskienhallintakeinot

Onko omaisuuden suojaamiseksi tehty seuraavia toimia?
Tuotanto- ja toimitilojen suojaus:

	Kyllä/ Ei /Ei osaa sanoa
Murtohälytys	
Videovalvonta	
Vierailujen ohjeistus	
Vartiointi	
Henkilöstön koulutus	

7. TURVALLISUUDEN KEHITTÄMINEN

Miten yritykseenne kohdistuvat rikosriskit ovat muuttuneet viimeisen kolmen vuoden aikana? Panostaako yrityksenne seuraaviin yritysturvallisuuden osa-alueisiin seuraavien kolmen vuoden aikana…

	nykyistä enemmän	saman verran kuin nykyisin	nykyistä vähemmän
Tietoturvallisuus			
Henkilöturvallisuus			
Tuotantotilojen ja välineiden turvallisuus			
Terrorismiin varautuminen			
Muiden uhkien torjunta			

Jos kyllä, mitä muita uhkia tarkoitatte

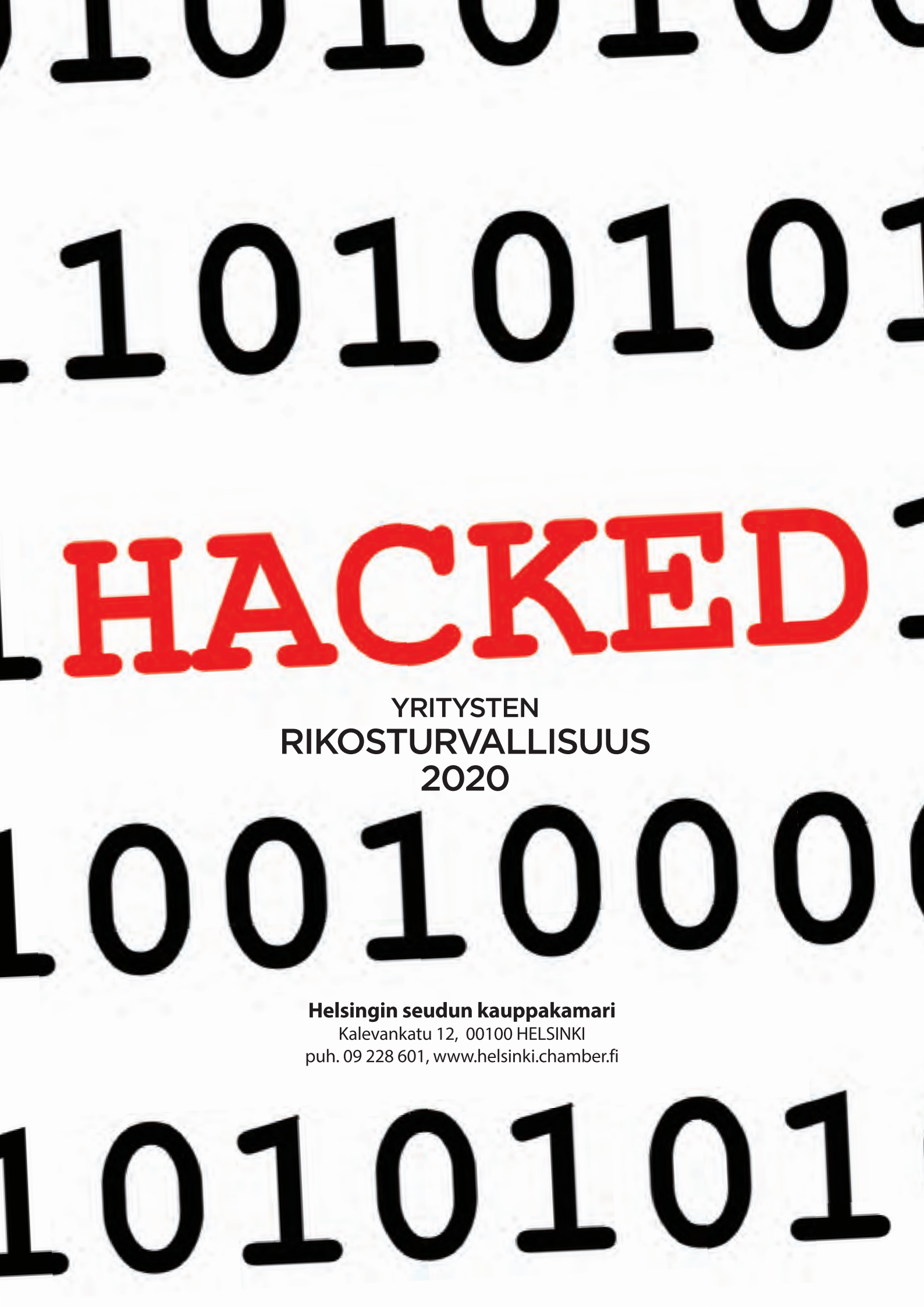
Rikosriskeihin liittyvä tiedonsaanti viranomaisilta

	Kyllä/ Ei /Ei osaa sanoa
Saako yrityksenne tietoa viranomaisilta yrityksiin kohdistuvista rikoksista ja rikosilmiöistä	
Saako yrityksenne tietoa jostain muualta?	
Tarvitseeko yrityksenne tietoa viranomaisilta?	

8. AVOIMET KYSYMYKSET

Mitä asioita pidätte suurimpina esteinä yritysturvallisuudelle?

Mainitse tilanne / tilanteita, jossa turvallisuudessa oli puutteita / turvallisuusjärjestelyt pettivät?



YRITYSTEN RIKOSTURVALLISUUS 2020

Helsingin seudun kauppakamari
Kalevankatu 12, 00100 HELSINKI
puh. 09 228 601, www.helsinki.chamber.fi