YRITYSTEN RIKOSTURVALLISUUS 2017

Riskit ja niiden hallinta

KAUPPAKAMARI

YRITYSTEN RIKOSTURVALLISUUS 2017:
Riskit ja niiden hallinta

Lokakuu 2017

Selvityksen laatijat:
Keskuskauppakamari
Helsingin seudun kauppakamari

Julkaisija:
KESKUSKAUPPAKAMARI

Taitto:
Markus Lähdesmäki

Keskuskauppakamari, Aleksanterinkatu 17,
PL 1000, 00101 Helsinki
www.chamber.fi

ISBN 978-952-5620-85-6

SISÄLLYS

ESIPUHE

Kauppakamarit kehittävät yritysten toimintaedellytyksiä. Keskuskauppakamari ja Helsingin seudun kauppakamari ovat kartoittaneet suomalaisten yritysten turvallisuustilannetta vuodesta 2005 lähtien. Yritysten rikosturvallisuus 2017 on neljäs aihepiiriin liittyvä tutkimus. Aikaisemmat selvitykset on julkaistu vuosina 2012, 2008 ja 2005.

Vuoden 2017 valtakunnallinen selvitys perustuu 762 yritysjohtajan vastauksiin. Yritysjohtajat ovat antaneet maan kattaviin selvityksiin runsaasti arvokasta tietoa yritysturvallisuuden tilasta ja kehityksestä.

Selvitysten tavoitteena on saada vertailukelpoista tietoa erikokoisten ja eri toimialoilla toimivien yritysten tilanteesta. Selvitykset ovat auttaneet sekä yritysturvallisuuden nykytilan kartoittamisessa että yritysten riskienhallinnan tukemisessa. Selvitysten toistaminen on auttanut myös havaitsemaan yritysten turvallisuustilanteen muutoksia.

Tutkimus tuo esiin muutaman selkeän viestin. Ensimmäiseksi yritykset arvioivat, että yrityksiin kohdistuvat rikosriskit ovat selvässä kasvussa. Riskit ovat muuttuneet ja vaativat uusia tapoja torjua niitä.

Toiseksi yritysten jatkuvuuden ja toiminnan turvaaminen vaatii muuttuvassa toimintaympäristössä lisää panostusta. Toimenpiteet vahvistavat koko yhteiskunnan toimivuutta ja turvallisuutta.

Kolmanneksi kyselyn tulokset vahvistavat sen, että osa tietoa tarvitsevista yrityksistä ei sitä saa viranomaisilta eikä muistakaan lähteistä. Tästä syystä olisi tärkeää kehittää tiedonvaihtomalleja.

Selvityksen tulokset antavat yritysjohtajille eväitä toimivaan riskienhallintaan. Yritysjohtajilla on nyt hyvä mahdollisuus tutkia, mitä riskienhallinnan keinoja eri toimialoilla toimivat yritykset käyttävät ja valita oman liiketoiminnan ja resurssien kannalta tarpeelliset keinot.

Selvityksen laatijat,
Asiantuntija Kaisa Saario, Keskuskauppakamari ja
asiantuntija Panu Vesterinen, Helsingin seudun kauppakamari

1 JOHDANTO

Yritysten rikosturvallisuus 2017 –selvityksen tavoitteena on tutkia, mikä on yritysturvallisuuden tila Suomessa, mitä riskejä eri toimialoilla toimiviin yrityksiin kohdistuu ja miten yritykset ovat varautuneita riskeihin. Selvitys kuvaa myös sellaisia yrityksiin kohdistuvia rikoksia ja väärinkäytöksiä, jotka usein jäävät tilastoimattomaksi piilorikollisuudeksi.

Tutkimustuloksista yritykset saavat kokonaiskuvan esimerkiksi omaa toimialaa uhkaavista riskeistä ja muiden yritysten käyttämistä riskienhallintakeinoista. Useana vuotena toistetut selvitykset auttavat havaitsemaan muutoksia uhkien tai riskienhallinnan tasossa ja puuttumaan esimerkiksi lainsäädännössä esiintyviin ongelmiin tai lisäämään tietoa tai koulutusta havaituista turvallisuusriskeistä.

Selvitys on osa kauppakamarien edunvalvontaa. Kauppakamareilla on Suomessa 20 000 jäsentä, joista valtaosa on yrityksiä. Kauppakamarit edistävät yritysten toimintaedellytyksiä. Keskuskauppakamari koordinoi 19 kauppakamarin yhteistoimintaa, kun taas kauppakamarit palvelevat erityisesti oman toiminta-alueensa yrityksiä.

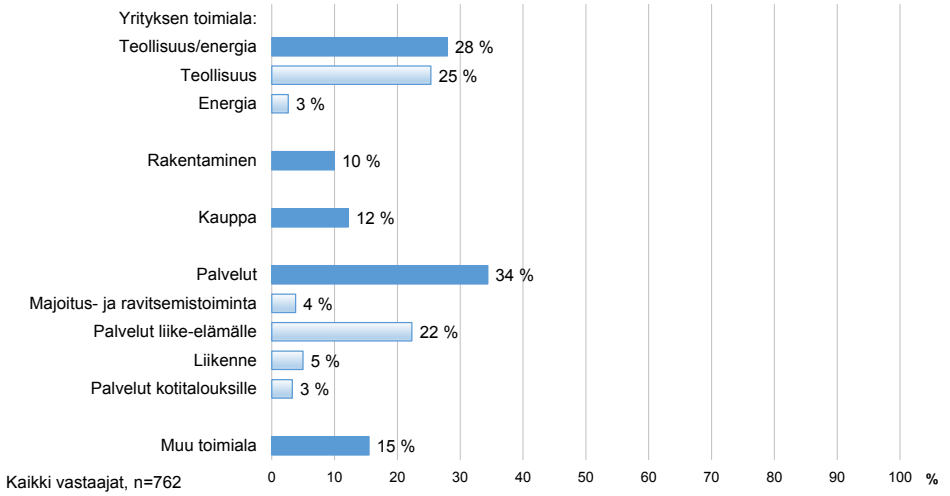
Tutkimuksen toteuttaminen ja vastaajien taustatiedot

Yritysten rikosturvallisuus – riskit ja niiden hallinta – selvitykset ovat koko maan ja kaikki toimialat ja yrityskoot kattavia. Yritysten rikosturvallisuus 2017 – riskit ja niiden hallinta -selvitys perustuu 762 Suomessa toimivan yrityksen vastauksiin. Kaikki vastaajat ovat kauppakamarien jäseniä. Yritysturvallisuusselvityksiä on toteutettu neljästi - vuosina 2017, 2012, 2008 ja 2005. Eri vuosien tuloksia vertailevissa kaavioissa ei ole mukana alle viisi henkilöä työllistäviä yrityksiä, jotta tulokset ovat täysin vertailukelpoisia.

Kyselyn toteutti Taloustutkimus yhteistyössä kauppakamarien ja Huoltovarmuuskeskuksen kanssa. Selvityksen ovat laatineet asiantuntija Kaisa Saario Keskuskauppakamarista ja asiantuntija Panu Vesterinen Helsingin seudun kauppakamarista. Selvityksen jatkuvuussuunnittelua koskevat kysymykset on laadittu yhteistyössä Huoltovarmuuskeskuksen kanssa.

Yritykset vastasivat kyselyyn Internet-pohjaisella kyselyohjelmalla keväällä 2017. Yrityksen vapaamuotoiset vastaukset ovat kursiivilla ja vastaajan äidinkielellä. Ruotsiksi vastasi 11,5 prosenttia vastaajista. Ruotsiksi vastanneet ovat Ahvenanmaan, Helsingin seudun, Länsi-Uudenmaan sekä Pohjanmaan kauppakamarin alueilta.

Vastaajat toimialoittain

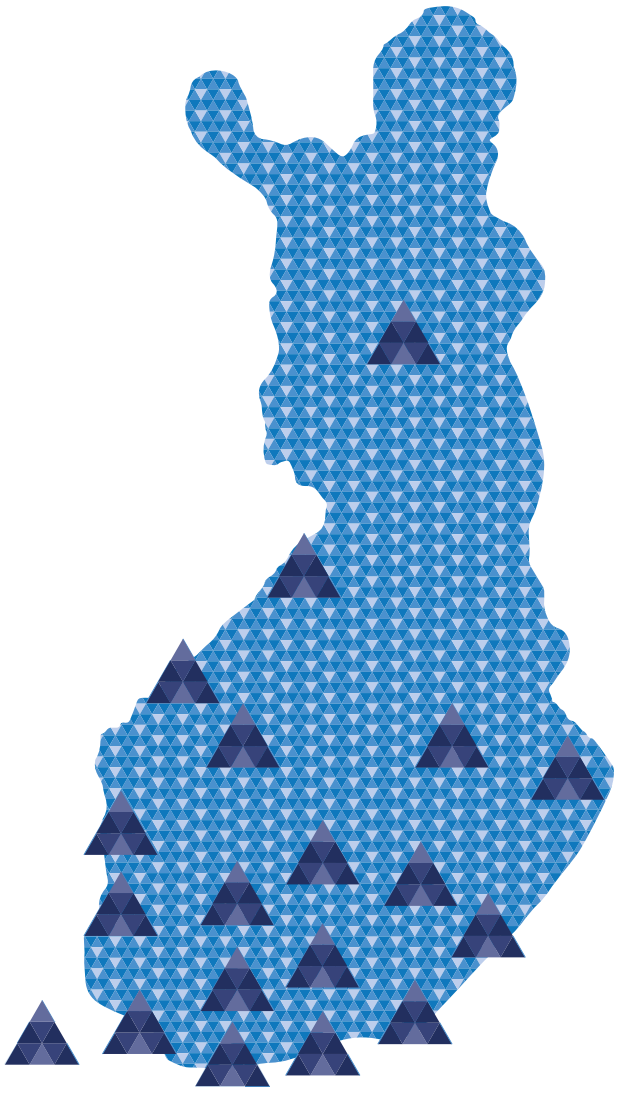


Taloustutkimus Oy
KAUPPAKAMARI

Lähde: Yritysten rikosturvallisuus 2017.
Keskuskauppakamari ja Helsingin seudun kauppakamari.

Selvityksen tuloksia tarkastellaan pääasiassa yrityskoon ja toimialan perusteella. Selvityksessä käytetään Tilastokeskuksen yrityskokoluokitusta. Suurin osa (72 %) vastanneista yrityksistä on henkilömäärältään pieniä yrityksiä, jotka työllistävät alle 50 henkilöä. Alle 10 henkilön mikroyrityksiä on vastanneista 28 prosenttia. Henkilömäärältään keskisuuria, 50 – 249 henkilöä työllistäviä yrityksiä on 19 prosenttia ja suuria, vähintään 250 henkilöä työllistäviä yrityksiä on yhdeksän prosenttia.

Vastanneista yrityksistä 28 prosenttia edustaa teollisuutta, 12 prosenttia kauppaa, 34 prosenttia palveluita ja 10 prosenttia rakentamista. Vastaajista 15 prosenttia ilmoitti jonkin muun toimialan kuin yllä mainitun. Näitä vastaajia ei ole piirretty toimialakohtaisiin tuloksiin, mutta sen sijaan ne sisältyvät kaikkia vastanneita yrityksiä kuvaaviin kaavioihin.



Selvityksen vastaajista suurin osa (68 %) on yritysten toimitusjohtajia. 13 prosenttia vastaajista on edustettuina yrityksen hallituksessa. Talousjohtajia tai kehitysjohtajia on kolme prosenttia vastaajista ja turvallisuus- ja riskienhallintajohtajia yhtä paljon.

Vastaukset kattavat koko maan. Vastaajista viidennes (21 %) edustaa Helsingin seudun kauppakamarialueella toimivia yrityksiä. Tampereen vastaajien osuus on yhdeksän prosenttia ja Kuopion alueen, Oulun, Pohjanmaan ja Turun kauppakamarialueilla seitsemän prosenttia. Ahvenanmaalla osuus on kuusi prosenttia ja Hämeen ja Kuopion vastaajien osuudet ovat viisi prosenttia. Muiden kauppakamarialueiden vastaajien osuudet ovat alle viisi prosenttia.

Selvityksessä käytetään nettoprosenttiosuutta ja saldolukua. Nettoprosentti ilmaisee, kuinka suuri osa vastaajista on ilmoittanut, että ainakin yksi mainituista turvallisuusriskeistä on toteutunut. Riskien hallintaa 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.

ETELÄ-KARJALAN KAUPPAKAMARI
ETELÄ-POHJANMAAN KAUPPAKAMARI
ETELÄ-SAVON KAUPPAKAMARI
HELSINGIN SEUDUN KAUPPAKAMARI
HÄMEEN KAUPPAKAMARI
KESKI-SUOMEN KAUPPAKAMARI
KUOPION ALUEEN KAUPPAKAMARI
KYMENLAAKSON KAUPPAKAMARI
LAPIN KAUPPAKAMARI
LÄNSI-UUDENMAAN KAUPPAKAMARI
OULUN KAUPPAKAMARI
POHJANMAAN KAUPPAKAMARI
RAUMAN KAUPPAKAMARI
RIIHIMÄEN-HYVINKÄÄN KAUPPAKAMARI
SATAKUNNAN KAUPPAKAMARI
POHJOIS-KARJALAN KAUPPAKAMARI
TAMPEREEN KAUPPAKAMARI
TURUN KAUPPAKAMARI
ÅLANDS HANDELSKAMMARE

Yritysrikosten määrän kehitys

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.

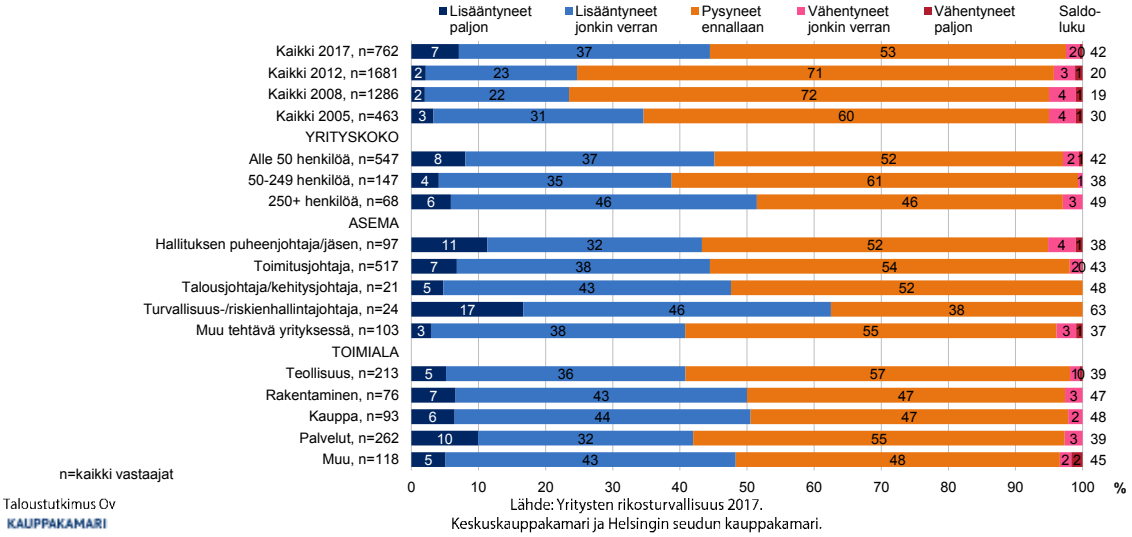
Yritysrikosten määrän kehitystä on vaikea arvioida pelkästään poliisin tilastojen perusteella. Piilorikollisuuden suuri osuus yritysrikoksista johtuu pääasiassa kahdesta tekijästä: rikosten ilmoittamishalukkuudesta ja tilastointikäytännöistä. Yritykset eivät aina ilmoita rikos- tai väärinkäytösepäilyistä poliisille. Esimerkiksi Helsingin seudun kauppakamarin pääkaupunkiseudulla tehdyssä tiedon suojaamiseen keskittyvässä kyselyssä ilmeni, että enemmistö yrityksistä on jättänyt rikosilmoituksen tekemättä. Yritysrikollisuuden kokonaiskuvan hahmottamista vaikeuttaa edelleen se, ettei virallisissa tilastoissa kuten poliisin tietokannassa myöskään pääsääntöisesti eritellä yrityksiin kohdistuvia rikoksia.

Miten saldoluvulla seurataan yritysturvallisuuden tilaa?

Yritysrikosten määrän kehitystä kuvaavissa taulukoissa saldoluku on rikosten lisääntymistä kokeneiden yritysten osuuden ja vähentymistä ilmoittaneiden yritysten osuuden erotus.

Jos saldoluku on nolla, on rikosten lisääntymistä ja vähentymistä kokeneita yrityksiä yhtä paljon. Positiivinen luku ilmaisee, että rikosten lisääntymistä kokeneita yrityksiä on enemmän kuin vähentymistä kokeneita yrityksiä. Keskimääräistä suurempi saldoluku tarkoittaa sitä, että yritysluokan tai toimialan yritykset ilmoittavat muita vastaajia useammin yritysrikosten kasvusta. Saldoluvun kasvaminen vertailuvuosien välillä kertoo turvallisuustilanteen todellisesta tai koetusta heikkenemisestä toimialalla.

Yritysrikosten määrän kehitys
Yritykseen kohdistuvat rikosriskit ja väärinkäytökset ovat viimeisen kolmen vuoden aikana...



n=kaikki vastaajat

Taloustutkimus Oy
KAUPPAKAMARI

Lähde: Yritysten rikosturvallisuus 2017.
Keskuskauppakamari ja Helsingin seudun kauppakamari.

Vastanneet 762 yritystä arvioivat yrityksiin kohdistuvien rikosriskien kehitystä viimeisen kolmen vuoden aikana. Yrityksistä 44 prosenttia arvioi, että rikosten määrä on kasvanut viimeisen kolmen vuoden aikana ja tästä seitsemän prosenttia arvioi, että rikosten määrä on lisääntynyt paljon. Turvallisuustilanteen heikkenemistä indikoi se, että yrityksiä, jotka arvioivat, että rikosten määrä on pysynyt ennallaan viime vuosina oli puolet vuonna 2017, kun taas vuonna 2012 näitä yrityksiä oli lähes kolme neljästä.

Kaikki yritykset	Teollisuus	Rakentaminen	Kauppa	Palvelut
+42	+39	+47	+48	+39

Näkemykset yritysten rikosriskien kehityksestä yleensä eri toimialoilla (punaisella keskimääräistä synkemmät arviot)

Joka toinen suuri yritys näkee kasvua yrityksiin kohdistuvien rikosten ja väärinkäytösten määrässä viimeisen kolmen vuoden aikana. Edelliseen mittauskertaan verrattuna osuus on selvässä kasvussa (34 %-->52%). Kaikissa neljässä kyselyssä (2017, 2012, 2008 ja 2005) suuret yritykset kokevat joutuvansa keskimääräistä useammin rikosten ja väärinkäytösten kohteeksi. Myös vuonna 2017 saldoluku on suurin suurissa yrityksissä (+49). Saldoluvut ovat kasvaneet kaikissa yrityskokoluokissa edellisestä mittauskerrasta, mikä kuvaa sitä, että yritykset kokevat rikosten ja väärinkäytösten määrän kasvaneen. Ne yritykset, joissa vastauksen on antanut turvallisuus- ja riskienhallintajohtaja, arvioivat useimmin, että rikosten määrä on kasvanut.

Toimialojen arviot ovat lähentyneet toisiaan, mikä kertoo siitä, että monet uusista turvallisuusriskeistä (esimerkiksi identiteettikaappaukset) eivät ole enää niin toimialasidonnaisia.

Turvallisuustilannetta pidetään kaikilla aloilla selvästi heikompana kuin edellisellä mittauskerralla. Viisi vuotta sitten tehdyssä selvityksessä viidennes rakennusalan ja teollisuusalan yrityksistä, neljännes palvelualan yrityksistä ja kolmannes kaupan alan yrityksistä arvioi rikosten määrän olevan kasvussa. Vuonna 2017 puolet rakennusalan ja kaupan yrityksistä ja neljä kymmenestä teollisuuden ja palvelualan yrityksistä arvioi rikosten määrän olevan kasvussa. Yritysturvallisuuskyselyn mukaan teollisuuden ja palveluiden toimialoilla on kuitenkin vielä enemmän niitä yrityksiä, jotka arvioivat yrityksiin kohdistuvan rikostilanteen pysyneen ennallaan kuin niitä, jotka arvioivat tilanteen heikentyneen viime vuosina.

Yritysrikosten kehitystä pidettiin synkimpänä kaupan alalla ja rakennusalalla. Näillä aloilla joka toinen vastaaja arvioi, että rikosten määrä on kasvanut. Turvallisuus on molemmilla toimialoilla vetovoimatekijä (Alueiden kilpailukyky 2016-selvitys), mikä vaikuttaa yrityksen arkeen ja liiketoimintaan. Käytännössä turvallisuuden varmistaminen voi olla vaikeaa murtojen ja näpistystenkin osalta, saati sitten uudenlaisissa riskeissä. Rakennusalan vapaissa vastauksissa ilmeni muun muassa se, että vaihtuvien työmaiden suojaaminen on vaikeaa ja riittävä suojaus tulee yrityksille liian kalliiksi. Päivittäiskaupassa poliisin resurssien vähentyminen on näkynyt viime vuosina siinä, että poliisi ei välttämättä ehdi paikalle kauppaa koskettavissa turvallisuusongelmissa. Kauppa kohtaa myös entistä enemmän uudenlaisia riskejä, joita käsitellään tarkemmin luvussa neljä.

Ihmiset yritysrikosten kohteina ja tekijöinä

3 IHMISET YRITYSRIKOSTEN KOHTEINA JA TEKIJÖINÄ

Lukuisia uhkatilanteita tiskissä, turhautuneita juoppoja, juoppohulluja, sekakäyttäjiä, huumeidenkäyttäjiä. Poliisin tulo kestää tunnin joten puhumalla täytyy pärjätä.
(Kaupan alan yritys, alle 50 henkilöä)

Kaikista vastanneista yrityksistä 38 prosenttia oli kokenut henkilöstöön liittyviä turvallisuusriskejä viimeisen kolmen vuoden aikana. Nettotulos on sama kuin edellisellä mittauskerralla vuonna 2012. Yleisimpiä turvallisuusriskejä ovat työntekijän uhkailu tai häirintä töissä sekä työntekijän syyllistyminen rikokseen tai väärinkäytökseen yritystä kohtaan. Yrityksen henkilöstöön liittyvät riskit yleistyvät yrityksen kasvaessa. Suurista, yli 250 henkilöä työllistävistä yrityksistä 72 prosenttia ilmoitti toteutuneista henkilöriskeistä, eli yrityksessä oli realisoitunut yksi tai useampi alla kuvatussa kaaviossa kuvatuista riskeistä. Henkilömäärältään pienemmissä yrityksissä toteutuneita riskejä oli selvästi vähemmän.

Yritysten henkilöriskit viimeisen kolmen vuoden aikana

Saldoluvulla voidaan kuvata myös henkilöriskien kehitystä ja verrata eri toimialoilla toimivien yritysten turvallisuustilannetta. Punaisella merkityt keskimääräistä suuremmat saldoluvut tarkoittavat sitä, että toimialojen yritykset pitävät muita vastaajia useammin henkilöriskien kehitystä epäsuotuisana. Yrityksen henkilöriskien kehitystä kuvaava saldoluku oli heikoin kaupan ja palvelujen toimialoilla ja paras teollisuudessa. Henkilömäärältään suuret yritykset pitivät henkilöriskien kehitystä huomattavasti synkempänä kuin henkilömäärältään pienet yritykset.

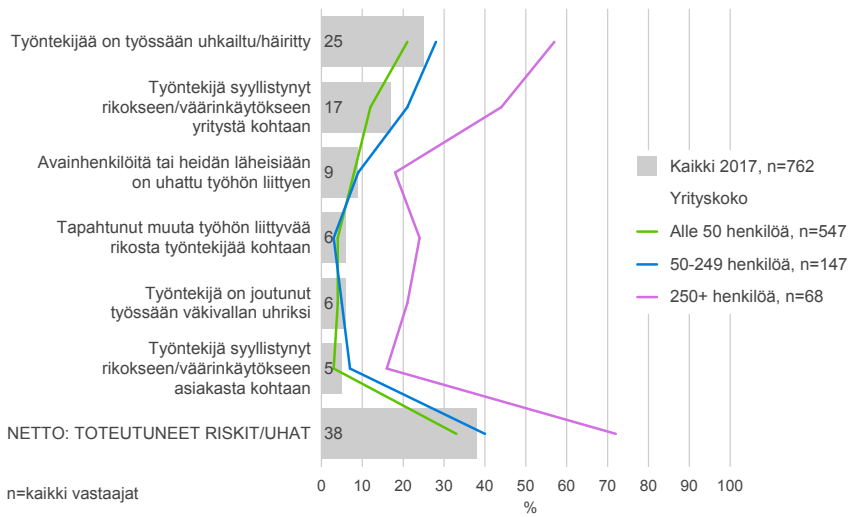
Toteutuneita henkilöriskejä tarkastellessa voidaan havaita, että kaupan ja palvelualojen yritykset ilmoittavat useimmin työntekijöiden tai avainhenkilöiden kokemista uhkailutilanteista ja väkivallasta. Teollisuuden ja rakennusalan vastaajat eivät ilmoittaneet väkivaltatapauksista viimeisen kolmen vuoden aikana. Työntekijän tai avainhenkilöön kohdistuvia uhkailutilanteita oli kuitenkin näilläkin toimialoilla.

Työntekijän uhkailu esimerkiksi palvelutilanteessa on yleisin henkilöstöön liittyvä toteutunut riski. Joka kolmannessa kaupan ja palvelualan yrityksessä on ollut uhkatilanteita viimeisen kolmen vuoden aikana.

Kaikki yritykset	Teollisuus	Rakentaminen	Kauppa	Palvelut
+19	+11	+16	+29	+24

Näkemykset henkilöriskien kehityksestä eri toimialoilla
(punaisella keskimääräistä synkemmät arviot)

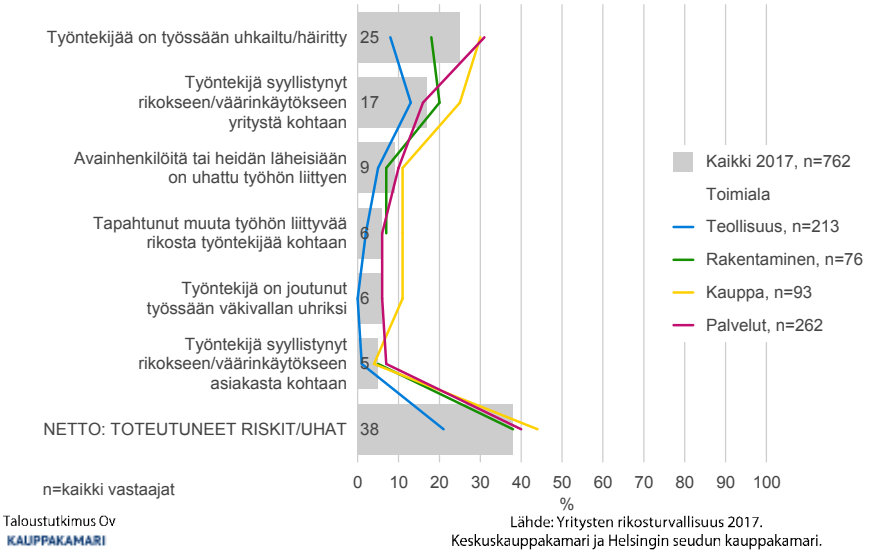
Yrityksen henkilöstöön kohdistuvat turvallisuusriskit
Toteutuneet riskit/uhat



Taloustutkimus Oy
KAUPPAKAMARI

Lähde: Yritysten rikosturvallisuus 2017.
Keskuskauppakamari ja Helsingin seudun kauppakamari.

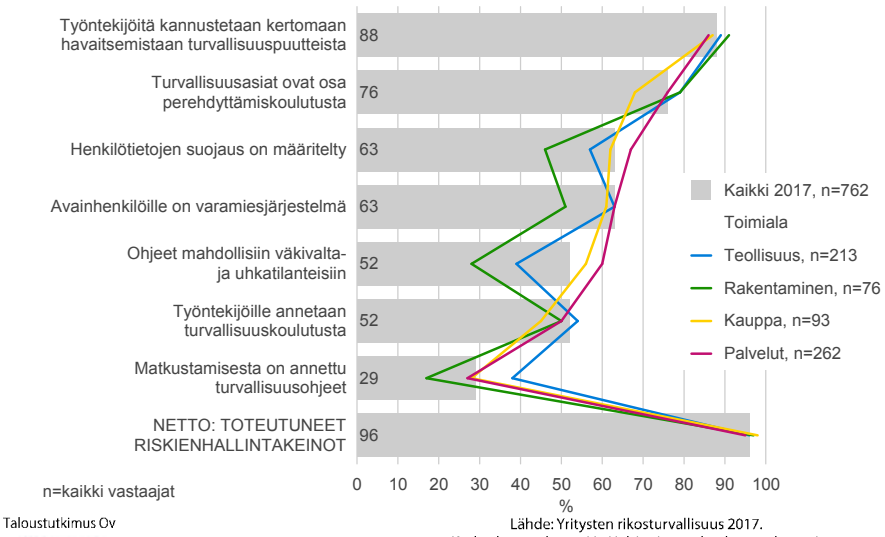
Yrityksen henkilöstöön kohdistuvat turvallisuusriskit
Toteutuneet riskit/uhat



Taloustutkimus Oy
KAUPPAKAMARI

Lähde: Yritysten rikosturvallisuus 2017.
Keskuskauppakamari ja Helsingin seudun kauppakamari.

Yrityksen henkilöstöön kohdistuvat turvallisuusriskit
Varautuminen rikosriskeihin



Taloustutkimus Oy
KAUPPAKAMARI

Lähde: Yritysten rikosturvallisuus 2017.
Keskuskauppakamari ja Helsingin seudun kauppakamari.

Osuus oli jopa tätäkin korkeampi yrityksissä, jotka ilmoittivat toimialakseen muun toimialan (46 %). Varsinaisia väkivaltatilanteita on eniten kaupan alan yrityksissä. Kaupan alan yrityksistä joka kymmenes (11 %) raportoi väkivaltatilanteesta viimeisen kolmen vuoden aikana. Palvelualalla, johon lukeutuu muun muassa ravintola-ala, matkailuala ja erilaiset palvelut liike-elämälle ja kotitalouksille, kuudella prosentilla yrityksistä on ollut väkivaltatilanteita.

Vuosien 2017, 2012, 2008 ja 2005 selvitysten tuloksia vertailtaessa voidaan havaita se, että avainhenkilöiden uhkailu on kasvanut verrattuna ensimmäiseen mittauskertaan vuonna 2005. Nykyisin joka kymmenennessä yrityksessä avainhenkilöä uhataan. Avainhenkilöiden uhkailusta ilmoitti 18 prosenttia suurista yrityksistä 18 %), kun taas pienissä ja keskisuurissa yrityksissä osuus oli keskimääräisellä tasolla (8 – 9 %).

Miten varautua uhkatilanteisiin?

Päivystäjää on uhkailtu ovenavaustilanteessa puukolla ja muutoin väkivallalla, jonka seurauksena on järjestetty turvallisuuskoulutusta sekä hankittu viiltosuojaliivit päivystäjän käyttöön.
(Palvelualan yritys, 50-249 henkilöä)

Väkivallan riskiä lisää erityisesti yksintyöskentely tiloissa, joihin on vapaa pääsy, työpaikan sijainti rauhattomalla alueella, päihtyneiden asiakkaiden tapaaminen, rahan tai arvokkaan omaisuuden käsittely tai vartiointi ja asiakkaan etuisuuksia tai oikeuksia koskevien päätösten käsittely. Työturvallisuuslain mukaan työssä, johon liittyy väkivallan uhka, työskentelyolosuhteet on järjestettävä siten, että väkivallan uhka ja uhkatilanteet ehkäistään mahdollisuuksien mukaan ennakolta. Väkivalta- ja uhkatilanteita ehkäisevät niin tekniset turvallisuuslaitteet, tilojen eriyttäminen kuin esimerkiksi vierailijaohjeistukset, joilla suojataan myös yrityksen omaisuutta ja tietoa (ks. luku 5).

Jos yritys toimii sellaisella toimialalla, jossa esiintyy tavallista enemmän uhkatilanteita, tai jos työpaikalla on jo sattunut väkivaltatilanteita, työntekijään kohdistuvan väkivallan uhan arviointi pitää tehdä lainkin mukaan perusteellisemmin kuin sellaisella alalla, jossa väkivallan uhkaa ei juuri esiinny. Väkivallan riskiä voidaan vähentää jossain määrin myös kiinnittämällä huomiota työtapoihin, työympäristöön ja työaikajärjestelyihin. Erityisesti yksintyöskentelyä pitäisi rajoittaa työssä, jossa väkivallan riski on ilmeinen.

Yritysturvallisuuskyselyyn vastanneet yritysjohtajat kertoivat yrityksen tavoista suojata henkilöstöä ja johtoa väkivallalta ja uhkatilanteilta. Lähes kaikkien tarkasteltujen riskienhallintakeinojen käyttö yrityksen henkilöstöön kohdistuvien turvallisuusriskien hallitsemiseksi on lisääntynyt vuodesta 2012 ainakin hieman. Seuraavilla yrityksen yleisimmillä henkilöstöä suojaavilla keinoilla voidaan estää monia riskejä toteutumasta:

1. Työntekijöitä kannustetaan kertomaan turvallisuuspuutteista (88 %)
Yritysten henkilöstöön tai johtoon kohdistuviin riskeihin voidaan varaitua monin keinoin. Valtaosassa yrityksistä työntekijää kannustetaan kertomaan havaitsemistaan turvallisuuspuutteista. Suurissa yrityksissä näin tehdään lähes poikkeuksetta. Turvallisuuspuutteista ilmoittaminen auttaa parantamaan yrityksen turvallisuustilannetta ja saamaan todellista tietoa yritykseen kohdistuvista riskeistä. Uhkatilanteiden systemaattinen seuranta auttaa myös puuttumaan havaittuihin ongelmakohtiin ja turvallisuuskehityksen muutoksiin.

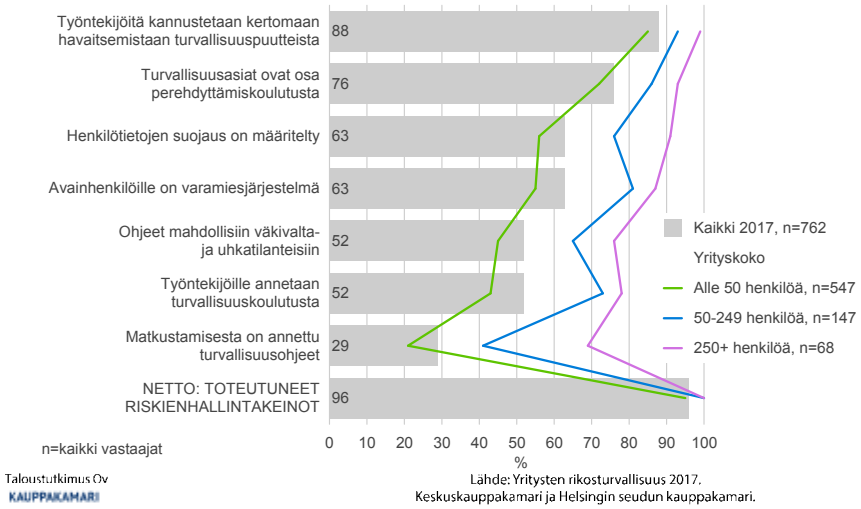
2. Turvallisuusasiat osana perehdytystä (76 %)
Yrityksen kannattaa sisällyttää turvallisuusasiat osaksi työhön tuloon liittyvää perehdytystä. Käytännössä mitä suurempi yritys, sitä useammin perehdytyksessä käsitelläänkin turvallisuusasioita. Kolme neljästä yrityksestä käsittelee turvallisuusasioita perehdytyksen yhteydessä. Yllättävä tulos oli kuitenkin se, että vaikka uhkatilanteita oli eniten kaupan ja palvelualan yrityksissä, turvallisuusasioiden käsittely perehdytysvaiheessa oli yleisempää teollisuusalan ja rakennusalan yrityksissä. Kaupan alan yrityksistä joka kolmas ja palvelualan yrityksistä joka neljäs ei käsitellyt turvallisuusasioita perehdytyksen yhteydessä.

3. Henkilötietojen suojaus on määritelty (63 %)
Yrityksellä on velvollisuus pitää hyvää huolta sekä työntekijöiden että asiakkaidensa henkilötiedoista. Tietosuoja-asioista huolehtiminen kannattaa vastuuttaa yrityksessä, vaikka työntekijöiden pitäisi myös tietää miten esimerkiksi asiakkaiden henkilötiedoista huolehditaan. Suuret yritykset ilmoittivat lähes poikkeuksetta, että niissä henkilötietojen suojaus on määritelty. Osuudet olivat heikoimmat pienissä yrityksissä (56 %) sekä rakennus- (46 %) ja teollisuusalojen (57 %) yrityksissä.

4. Avainhenkilöille on varamiesjärjestelmä (63 %)
Lain mukaan yrityksen pitää huolehtia työntekijöidensä turvallisuudesta. Huolehtimisvelvoitteeseen kuuluu myös se, että avainhenkilöihin kohdistuviin turvallisuusriskeihin on varauduttu. Avainhenkilöriskien hallintaan kuuluu nykyisten ja uusien avainhenkilöiden tunnistaminen ja sitouttaminen sekä tarvittavista sijaisuusjärjestelyistä ja henkilöiden turvallisuudesta huolehtiminen. Avainhenkilöriskien hallintaan lukeutuu toki myös tietoturvallisuus (ks. luku 4) ja matkustamisen turvallisuus, jota on ohjeistanut vajaa kolmannes yrityksistä. Kyselyyn vastanneista yrityksistä 63 prosenttia ilmoitti, että yrityksessä on avainhenkilöille varamiesjärjestelmä. Tulos on pysynyt edellisen tutkimuskerran tasolla. Vuonna 2017 osuudet olivat käytännössä yhtä korkeita kolmella toimialalla kaupassa, teollisuudessa ja palvelualalla (61 – 63 %), kun taas rakennusalalla varamiesjärjestelmä oli vain joka toisessa yrityksessä (51 %).

5. Ohjeet väkivalta- ja uhkatilanteiden hallintaan ja turvallisuuskoulutus (52 %)
Työturvallisuuslain mukaan työnantajan on kerrottava työntekijälle työpaikan haitta- ja vaaratekijöistä ja työntekijän pitää noudattaa annettuja turvallisuusohjeita. Ohjeet voidaan ottaa osaksi perehdytysvaihetta. Joka toisella kyselyyn vastanneella yrityksellä on ohjeet mahdollisiin uhka- ja väkivaltatilanteisiin. Vapaissa vastauksissa kaupan ja palvelualojen yritykset kertoivat monista työntekijään kohdistuneista vaaratilanteista. Ohjeet väkivalta- ja uhkatilanteiden hallintaan puuttuvat edelleen monelta kaupan (44 %) ja palvelualan (38 %) yritykseltä. Näissä yrityksissä ohjeiden teko on tarpeellisempaa kuin muiden alojen yrityksissä, jossa uhkailun tai väkivallan riski on vähäisempää. Kaikissa yrityskokoluokissa ohjeiden teko uhkatilanteita varten on kuitenkin yleistynyt selvästi edellisestä mittauskerrasta vuonna 2012. Vuonna 2017 puolet henkilömäärältään pienistä yrityksistä, kolmannes keskisuurista ja viidennes suurimmista yrityksistä ei ole tehnyt ohjeita uhkatilanteiden varalle.

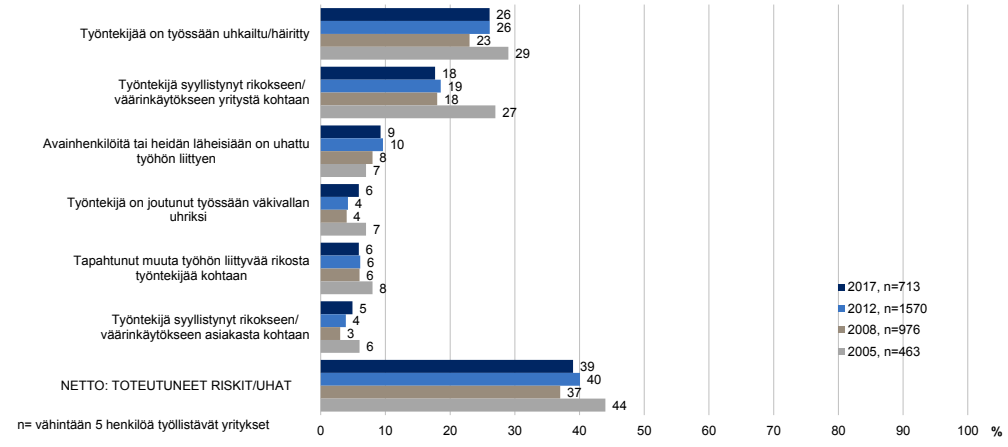
Yrityksen henkilöstöön kohdistuvat turvallisuusriskit
Varautuminen rikosriskeihin



Taloustutkimus Oy
KAUPPAKAMARI

Lähde: Yritysten rikosturvallisuus 2017.
Keskuskauppakamari ja Helsingin seudun kauppakamari.

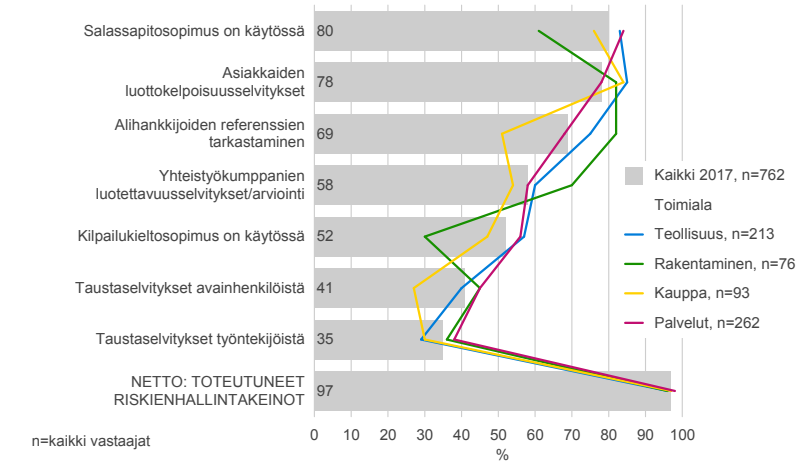
Selvitykset 2005 - 2017: Yrityksen henkilöstöön kohdistuvat turvallisuusriskit
Toteutuneet riskit/uhat



Taloustutkimus Oy
KAUPPAKAMARI

Lähde: Yritysten rikosturvallisuus 2017.
Keskuskauppakamari ja Helsingin seudun kauppakamari.

Varautuminen väärinkäytöksiin



Taloustutkimus Oy
KAUPPAKAMARI

Lähde: Yritysten rikosturvallisuus 2017.
Keskuskauppakamari ja Helsingin seudun kauppakamari.

Väärinkäytökset ja niihin varautuminen

Työkalu- ja tavarahävikki. (Palvelualan yritys, yli 250 henkilöä)

Anställd har stulit pengar av vårt företag. (Palvelualan yritys, alle 50 henkilöä)

Joka kuudes (17 %) yritys ilmoitti työntekijän tai työntekijöiden väärinkäytöksistä yritystä kohtaan. Yrityksen koon kasvaessa väärinkäytösten todennäköisyys kasvaa. Pienistä yrityksistä 12 prosenttia, keskisuurista yrityksistä 21 prosenttia ja suurista peräti 44 prosenttia ilmoitti työntekijän väärinkäytöksistä yritystä kohtaan. Väärinkäytökset keskittyivät kahdelle alalle; kaupan alalle, jossa väärinkäytöksistä raportoi joka neljäs yritys (25 %) ja rakennusalalle, jossa väärinkäytöksistä raportoi joka viides yritys (20 %). Teollisuudessa väärinkäytöksiä oli vähiten (13 %). Väärinkäytöksistä osa on tarkoituksellisia ja osa on tietämättömyydestä tai inhimillisestä virheestä johtuvia.

Väärinkäytökset asiakasta kohtaan olivat vastaajayrityksissä melko harvinaisia tai ne jäivät havaitsematta. Viisi prosenttia kaikista yrityksistä ilmoitti väärinkäytöksistä asiakasta kohtaan. Palvelualalla osuus oli korkein, seitsemän prosenttia. Teollisuudessa osuus oli pienin, yksi prosentti.

Lähetimme asiakkaan omistamaa aineistoa väärien henkilöiden nähtäväksi. Virhe oli inhimillinen eikä tarkoituksellinen tai tuottamuksellinen. (Palvelualan yritys, alle 50 henkilöä)

Taustaselvitykset työntekijöistä ja avainhenkilöistä ja yhteistyökumppanien ja alihankkijoiden luotettavuuden arviointi

Yrityksistä kolmannes tekee taustaselvityksiä työntekijöistä, neljä kymmenestä avainhenkilöistä ja yli puolet (58 %) arvioi yhteistyökumppanin luotettavuutta. Moni yritys on törmännyt epäluotettavaan yhteistyökumppaniin, mikä tulee esille luvussa kuusi (toimintaan liittyvät riskit). Yhteistyökumppanien luotettavuuden arviointi edellyttää kokonaistarkastelua - ei ainoastaan rekistereistä tai esimerkiksi luotettava kumppani -järjestelmistä saatavaa tietoa. Luotettavuuden arviointi sisältää yrityksen kokonaisuuden ja henkilöiden tarkastamista, ennen kuin yritys voi arvioida sitä, onko kyseessä todellinen luotettava kumppani tai alihankkija. Myös alihankkijoiden referenssit on syytä tarkistaa. Valtaosa yrityksistä ilmoittaa tarkistavansa referenssejä.

Yrityksiä, jotka tarkistavat yhteistyökumppanin luotettavuuden oli eniten (70 %) rakennusalalla ja vähiten (54 %) kaupan alalla. Muilla toimialoilla osuudet olivat keskimääräisellä tasolla. Alihankkijoiden referenssien tarkistamisessa rakennusalan yritysten osuus oli myös suurin, 82 prosenttia ja kaupan alalla pienin, 51 prosenttia. Teollisuusyrityksistä 75 prosenttia ja palvelualan yrityksistä 68 prosenttia tarkistaa alihankkijoiden referenssit.

Asiakkaan luottokelpoisuuden tarkistaminen

Valtaosa (78 %) yrityksistä tarkistaa asiakkaan luottokelpoisuuden. Luottotietojen tarkistus on keino varmistaa asiakkaan maksukyky. Tarkistuksessa mahdollisesti löytyvät maksuhäiriömerkinnät kertovat siitä, että luotonantoon tai laskulla myyntiin liittyy tavanomaista suurempi luottotappioriski.

Sopimukset riskienhallintakeinona

Työntekijöillä on tiedossaan monia asioita, joita yritykset eivät halua kilpailijansa tietävän. Työsuhteen aikana tähän voi varautua muun muassa rajaamalla tiedon saatavuutta käyttöoikeuksilla (ks. luku 4). Sopimukset ja -sitoumukset ovat myös yritysten yleisesti käyttämä riskienhallintakeino. Sopimuksia tietoturvan tasosta kannattaa tehdä myös yhteistyökumppanien kanssa. Kriittisen tietopääoman jako kannattaa kuitenkin olla tarkkaan harkittua sekä yrityksen sisällä että yhteistyökumppanien kesken.

Kilpailukieltosopimuksia käytetään joka toisessa yrityksessä. Yli viisi henkilöä työllistävissä yrityksissä kilpailukieltosopimusten käyttävien yritysten osuus oli sama sekä vuosien 2005 ja 2017 mittauksissa (54 %). Pienissä yrityksissä kilpailukieltosopimukset ovat edelleen harvinaisempia (46 %) kuin suurissa (74 %) yrityksissä, vaikka pienet yritykset ovat usein haavoittuvampia tilanteissa, joissa yrityssalaista tietoa siirtyy kilpailijalle. Kilpailukieltosopimusta käyttää yli puolet teollisuuden ja palvelualan vastaajista ja lähes joka toinen kaupan alan vastaajayritys.
Taustaselvitysten ja huolellisen rekrytoinnin lisäksi yritysten pitäisi panostaa ainakin kirjallisen työsopimuksen ja työntekijän salassapitositoumuksen tekemiseen. Näiden avulla voidaan vähentää riskiä esimerkiksi asiakasrekisteriin ja hintapolitiikkaan liittyviin väärinkäytöksiin. Nämä ovat tyypillisiä esimerkkejä työsuhteen päättyessä havaitusta tiedon luvattomasta kopioinnista. Nämä vähentävät myös kilpailukieltosopimusten tarvetta.

Työsuhteen päätyttyä työntekijää sitoo rikoslaki ja mahdollisesti allekirjoitettu salassapitosopimus tai kilpailukieltosopimus. Salassapitositoumuksen tekeminen on riskienhallintakeinona helpompi kuin kilpailukieltosopimus, jota helposti tehdään laajemmin kuin laki sallii. Kilpailukieltosopimuksen käyttöä, sisältöä, laajuutta ja kestoa on rajoitettu työsopimuslaissa. Työsopimuslain mukaan kilpailukieltosopimuksen tekemiseen on oltava työnantajan toimintaan liittyvä erityisen painava syy, jollainen voi olla muun muassa työnantajan tarve suojata liike- ja ammattisalaisuuksiaan. Kilpailukieltosopimus, jolle ei ole perusteltua syytä, ei sido työntekijää. Kilpailukieltosopimus ei sido työntekijää myöskään esimerkiksi silloin, jos yritys on irtisanonut työntekijän tuotannollisin ja taloudellisin perustein. Kilpailukieltosopimuksen laatiminen voi myös heikentää työntekijän motivaatiota, mikäli sopimuksella käytännössä pyritään estämään työntekijän siirtyminen muiden työnantajien palvelukseen.

Henkilön siirtyessä toisen työnantajan palvelukseen epäilys tietovuodosta.
(Palvelualan yritys, alle 50 henkilöä)

Salassapitosopimuksia tai -sitoumuksia ei ole tehnyt viidennes yrityksistä. Salassapitosopimusten teko on pienissä yrityksissä huomattavasti harvinaisempaa kuin suurissa yrityksissä. Tämä lisää pienten yritysten haavoittuvuutta. Pienistä 23 prosenttia, keskisuurista 11 prosenttia, mutta suurista yrityksistä vain kolme prosenttia ei ole tehnyt salassapitosopimuksia tai -sitoumuksia.

Tietosuoja ja varautuminen EU:n tietosuoja-asetukseen

EU:n uuden tietosuoja-asetuksen soveltaminen alkaa 25.5.2018. EU:n tietosuoja-asetus tuo lisää velvoitteita rekisterinpitäjälle ja henkilötietojen käsittelijälle.

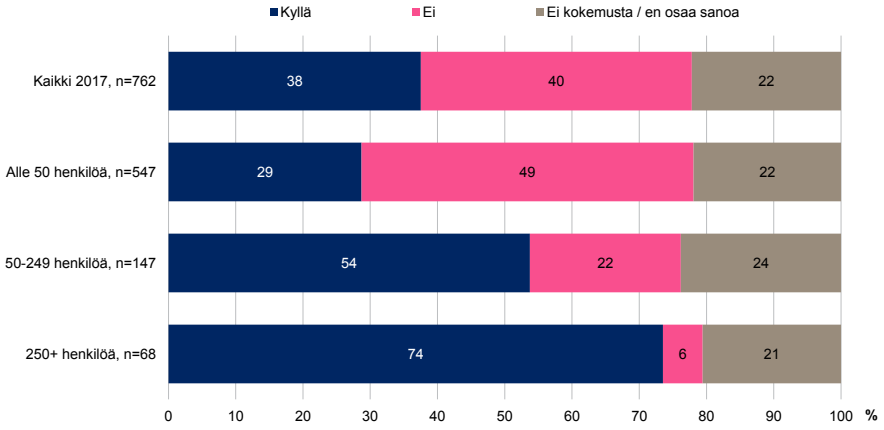
Papereita, joissa oli henkilötietoja, meinasi joutua tavalliseen roskakoriin, ei silppuriin.
(Palvelualan yritys, alle 50 henkilöä)

Yritysturvallisuuskyselyyn vastanneista yrityksistä vain 38 prosenttia on varautunut uuteen EU:n tietosuoja-asetukseen. Yhtä suuri osuus (40 %) ei ole varautunut tietosuoja-asetukseen, ja vajaa viidesosa ei osaa ottaa kantaa asiaan. Keskimääräistä heikompaa varautuminen on henkilömäärältään pienissä yrityksissä (29 %) sekä rakennusalalla (16 %) ja teollisuudessa (31 %). Kaupan ja palvelualan yrityksistäkin vain neljä kymmenestä on varautunut muutokseen. Käytännössä mitä suurempi yritys, sitä paremmin yritys on varautunut tietosuoja-asetukseen. Pienistä, alle 50 henkilöä työllistävistä yrityksistä vajaa kolmannes, keskisuurista yrityksistä puolet ja suurista yrityksistä kolme neljästä on varautunut asetukseen.

Miten yritys voi varautua tietosuoja-asetukseen?

- Selvitä tuleeko yritykseen nimetä tietosuojavastaava. Tietosuojavastaavan tehtävänä on varmistaa tietosuojavelvoitteiden noudattaminen ja toimia yhteyshenkilönä viranomaisiin ja rekisteröityihin. Tietosuojavastaava voi kuulua henkilöstöön tai hän voi toimia sopimuksen perusteella.
- Ota huomioon toiminnassasi osoitusvelvollisuus. Yrityksen pitää pystyä osoittamaan, että lainsäädännön vaatimukset on otettu sen toiminnassa huomioon.
- Huomioi vahvistuvat yksilön / rekisteröidyn oikeudet. Uusia oikeuksia ovat esim. oikeus tulla unohdetuksi ja oikeus siirtää tiedot järjestelmästä toiseen.
- Valmistaudu ilmoittamaan henkilötietoihin kohdistuvasta tietoturvaloukkauksesta valvovalle viranomaiselle 72 tunnin määräajassa
- Tarkista ja tarvittaessa päivitä tietosuojaa koskevat sopimukset. Asetus mm. edellyttää kirjallista sopimusta, jos henkilötietojen käsittelyä on ulkoistettu (esim. asiakkaisiin kohdistuvaa myyntityötä tekevä alihankkija tai ulkopuolinen tietohallinnon tarjoaja.)
- Osa yrityksistä on velvollinen tekemään henkilötietojen käsittelyä koskevan vaikutusarvion (Data protection impact assessment).
- Varaudu hallinnollisen sakon varalta. Sanktiotaso on korkea: 10 tai 20 miljoonaa euroa tai 2 tai 4 prosenttia yrityksen maailmanlaajuisesta kokonaisliikevaihdosta.

Onko yrityksenne varautunut 25.5.2018 voimaan tulevaan EU:n tietosuoja-asetukseen?

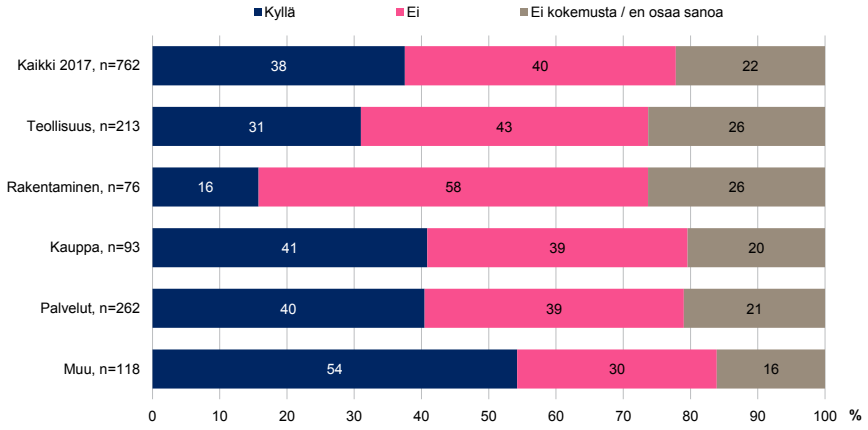


n=kaikki vastaajat

Taloustutkimus Oy
KAUPPAKAMARI

Lähde: Yritysten rikosturvallisuus 2017.
Keskuskauppakamari ja Helsingin seudun kauppakamari.

Onko yrityksenne varautunut 25.5.2018 voimaan tulevaan EU:n tietosuoja-asetukseen?



n=kaikki vastaajat

Taloustutkimus Oy
KAUPPAKAMARI

Lähde: Yritysten rikosturvallisuus 2017.
Keskuskauppakamari ja Helsingin seudun kauppakamari.

Tietoon kohdistuvat rikokset ja väärinkäytökset

4 TIETOON KOHDISTUVAT RIKOKSET JA VÄÄRINKÄYTÖKSET

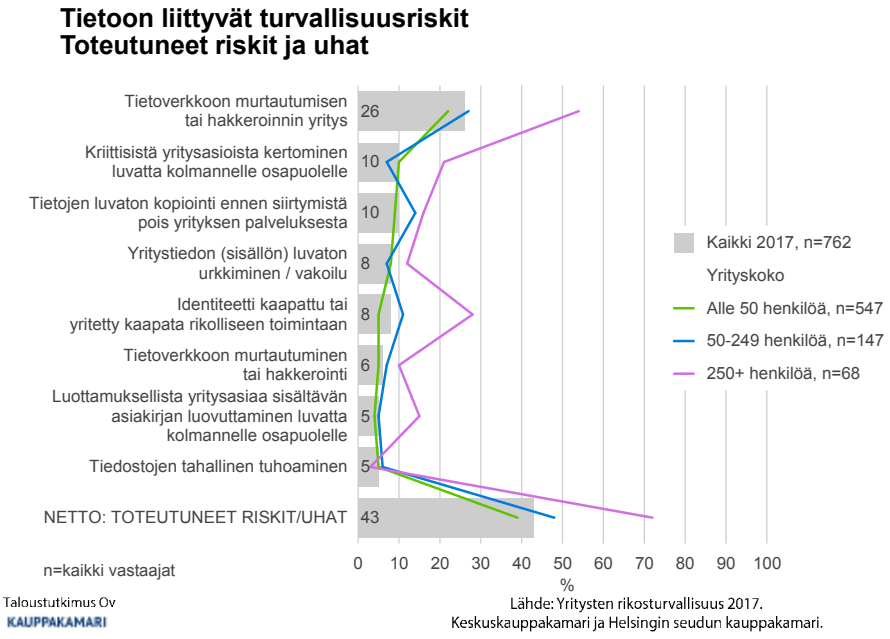
Kaikista vastanneista yrityksistä 43 prosenttia oli kokenut erilaisia tietoon kohdistuneita rikoksia tai tahallisia väärinkäytöksiä viimeisen kolmen vuoden aikana. Toteutuneita riskejä ilmoitettiin sitä enemmän, mitä suuremmasta yrityksestä oli kyse. Vastaajista 44 prosenttia arvioi tietoturvallisuusriskien lisääntyneen paljon tai jonkin verran. Yleisimmät tietoon liittyvät rikokset ja väärinkäytökset ovat samat kuin edellisellä mittauskerralla vuonna 2012: tietoverkkoon murtautumiset tai hakkeroinnin yritykset, kriittisten yritysasioiden kertominen luvatta kolmannelle osapuolelle ja tietojen luvaton kopiointi ennen siirtymistä pois yrityksen palveluksesta.

Selvityksessä tuodaan esille yrityksen havaitsemia eli ilmi tulleita tapauksia kuten tietojen luvaton kopiointia tai kriittisistä yritysasioista kertomista ulkopuoliselle. Nämä ovat tyypillistä piilorikollisuutta, joka ei näy poliisin tilastoissa. Tietoon liittyvistä riskeistä yritykset kohtaavat myös uusia voimakkaasti kasvavia rikosilmiöitä kuten identiteettikaappauksia tai uudenlaisia kyberhyökkäyksiä, joihin lukeutuu muun muassa tietojen salaaminen ja yrityksen kiristäminen.

Yritysten tietoriskit viimeisen kolmen vuoden aikana

Yrityksen tietoon liittyvät turvallisuusriskit ovat saldolukujen perusteella lisääntyneet melko selvästi viimeisen kolmen vuoden aikana (tietoturvallisuusriskejä kuvaava saldoluku: +34-->+42).

Saldoluvulla voidaan kuvata tietoriskien kehitystä ja verrata eri toimialoilla toimivien yritysten turvallisuustilannetta. Punaisella merkityt keskimääräistä suuremmat saldoluvut tarkoittavat sitä, että toimialojen yritykset pitävät muita vastaajia useammin tietoriskien kehitystä epäsuotuisana. Tietoriskien epäsuotuisaa kehitystä indikoiva saldoluku oli kaikkein heikoin kaupan alalla ja teollisuudessa. Saldoluvut heikentyivät teollisuudessa (+31-->+47), rakentamisessa (+19-->+37) ja kaupan alalla (+33-->+54). Palvelualalla saldoluku pysyi samana kuin vuonna 2012.



Lähde: Yritysten rikosturvallisuus 2017.
Keskuskauppakamari ja Helsingin seudun kauppakamari.

Kaikki yritykset	Teollisuus	Rakentaminen	Kauppa	Palvelut
+42	+47	+37	+54	+39

Näkemykset tietoriskien kehityksestä eri toimialoilla (punaisella keskimääräistä synkemmät arviot)

Henkilömäärältään suurissa yrityksissä arvioitiin useimmin, että tietoriskit ovat kasvaneet. Keskimääräistä korkeampi saldoluku (lisääntyneet - vähentyneet) kertoo riskien koetusta kasvusta. Tietoriskien osalta heikoimmat saldoluvut selittyvät tunnettujen ja usein suurien yritysten valiokoitumisella kohteeksi ja myös sillä, että yritykset havaitsevat toteutuneita tietoriskejä pieniä yrityksiä paremmin.

Kaikki yritykset	Pienet yritykset	Keskisuuret yritykset	Suuret yritykset
+42	+37	+51	+63

Näkemykset tietoriskien kehityksestä erikokoisissa yrityksissä (punaisella keskimääräistä synkemmät arviot)

Yleisimmät tietoriskit eri toimialojen yrityksissä

Yritysten kokemien tietoturvaloukkausten kärjessä olivat yritykset murtautua tietoverkkoon ja sisäiset tietoon liittyvät väärinkäytökset. Kaupan alan yritykset ilmoittivat toteutuneista tietoriskeistä kaikkein useimmin ja rakennusalan yritykset muiden toimialojen yrityksiä harvemmin. Kaupan alalla yritystiedon luvattomasta urkinnasta ilmoittaneiden osuus, 15 prosenttia, oli niin suuri, että riskienhallintaan on syytä alalla erityisesti panostaa. Muilla aloilla osuudet olivat 7- 8 prosentin tasolla.

Kaupan alan yritysten yleisimmät tietoon kohdistuvat rikokset ja väärinkäytökset

1) Tietoverkkoon murtautumisen tai hakkeroinnin yritykset (26 %, kaikkien vastaajien ka.26 %)

2) Tietojen luvaton kopiointi ennen siirtymistä yrityksen palveluksesta (15 % - toimialoista suurin osuus, kaikkien vastaajien ka. 10 %)

3) Yritystiedon luvaton urkkiminen / yritysvakoilu (15 % - toimialoista suurin osuus, kaikkien vastaajien ka. 8 %)

Muihin toimialoihin verrattuna kaupan alan yritykset raportoivat useammin kriittisistä yritysasioista kertomisesta luvatta kolmannelle osapuolelle (13 %, kaikkien vastaajien ka.10 %), toteutuneista tietoverkkomurroista (12 %, kaikkien vastaajien ka. 6 %), identiteettikaappauksista tai kaappausyrityksistä (10 %, kaikkien vastaajien ka. 8 %).

Teollisuusyritysten yleisimmät tietoon kohdistuvat rikokset ja väärinkäytökset

1) Tietoverkkoon murtautumisen tai hakkeroinnin yritykset (24 %, ka kaikki 26 %)

2) Tietojen luvaton kopiointi ennen siirtymistä yrityksen palveluksesta (9 %, kaikkien vastaajien ka. 10 %)

3) Yritystiedon luvaton urkkiminen / yritysvakoilu (7 %, kaikkien vastaajien ka. 8 %)

Rakennusalan yritysten yleisimmät tietoon kohdistuvat rikokset ja väärinkäytökset

1) Tietoverkkoon murtautumisen tai hakkeroinnin yritykset (13 %, kaikkien vastaajien ka. 26 %)

2) Tietojen luvaton kopiointi ennen siirtymistä yrityksen palveluksesta (13 %, kaikkien vastaajien ka. 10 %)

3) kriittisistä yritysasioista kertominen luvatta kolmannelle osapuolelle (11 %, kaikkien vastaajien ka.10 %)

Palvelualan yritysten yleisimmät tietoon kohdistuvat rikokset ja väärinkäytökset

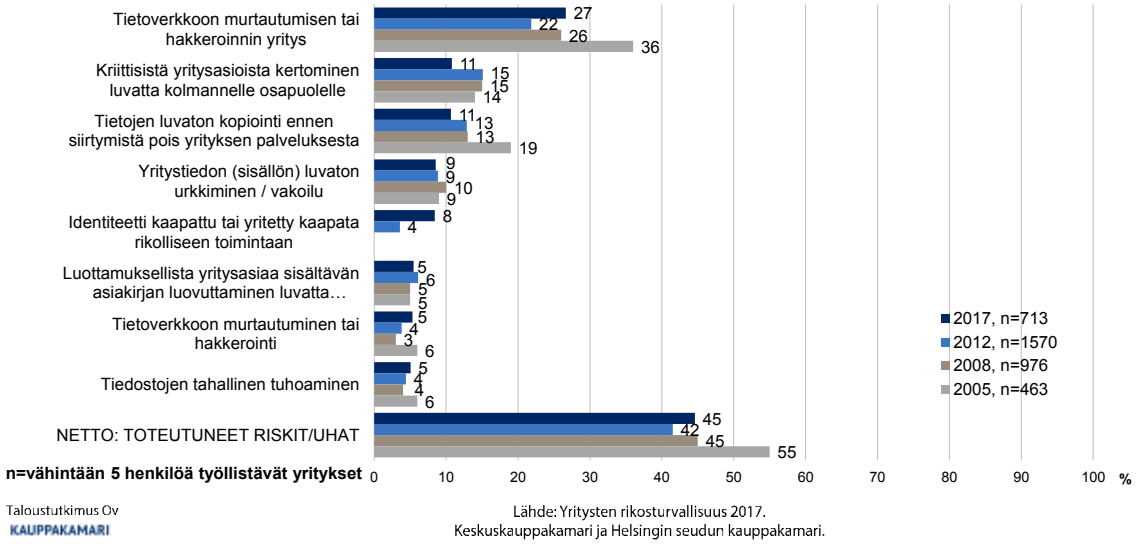
1)Tietoverkkoon murtautumisen tai hakkeroinnin yritykset (29 % - toimialoista suurin osuus, kaikkien vastaajien ka. 26 %)

2) Kriittisistä yritysasioista kertominen luvatta kolmannelle osapuolelle (11 %, kaikkien vastaajien ka.10 %)

3) Tietojen luvaton kopiointi ennen siirtymistä yrityksen palveluksesta (10 %, kaikkien vastaajien ka. 10 %)

Muihin toimialoihin verrattuna palvelualan yritykset raportoivat useammin tietoverkkoon murtautumisen tai hakkeroinnin yrityksistä.

Selvitykset 2005 - 2017: Tietoon liittyvät turvallisuusriskit
Toteutuneet riskit ja uhat



Taloustutkimus Oy
KAUPPAKAMARI

Lähde: Yritysten rikosturvallisuus 2017.
Keskuskauppakamari ja Helsingin seudun kauppakamari.

Kasvaneet tietoriskit: Identiteettikaappaukset ja tietomurron yritykset

Identiteetin kaappaukset tai kaappauksen yritykset

Identiteetin kaappaaminen on vakava ja nopeasti kasvava rikoksentekomuoto, jonka uhreina ovat yhtälailla yksittäiset henkilöt kuin yritykset. Identiteettikaappaukseen liittyy läheisesti niin yrityksen tietojen luvaton muuttaminen kuin väärentäminenkin.

Vuoden 2017 yritysturvallisuuskyselyssä tietoon kohdistuvista riskeistä nousi esille lukuisat tapaukset, joissa yrityksen identiteetti on kaapattu tai yritetty kaapata. Yleensä yritystä on haluttu erehdyttää maksamaan pieniä tai isoja summia rikollisen tilille. Huijausten yrityksiä ja identiteettivarkauksia on tehty kaiken kokoisiin yrityksiin. Yritykset kertoivat tapauksista myös avoimissa vastauksissaan.

Suuret yritykset näyttävät valikoituvan usein rikoksen kohteeksi. Henkilömäärältään pienistä yrityksistä viisi prosenttia, keskisuurista yrityksistä 11 prosenttia ja suurista yrityksistä peräti 28 prosenttia ilmoitti, että yrityksen identiteetti on kaapattu tai yritetty kaapata.

Vertailu eri kyselyjen välillä kuvaa ilmiön kasvua. Kun vuonna 2012 kolme prosenttia kaikista yrityksistä ja neljä prosenttia yli viisi henkilöä työllistävistä yrityksistä ilmoitti, että yrityksen identiteetti on kaapattu tai yritetty kaapata, vuonna 2017 osuus nousi molemmissa kohderyhmissä kahdeksan prosenttiin. Vuonna 2017 osuudet vaihtelivat toimialasta riippuen seitsemän ja kymmenen prosentin välillä, kun osuudet viisi vuotta aiemmin olivat kolmen ja viiden prosentin välillä. Sekä vuonna 2017 että 2012 osuudet olivat korkeimmat kaupan alalla (vuonna 2017: 10 % ja vuonna 2012: 5 %).

Kyselyssä ilmennyt ilmiön laajuus ja lukuisat tapaukset antavat vahvan viestin. Yritysten pitää ottaa riskienhallinnassaan ja henkilöstölle annettavassa ohjeistuksessa vakavasti ilmiö.

Identiteettikaappauksien avulla toteutetaan erilaisia petoksia, joilla rikollinen tavoittelee taloudellista hyötyä. Esimerkiksi toimitusjohtajahuijauksissa voi olla kyse myös identiteettivarkaudesta. Yritysten kohtaamia erityyppisiä petoksia ja petosyrityksiä käsitellään tarkemmin luvussa kuusi (yritysten toimintaan liittyvät riskit).

Luottokorttitiedot varastettu ja käytetty sitä tietämättämme. Facebook-tili otettu haltuun.
(Alle 50 henkilöä työllistävä kaupan alan yritys)

Yrityksemme ohjattiin maksamaan maksu väärälle tilille eli alkuperäinen vastaanottaja ei koskaan saanut suoritusta. Kysymyksessä oli sähköpostitilin kaappaus.
(Alle 50 henkilöä työllistävä teollisuusyritys)

Tietomurrot ja tietomurron yritykset

Vuonna 2017 yritystoimintaa haittasivat kyberhyökkäykset, jossa kiristäjävirusohjelman avulla yritettiin kaapata tai lukita tietoja ja vaatia niistä lunnaita. Hyökkäykseltä suojautuminen edellyttää, että tietokoneen päivitykset pidetään ajan tasalla. Myös varmuuskopiot turvaavat yrityksen tietoja. Yrityksen kannattaa myös ohjeistaa työntekijöitä tietoturvahyökkäysten varalle. Viestintäviraston mukaan kiristyshaittaohjelmia levitetään sekä hyökkäämällä suoraan järjestelmiin tietomurtojen ja haavoittuvuuksien avulla että perinteisten menetelmien kuten sähköpostin liitetiedostojen avulla. Osa yrityksistä ilmoitti myös joutuneensa palvelunestohyökkäyksen kohteeksi. Viestintävirasto on myös tehnyt ohjeen, jossa kerrotaan palvelunestohyökkäyksen torjumisesta ja toimintaohjeista palvelunestohyökkäyksen kohteeksi joutuneelle.

Dataosaamisemme ei riitä estämään tietovarkauksia. (Kaupan alan yritys, alle 50 henkilöä)

Olimme palvelunestohyökkäyksen kohteena. Torjunta kallista.
(Alle 50 henkilöä, muu toimiala)

Zeptovirus pääsi verkkoon ja salasi tiedostoja ja automaattikopioinnin palvelimelle ja kannettavaan koneeseen tallennetun varmuuskopion. Nyt otamme tiedoista automaattisesti SyncBack -ohjelmalla joka viikonpäivälle omalle tikulle varmuuskopion.
(Alle 50 henkilöä työllistävä teollisuusyritys)

Yrityksen ulkopuolinen taho / alihankkijan edustaja ei noudattanut periaatteita turvallisuudesta. Tällöin havaittiin tietomurtoyritys, joka olisi voinut olla kohtalokas. Onneksi tilanne huomattiin ajoissa ja asia saatiin järjestykseen.
(Yli 250 henkilöä työllistävä kaupan alan yritys)

Kehittynyt yrityssalaisuuksien urkinta, liittyen normaaleihin yrityksen käyttämiin tietoyhteyksiin.
(Alle 50 henkilöä työllistävä teollisuusyritys)

Joka neljäs (26 %) yritys ilmoitti, että yrityksen tietoverkkoon oli yritetty murtautua. Suuret yritykset raportoivat tietomurron yrityksistä selvästi muita yrityksiä useammin ja useammin kuin vuonna 2012 (43 % -->54 %). Suuret yritykset saattavat valikoitua kohteeksi tunnettuuden vuoksi. Suojaamisessa isojen yritysten ongelmana on se, että ohjelmistoja, käyttäjiä ja työasemia on paljon ja päivitykset ovat aikaa vieviä. Suuret yritykset onnistuvat kuitenkin todennäköisesti suojaamaan tietoverkkoaan aikaisempaa paremmin, sillä yhä useampi ilmoittaa tietomurtojen yrityksistä, mutta toteutuneista tietomurroista ilmoittaneiden osuus ei ole kasvanut edellisestä mittauskerrasta. Toteutuneista tietomurroista ilmoitti kymmenesosa suurista yrityksistä vuosina 2017, 2012 ja 2005. Toteutuneiden tietomurtojen määrä on lievässä kasvussa edellisestä mittauskerrasta niin kaikkien yritysten tarkastelussa (4 %-->6 %) kuin yli viisi henkilöä työllistävien yritysten tarkastelussa (4 %-->5 %).

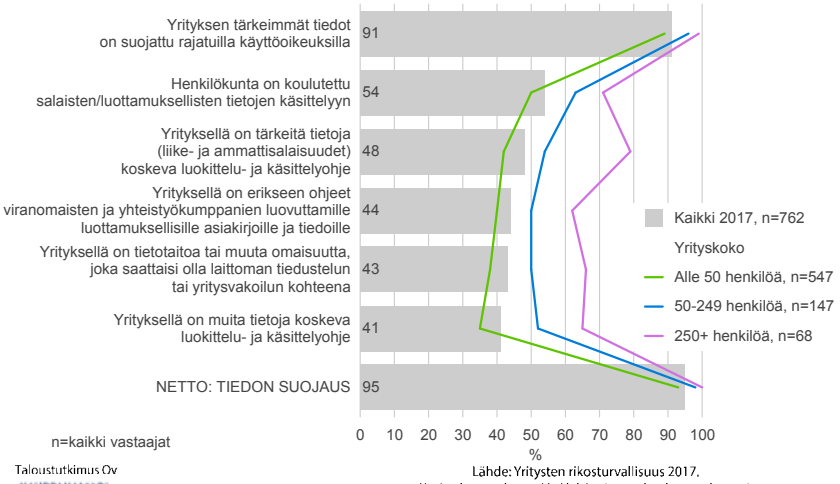
Yleisimmät riskienhallintakeinot tiedon suojaamiseksi

Yrityksistä 43 prosenttia tunnistaa, että niillä on tietotaitoa tai muuta omaisuutta, joka saattaisi olla laittoman tiedustelun kohteena. Edelleen merkittävä osa yrityksistä ei osaa sanoa, mitä tietoja ulkopuolinen tunkeutuja tai vaikkapa yrityksen oma työntekijä voisi viedä eli yrityksen liiketoiminnalle kriittistä tietoa ei tunnisteta. Yrityksen on hyvä myös tunnistaa yrityksen hallussa oleva asiakkaiden tai viranomaisten luottamuksellinen tieto. Yritystiedon luvattomasta urkinnasta tai vakoilusta ilmoitti lähes kymmenesosa yrityksistä. Urkintatapauksista huolimatta kaupan alan yrityksistä vain kolmannes tunnistaa, että niillä on kilpailijaa kiinnostavaa tietoa. Teollisuudessa oli eniten (50 %) yrityksiä, jotka tunnistavat, että niillä on tietoa, joka saattaisi olla laittoman tiedustelun tai yritysvakoilun kohteena.

Yrityksen pitää valmistautua tietoturvaloukkauksiin on sitten kyse ennakoivista toimista kuten varmuuskopioinnista ja virustorjunnasta tai jälkikäteisistä toimista kuten kriisiviestinnästä. Yrityksen on hyvä tietää, miten tietoturvaloukkaustilanteissa toimitaan ja miten tietoturvaloukkauksia voitaisiin estää. Suuri osa tietoturvaloukkauksista tapahtuu inhimillisten virheiden tai tekijöiden edesauttamana ja muistakin tapauksista suuri osa olisi estettävissä. Käytännössä kuitenkin varaustoimien laajuuteen vaikuttaa tarkoituksenmukaisuus ja kustannukset sekä toisaalta suojaustarpeet ja toiminnan luonne. Sataprosenttista turvallisuutta ei koskaan ole mahdollista saavuttaa.

Yrityksen tietoturvan rakentaminen lähtee pitkälti siitä, että yritys tunnistaa, mikä on salassa pidettävää tai luottamuksellista tietoa ja mikä tieto ei saa päätyä ulkopuolisille. Tietojen luokittelu vaikuttaa siihen, missä määrin tietoa pitää suojataa tietoisuutta lisäämällä, teknisillä suojauskeinoilla, tiloja ja toimintaympäristöä turvaamalla (luku 5) tai esimerkiksi tietoturvaa edistävillä rekrytointi- ja sopimuskäytännöillä (luku 3). Yrityksen kannattaa tehdä myös säännöllisiä riskikartoituksia, tunnistaa tietoturvaloukkauksien tekoa helpottavia haavoittuvuuksia ja seurata ja analysoida organisaation tietojärjestelmiä ja tietoliikennettä.

Tietoon liittyvät turvallisuusriskit
Käytetyt riskinhallintakeinot

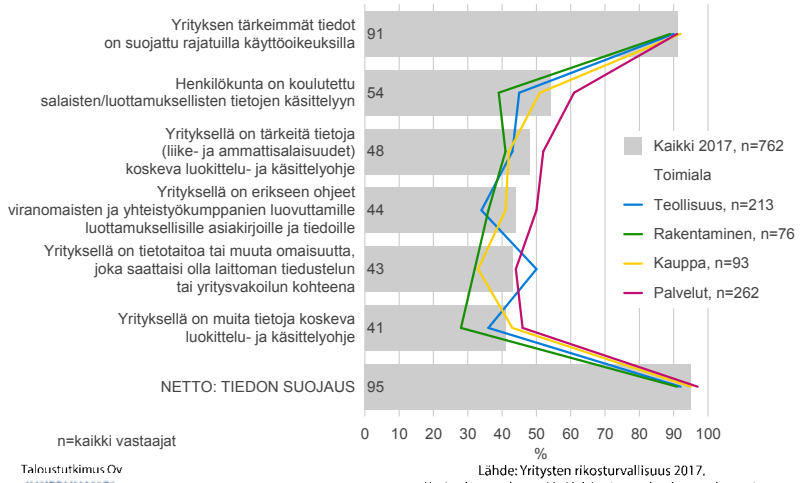


n=kaikki vastaajat

Taloustutkimus Oy
KAUPPAKAMARI

Lähde: Yritysten rikosturvallisuus 2017.
Keskuskauppakamari ja Helsingin seudun kauppakamari.

Tietoon liittyvät turvallisuusriskit
Käytetyt riskinhallintakeinot

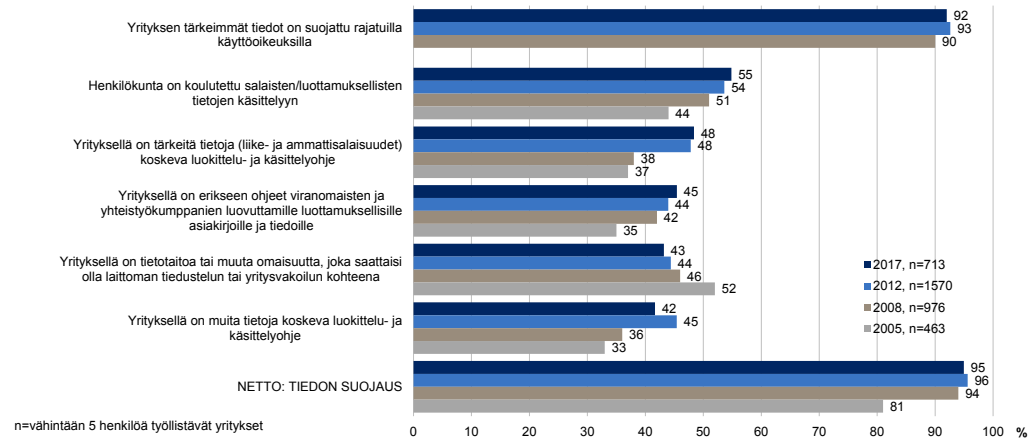


n=kaikki vastaajat

Taloustutkimus Oy
KAUPPAKAMARI

Lähde: Yritysten rikosturvallisuus 2017.
Keskuskauppakamari ja Helsingin seudun kauppakamari.

Tietoon liittyvät turvallisuusriskit
Käytetyt riskinhallintakeinot



n=vähintään 5 henkilöä työllistävät yritykset

Taloustutkimus Oy
KAUPPAKAMARI

Lähde: Yritysten rikosturvallisuus 2017.
Keskuskauppakamari ja Helsingin seudun kauppakamari.

Seuraavat suojauskeinot ovat tukijalkoja toimivalle tietoturvalle ja vaikuttavat olennaisesti siihen, missä määrin yritys saa lainsuojaa tilanteissa, joissa yritystietoa loukataan.

1. Tietojen luokittelu- ja käsittelyohjeet

Kaikissa yrityksissä on luottamuksellisen tiedon lisäksi yrityksen sisäistä tietoa ja julkista tietoa. Liike- ja ammattisalaisuuksien käsittelyä koskevan ohjeen lisäksi työnantajan kannattaisi tehdä myös muita tietoja koskeva käsittelyohje tai sisällyttää nämä samaan ohjeeseen. Yksinkertaisimmillaan ohje voi jakaa kaikki yrityksen tiedot julkisiin ja sisäisiin tietoihin. Ohjeet voidaan sisällyttää yrityksen omiin yleisiin ohjeisiin tai sitten niistä voidaan laatia omat erilliset ohjeet vain niille, jotka käsittelevät tietoa.

Tiedon luokittelu- ja käsittelyohjeeseen sisällytetään yleensä:

- tiedon luokittelun perusteet (salainen, luottamuksellinen, sisäinen, julkinen)
- tiedon käsittely liiketoiminnan tilanteissa
- tiedon käsittely tiedon elinkaaren aikana (käsittely, muuttaminen, säilyttäminen, jakelu ja hävittäminen)

Yritykset tekevät aikaisempaa enemmän ohjeita liike- ja ammattisalaisuuksien käsittelystä. Näiden ohjeiden laatiminen on välttämätöntä, jotta yritys voi suojata tietojaan ja kouluttaa henkilökuntaansa toimimaan oikein.

Yrityksistä lähes puolet (48 %) oli laatinut ohjeen liike- ja ammattisalaisuuksien käsittelystä. Pienten ja keskisuurten yritysten haavoittuvuutta tietoturvaloukkaustapauksissa lisää se, että yli puolet (56 %) pienistä yrityksistä ja 40 prosenttia keskisuurista yrityksistä ei ollut tehnyt ohjeita liike- ja ammattisalaisuuksien käsittelyyn.

Palvelualalla tietoa suojataan keskimäärin muita toimialoja monipuolisemmin. Palvelualan yrityksistä joka toisella ja muilla toimialoilla neljällä kymmenestä oli ohjeet liike- ja ammattisalisuuksien käsittelyyn. Verrattuna viisi vuotta aiemmin tehtyyn mittauskertaan, käsittelyohjeet ovat yleistyneet erityisesti suurissa yrityksissä (69 %-->79 %), kun taas muissa yrityksissä muutokset ovat olleet melko pieniä. Vuonna 2017 yrityksistä 41 prosentilla oli myös muita tietoja koskeva luokittelu- ja käsittelyohje.

Henkilön, jolla pääsy melko kriittisiin tietoihin, siirtyminen kilpailijalle. Tämän jälkeen rajauksen tiukentaminen. (Alle 50 henkilöä työllistävä palvelualan yritys)

2. Rajatut käyttöoikeudet

Rajaamalla tiedon tai tietojärjestelmän käyttöoikeuksia yritys voi turvata tiedon luottamuksellisuutta, eheyttä ja tarkoituksenmukaista saatavuutta. Nämä ovat peruselementit tietoturvan arvioimisessa.

- Luottamuksellisuus on sen varmistamista, että tietoa pääsevät näkemään tai käsittelemään vain ne henkilöt, joilla on siihen oikeutus. Tässä tiedonsiirron salaus ja rajatut käyttöoikeudet ovat keskeisessä asemassa.
- Eheys on sen varmistamista, että vain oikeutetut henkilöt voivat muokata tietoa. Yrityksen identiteetin väärinkäytökset esim. sähköpostiosoitetta väärentämällä ovat esimerkki riskeistä tiedon eheydelle.
- Saatavuus tarkoittaa sitä, että tieto on auktorisoitujen käyttäjien käytettävissä tarvittaessa. Palvelunestohyökkäys on esimerkki tiedon saatavuuden estymisestä. Tiedon saatavuutta voidaan parantaa esimerkiksi palveluita tarjoavien järjestelmien hajauttamisella ja kahdentamisella.

Valtaosa (91 %) kaikista yrityksistä suojaa tärkeimpiä tietojaan rajaamalla tiedon käyttäjien määrää.

Osuudessa ei ole merkittäviä eroja toimialan perusteella. Pienissä yrityksissä riskienhallintakeinon käyttö on lähes keskimääräisellä tasolla, kun taas keskisuurista ja suurista yrityksistä lähes kaikki suojaavat tärkeimpiä tietoja rajaamalla tiedon käyttäjien määrää.

3. Henkilökunta koulutetaan salaisten/ luottamuksellisten tietojen käsittelyyn

Tietoaineiston käsittely huolimattomasti, salassa pidettävän tiedon vaarantuminen, koska käsittelijä ei ollut sisäistänyt ohjeita (Yli 250 henkilöä työllistävä palvelualan yritys)

Henkilökunnan koulutus on tärkeä keino edistää tietojen käsittelyohjeiden sisäistämistä ja ohjeiden noudattamista. Koulutuksella ehkäistään tehokkaasti esimerkiksi kriittisistä yritysasioista kertomista. Joka toisessa (54 %) yrityksessä henkilökuntaa koulutetaan salaisten tai luottamuksellisten tietojen käsittelyyn. Teollisuudessa ja rakennusalalla on vielä enemmän yrityksiä, joissa ei kouluteta salaisten tai luottamuksellisten tietojen käsittelyyn kuin yrityksiä, joissa koulutusta on. Kaupan alallakin lähes joka toinen yritys ei kouluta salaisten tai luottamuksellisten tietojen käsittelyyn. Palvelualalla reilu kolmannes yrityksistä ei kouluta salaisten tai luottamuksellisten tietojen käsittelyyn.

Omaisuuteen kohdistuvat rikokset ja väärinkäytökset

5 OMAISUUTEEN KOHDISTUVAT RIKOKSET JA VÄÄRINKÄYTÖKSET

Kaikkiaan 42 prosenttia kaikista vastaajayrityksistä on kokenut yrityksen omaisuuteen kohdistuneita rikoksia tai väärinkäytöksiä viimeisen kolmen vuoden aikana. Vaikka enemmistöllä (73 %) yrityksistä omaisuuteen kohdistuvat turvallisuusriskit ovat pysyneet ennallaan viimeisen kolmen vuoden aikana, turvallisuusriskejä kuvaava saldoluku nousi vuonna 2012 tehtyyn kyselyyn verrattuna (14-->22). Joka neljännessä (25 %) yrityksessä omaisuuteen kohdistuvat turvallisuusriskit ovat lisääntyneet paljon tai jonkin verran.

Yritysten omaisuusriskit viimeisen kolmen vuoden aikana

Saldoluvulla voidaan kuvata omaisuusriskien kehitystä ja verrata eri toimialoilla toimivien yritysten turvallisuustilannetta. Punaisella merkityt keskimääräistä suuremmat saldoluvut tarkoittavat sitä, että toimialojen yritykset pitävät muita vastaajia useammin omaisuusriskien kehitystä epäsuotuisana. Yrityksen omaisuusriskien kehitystä kuvaavat saldoluvut olivat heikoimmat rakennusalalla ja kaupan toimialoilla. Kun katsotaan yritysten ilmoittamia toteutuneita riskejä (varkaudet, murrot ja ilkivalta, osuudet olivat myös korkeimmat rakennusalalla ja kaupan alalla.

Yritysten hallussa oleva asiakkaiden tieto ja omaisuus

Asiakkaiden tietoja on suurella osalla kaikista yrityksistä. Asiakassopimuksissa määritellyt tiedon suojaamisen velvoitteet ovat viimeisten vuosien aikana tiukentuneet ja tiedon suojaaminen tietoverkossa on noussut tärkeään asemaan. Kolmella neljästä yrityksestä on hallussaan asiakkaiden tietoja. Pienistä yrityksistä 72 prosentilla, keskisuurista yrityksistä 80 prosentilla ja suurista yrityksistä 82 prosentilla on asiakkaiden tietoja.

Palvelualalla valtaosalla (82 %) yrityksistä on hallussaan asiakkaan tietoja. Joka toisella (54 %) rakennusalan yrityksellä ja 69 prosentilla kaupan ja teollisuuden yrityksistä on hallussaan asiakkaiden tietoja.

Lähes joka toisella (46 %) yrityksellä on hallussaan asiakkaiden omaisuutta. Teollisuudessa joka toisella (50 %) yrityksellä, kaupan alalla neljällä kymmenestä, rakennusalalla kolmasosalla (36 %) ja palvelualalla lähes joka toisella (45 %) on hallussaan asiakkaan omaisuutta.

Pihalta ja työmaalta varastetut rakennustarvikkeet. Valvonta vaikeaa tai mahdotonta.
(Alle 50 henkilöä työllistävä rakennusalan yritys)

Työmaalla kameroiden siirtoajankohtana tapahtui murto.
(Alle 50 henkilöä työllistävä rakennusalan yritys)

Henkilökunnan tahalliset väärinkäytökset ja myymälävarkaudet.
(Yli 250 henkilöä työllistävä kaupan alan yritys)

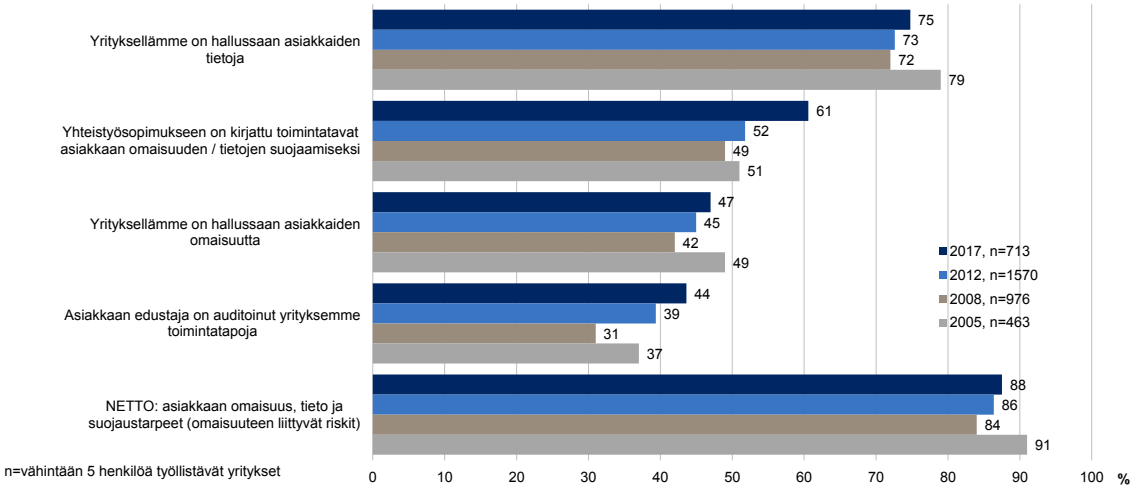
Snatteri, drogpåverkad snattare som inte kunde hållas kvar till polisen kom.
(Alle 50 henkilöä työllistävä kaupan alan yritys)

Varas leikkasi reiän aitaan ja tunkeutui pihalle ja murtautui erilliseen tuotantotilaan jossa ei ollut hälyttimiä, mutta videovalvonta kylläkin.
(Alle 50 henkilöä työllistävä kaupan alan yritys)

Kaikki yritykset	Teollisuus	Rakentaminen	Kauppa	Palvelut	Muu toimiala
+22	+21	+38	+26	+18	+19

Näkemykset omaisuusriskien kehityksestä eri toimialoilla (punaisella keskimääräistä synkemmät arviot)

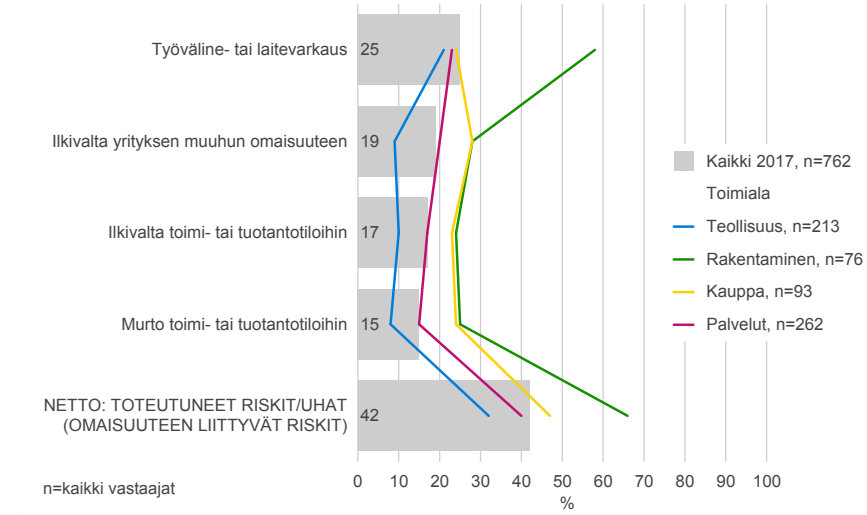
Selvitykset 2005 - 2017:
Yrityksen hallussa oleva asiakkaan omaisuus, tieto ja suojaustarpeet



Taloustutkimus Oy
KAUPPAKAMARI

Lähde: Yritysten rikosturvallisuus 2017.
Keskuskauppakamari ja Helsingin seudun kauppakamari.

Omaisuuteen liittyvät riskit
Toteutuneet riskit ja uhat



Taloustutkimus Oy
KAUPPAKAMARI

Lähde: Yritysten rikosturvallisuus 2017.
Keskuskauppakamari ja Helsingin seudun kauppakamari.

Yrityksiin kohdistuvien varkauksien, murtojen ja ilkivallan yleisyys

Kaikista vastaajayrityksistä joka neljänneltä (25 %) oli varastettu työvälineitä- tai laitteita viimeisen kolmen vuoden aikana. Suurista yrityksistä joka toinen (50 %), keskisuurista joka neljäs (25 %) ja pienistä joka viides (22 %) oli joutunut varkauden kohteeksi. Rakennusalan yrityksistä selvästi yli puolet (58 %) oli ollut varkauden kohteena. Syynä tähän ovat vaikeasti valvottavat työmaat. Vähiten työväline- tai laitevarkauksia oli teollisuudessa (21 %). Joka neljänneltä (24%) kaupan alan ja palvelualan yritykseltä oli varastettu työvälineitä tai laitteita.

Kaikista vastanneista yrityksistä joka seitsemäs (15 %) oli joutunut murron kohteeksi viimeisen kolmen vuoden aikana. Suurista yrityksistä neljään kymmenestä (38 %), keskisuurista viidesosaan (18 %) ja pienistä yrityksistä kymmenesosaan (12 %) oli murtauduttu. Rakennusalalla ja kaupan alalla joka neljännellä oli ollut murtoja toimi- tai tuotantotiloihin. Teollisuudessa kymmenesosa (8%) ja palvelualalla seitsemäsosa (15 %) yrityksistä oli joutunut murron kohteeksi.

Lähes joka viides (17 %) yritys oli joutunut toimi- tai tuotantotiloihin kohdistuvan ilkivallan kohteeksi. Suurista vastaajayrityksistä 41 prosenttia, keskisuurista yrityksistä viidesosa (20 %) ja pienistä yrityksistä kymmenesosa (13 %) oli joutunut ilkivallan kohteeksi. Ilkivalta toimi- tai tuotantotiloihin oli yleisintä rakennusalalla (24 %) ja kaupan alalla (23 %). Harvinaisinta se oli teollisuudessa (10 %).

Yrityksistä 19 prosenttia ilmoitti muuhun omaisuuteen kohdistuneesta ilkivallasta. Kohteeksi oli joutunut suurista yrityksistä neljä kymmenestä (41 %), keskisuurista lähes viidesosa (18 %) ja pienistä yrityksistä kuudesosa (16 %). Ilkivalta toimi- tai tuotantotiloihin oli yleisintä rakennusalalla (28 %) ja kaupan alalla (28 %) ja harvinaisinta teollisuudessa (9 %).

Asiakkaan omaisuuden ja tietojen suojaaminen: sopimukset ja auditointi

Omaisuutta tai tietoja luovutettaessa osapuolet kirjaavat yhteistyösopimukseen tai sen liitteeseen toimintatavat asiakkaan omaisuuden tai tietojen suojaamisesta. Kaikista yrityksistä 59 prosentilla on sopimukseen kirjattu toimintatavat tietojen suojaamiseksi. Yleisintä tämä on suurten yritysten keskuudessa (75 %) ja harvinaisinta pienissä yrityksissä (54 %). Palvelualalla (63 %) ja teollisuudessa (62 %) toimintatapojen kirjaaminen omaisuuden tai tietojen suojaamiseksi on yleisintä ja harvinaisinta kaupan (46 %) ja palvelualan (45 %) yrityksissä.

Auditoimalla yritys voi varmistaa sen, miten toinen osapuoli säilyttää ja suojaa asiakkaan tietoja tai muuta omaisuutta. Auditointi vaatii ammattitaitoa ja aikaa joten sitä käytetään erityisesti isoimpiin ja tärkeimpiin sopimussuhteisiin. Auditointi on hyvin yleinen pykälä sopimuksissa, mutta käytännössä sitä toteutetaan huomattavasti harvemmin.

Asiakkaat ovat auditoineet neljää yritystä kymmenestä (42 %). Suurista yrityksistä kahta kolmesta (66 %) ja pienistä kolmasosaa (35 %) on auditoitu. Keskisuurista yrityksistä yli puolta (54 %) oli auditoitu. Yleisintä auditointi oli teollisuudessa (68 %) ja harvinaisempaa kaupan alalla (25 %) sekä rakennusalalla (26 %). Palvelualalla kolmasosaa (35 %) vastaajayrityksistä oli auditoitu.

Yleisimmät riskienhallintakeinot tuotannon ja toimitilojen suojaamiseksi

Yrityksessä on usein työntekijöiden ja yrityksen oman omaisuuden lisäksi hallussaan jonkun toisen, esimerkiksi asiakkaan omaisuutta. Parantamalla toimitilaturvallisuuden tasoa yritys parantaa myös esimerkiksi tietoturvallisuuden tasoa. Monet yritysturvallisuuden osa-alueet ovat yhteydessä toisiinsa ja toimitilaturvallisuutta voi kutsua yritysturvallisuuden perustaksi. Henkilökunnalla on suuri merkitys toimitilaturvallisuuden toimivuuden kannalta. Tietämätön tai välinpitämätön henkilökunta voi esimerkiksi päästää tiloihin asiattomia tahoja ja tällöin moni toimitilaturvallisuuden toimenpide menettää merkityksensä.

Yritysturvallisuuskyselyyn vastanneet yritysjohtajat kertoivat yrityksen tavoista suojata tuotantoa ja toimitiloja. Yritysten tuotanto- tai toimitilojen suojaaminen kuten myös irtaimen omaisuuden suojaaminen on pysynyt melko samanlaisena viime tutkimuskertaan verrattuna.

1.Useimmat yritykset käyttävät murtohälytystä / rikosilmoitinjärjestelmää (76 %).
Murtohälytyksen käyttö on yleisintä suurissa (94 %) ja keskisuurissa yrityksissä (88 %) ja kaupan alalla (90 %). Vähiten rikosilmoitinjärjestelmää käytetään pienissä yrityksissä (70 %) ja palvelualalla (71 %).

2. Toiseksi yleisin tapa suojata omaisuutta on henkilöstön koulutus (70 %).
Suurimmat osuudet olivat suurissa yrityksissä (91 %). Teollisuudessa, kaupan alalla ja palvelualalla henkilöstön koulutus omaisuuden suojaamiseen on lähes yhtä yleistä (70 - 72 %). Henkilöstön koulutus omaisuuden suojaamiseksi on vähäisintä pienten yritysten (64 %) keskuudessa ja rakennusalalla (57 %).

3. Kolmanneksi eniten mainintoja sai vartiointi (64 %).
Lähes kaikki suuret yritykset (96 %) käyttävät vartiointipalveluja. Keskisuurista yrityksistä vartiointia käyttää kahdeksan kymmenestä (84 %). Pienistä yrityksistä vain puolet (54 %) käytti vartiointia.

4. Kulunvalvontaa, valvontajärjestelmien toimivuuden säännöllistä testausta, videovalvontaa ja tuotanto-, toimisto- ja tuotekehitystilojen eriyttämistä käyttää kuusi kymmenestä yrityksestä.

Kulunvalvonta on yleistä suurissa yrityksissä (99 %) ja keskisuurissa yrityksissä (80 %). Pienistä yrityksistä puolet (49 %) käyttää kulunvalvontaa. Toimialoista kulunvalvonta on yleisintä teollisuudessa (67 %) ja vähäisintä palvelualalla (53 %).

Yleisintä videovalvonta on suurten (88 %) ja keskisuurten (82 %) yritysten keskuudessa ja toimialoista kaupan alalla (63 %). Videovalvonta on harvinaisinta pienissä yrityksissä (46 %) ja palvelualalla (51 %).

Tilojen eriyttäminen on melko yleistä keskisuurissa (74 %) ja suurissa (69 %) yrityksissä. Pienistä yrityksistä puolet (50 %) eriyttää tiloja. Tilojen eriyttäminen on yleisintä teollisuudessa (73 %) ja harvinaisinta palvelualalla (47 %) ja kaupan alalla (47 %).

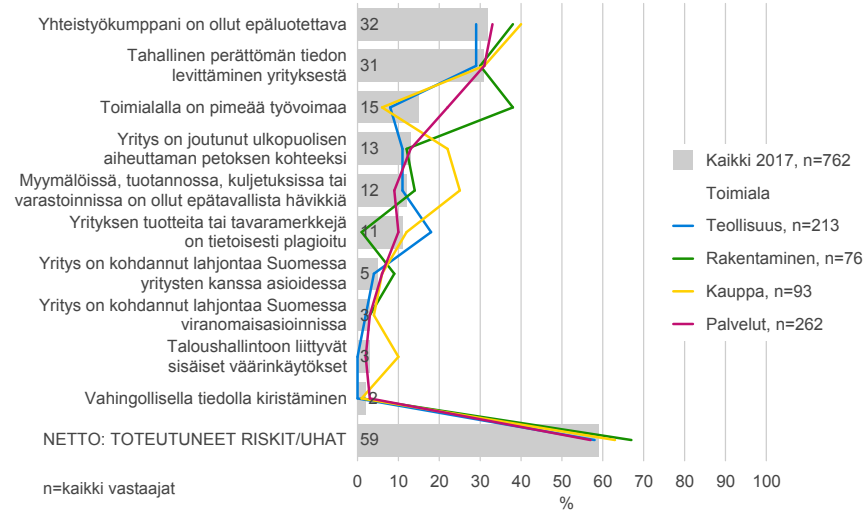
5. Puolet yrityksistä (48 %) ohjeistaa vierailukäytännöt.
Suurissa yrityksissä (88 %) vierailujen ohjeistaminen on yleisintä. Keskisuurista yrityksistä seitsemän kymmenestä (70 %) ja pienistä yli kolmannes (37 %) ohjeistaa vierailut. Vierailujen ohjeistus on yleisintä teollisuudessa (59 %) ja harvinaisinta rakennusalalla (26 %).

Toimintaan kohdistuvat rikokset ja väärinkäytökset

6 TOIMINTAAN KOHDISTUVAT RIKOKSET JA VÄÄRINKÄYTÖKSET

Yrityksen toimintaan kohdistuvista rikoksista ja väärinkäytöksistä ei ole olemassa kattavia tilastotietoja. Keskuskauppakamarin ja Helsingin seudun kauppakamarin selvitykseen vastanneet 762 yritysjohtajaa tarkastelivat aihetta hävikin, perättömän tiedon levittämisen, kiristyksen, yhteistyökumppanin epäluotettavuuden, pimeän työvoiman, lahjonnan ja taloushallintoon liittyvien sisäisten väärinkäytösten sekä erilaisten ulkopuolisten henkilöiden tekemien petosten kannalta.

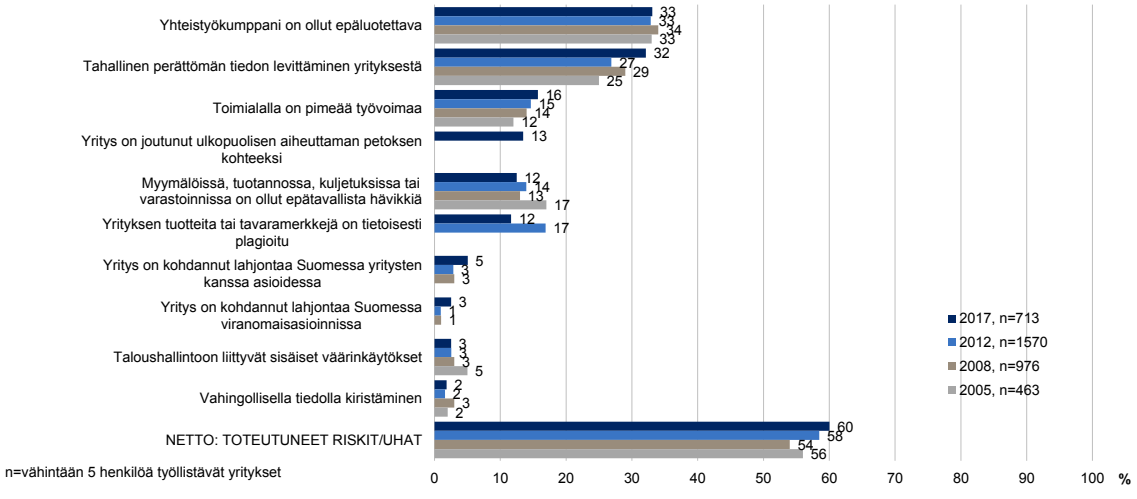
Toimintaan liittyvät riskit
Toteutuneet riskit ja uhat



Taloustutkimus Oy
KAUPPAKAMARI

Lähde: Yritysten rikosturvallisuus 2017.
Keskuskauppakamari ja Helsingin seudun kauppakamari.

Selvitykset 2005 - 2017: Toimintaan liittyvät riskit
Toteutuneet riskit ja uhat



Taloustutkimus Oy
KAUPPAKAMARI

Lähde: Yritysten rikosturvallisuus 2017.
Keskuskauppakamari ja Helsingin seudun kauppakamari.

Yrityksen toimintaan liittyvät riskit viimeisen kolmen vuoden aikana

Epäluotettava yhteistyökumppani

Yhteistyökumppanin taustatiedot olisi pitänyt selvittää paremmin ennen sopimusten tekoa.
(Alle 50 henkilöä työllistävä teollisuusyritys)

Vuoden 2017 yritysturvallisuuskyselyssä ilmeni, että joka kolmannella yrityksellä (32 %) oli huonoja kokemuksia yhteistyökumppaneista. Osuus on pysynyt samalla tasolla eri mittauskerroilla (2017, 2012, 2008 ja 2005). Vuoden 2017 kyselyssä epäluotettavasta yhteistyökumppanista raportoivia oli eniten suurissa yrityksissä, joista 47 prosenttia raportoi epäluotettavasta yhteistyökumppanista ja kaupan alalla, jossa 40 prosenttia raportoi epäluotettavasta yhteistyökumppanista.

Kaikilla aiemmilla mittauskerroilla rakennusalalla on ollut toimialoista suurin osuus yrityksiä, jotka raportoivat epäluotettavasta yhteistyökumppanista. Vuoden 2017 kyselyssä rakennusalan yrityksistä 38 prosentilla oli ollut epäluotettava yhteistyökumppani viimeisen kolmen vuoden aikana. Yhteistyökumppaniin tyytymättömien yritysten osuus rakennusalalla on kuitenkin jatkuvasti pienentynyt muutamalla prosenttiyksiköllä mittauskertojen välillä. Osuuteen voi vaikuttaa rakennusalan kaupalliset palvelut kuten tilaajavastuulain velvoitteisiin vastaava luotettava kumppani-palvelu.

Osuudet olivat keskimääräisellä kolmanneksen tasolla palvelualalla (33 %) ja teollisuudessa (29 %). Kaikilla toimialoilla on kuitenkin niin paljon yrityksiä, jotka ovat kohdanneet epäluotettavia kumppaneita, että yhteistyökumppanin luotettavuuden arviointiin pitäisi käyttää yrityksissä selvästi nykyistä enemmän aikaa. Yhteistyökumppanin luotettavuuden arviointia on käsitelty tarkemmin luvussa kolme.

Perättömän tiedon levittäminen yrityksestä

Meidän tapauksessamme haasteina ovat tietomurrot, väärien tietojen levitys ja edustussopimusten kaappaaminen.
(Alle 50 henkilöä työllistävä kaupan alan yritys)

Sähköisessä tai printtimediassa leviävä perätön tieto aiheuttaa aina haittaa liiketoiminnalle, mutta erityisesti toimialoilla, joissa asiakkaat ovat kuluttajia. Kun ensimmäisellä mittauskerralla, vuonna 2005 perättömän tiedon levittäminen oli merkittävä ongelma lähes ainoastaan rakennusalalla ja kaupan alalla, niin sen jälkeen ilmiö on ollut käytännössä yhtä yleinen kaikilla toimialoilla.

Vuonna 2017 kaikista yrityksistä lähes joka kolmas (31 %) raportoi yritystä koskevasta perättömästä tiedon levittämisestä. Vertailtaessa eri vuosina tehtyjen yritysturvallisuuskyselyjen tuloksia keskenään voidaan havaita, että viime vuosina perättömän tiedon levittäminen yrityksestä on ollut kasvussa. Perättömästä tiedon levittämisestä raportoivien osuus kasvoi viidellä prosenttiyksiköllä sekä kaikissa yrityksissä että yli viisi henkilöä työllistävissä yrityksissä. Vuosien 2005 ja 2017 välillä osuus kasvoi yli viisi henkilöä työllistävissä yrityksissä seitsemällä prosenttiyksiköllä (25 %-->32 %).

Yrityksen tuotteita tai tavaramerkkejä on tietoisesti plagioitu

Yritysten tuotteiden ja tavaramerkkien suojaaminen on tärkeää liiketoiminnan kannalta. Vastaajista joka kymmenes (11 %) ilmoitti, että yrityksen tuotteita tai tavaramerkkejä on tietoisesti plagioitu. Osuus oli keskimääräistä korkeampi keskisuurissa (14 %) ja suurissa (16 %) yrityksissä. Tuotteiden ja tavaramerkkien plagioinnista raportoitiin eniten teollisuudessa (18 %). Rakennusalalla tapauksia ei juuri ollut (1 %). Muilla toimialoilla osuus oli lähes keskimääräisellä tasolla (10 –12 %).

Yrityksen tuotteiden tai tavaramerkkien plagioinnista raportoivien yli viisi henkilöä työllistävien yritysten osuus on vähentynyt seitsemällä prosenttiyksiköllä edelliseen mittauskertaan verrattuna (17 %-->12 %).

Ulkopuolisen henkilön tekemät petokset

Poliisin mukaan petokset ovat voimakkaassa kasvussa ja niitä tehdään yhä useammin tietoverkkojen avustuksella. Kaikesta petosrikollisuudesta vain pieni osa tulee poliisin tietoon.

Yritysturvallisuuskyselyyn vastanneista 762 yrityksestä 13 prosenttia ilmoitti joutuneensa ulkopuolisen aiheuttaman petoksen kohteeksi viimeisen kolmen vuoden aikana. Monia petosyrityksiä pidetään julkisuudessa lähinnä pienten yritysten ongelmina. Tämä johtuu siitä, että pienet ja keskisuuret yritykset tuovat suuria yrityksiä useammin esille petosyrityksiä esimerkiksi yritysjärjestöjen neuvontapalveluissa. Yrityskokoluokkavertailussa ilmeni kuitenkin se, että pienissä ja keskisuurissa yrityksissä petosten kohtaaminen oli keskimääräisellä tasolla (12 -13 %), kun taas suurista yrityksistä peräti neljännes (25 %) ilmoitti ulkopuolisen tekemistä petoksista. Petoksia voidaan kohdistaa tarkoituksella suuriin yrityksiin, joiden työntekijät eivät voi käytännössä aina tuntea toisiaan. Tämä helpottaa petoksen tekoa, mikäli henkilökunta ei ole varautunut petosyritysten mahdollisuuteen.

Valelaskuja on tullut. On myös yritetty saada aikaa varojen siirtoa tekeytymällä konsernin johdon valtuuttamaksi On myös tietoisesti ostettu meiltä palveluja ja sitten jätetty maksut maksamatta.
(Yli 250 henkilöä työllistävä palvelualan yritys)

Taloudelliset riskit lisääntyvien netin kautta tapahtuvien huijausten- ja tietojärjestelmien kaappausyritysten vuoksi.
(Alle 50 henkilöä työllistävä palvelualan yritys)

Kaupan alalla yrityksiin kohdistuvia petoksia kohdattiin eniten. Kaupan alan yrityksistä peräti joka viides (22 %) ilmoitti petoksista viimeisen kolmen vuoden aikana. Palvelualalla osuus oli keskimääräisellä 13 prosentin tasolla. Osuudet olivat lähes yhtä suuria rakennusalalla, jossa 12 prosenttia yrityksistä ilmoitti petoksista ja teollisuudessa, jossa 11 prosenttia ilmoitti petoksista.

Vastaajayritysten antamista vastauksista ilmeni selvästi, että erityyppisiä petoksia ilmenee kaikilla toimialoilla. Eri huijaustyypit liittyvät usein toisiinsa. Yritysten kohtaamia petoksia ovat:

• maksuvälinepetokset (esim. luottokortin tiedon kopioiminen)

Korttitiedot anastettu - pankista otettiin yhteyttä ja kortti suljettiin.
(Alle 50 henkilöä työllistävä teollisuusyritys)

Luottokorttitiedot varastettu. Korttia käytetty tietämättämme.
(Alle 50 henkilöä työllistävä kaupan alan yritys)

Maksukortin tiedot varastettu ja tehty yksi ostos. Pankki palauttanut rahat yrityksen tilille.
(Alle 50 henkilöä työllistävä teollisuusyritys)

Maksukorttipetos, jossa henkilökunnalta jäi huomaamatta väärennetty asiakirja.
(Yli 250 henkilöä työllistävä kaupan alan yritys)

Maksuvälinepetoksista kannattaa ilmoittaa pankin lisäksi poliisille, jotta verkkorikostapaukset eivät jäisi piilorikollisuudeksi ja jotta niiden selvittämiseen osattaisiin kohdentaa riittävä määrä resursseja.

• myyntipetokset (esim. ostettavaa tavaraa ei olekaan tai se on olennaisesti erilaista ainesta)

Usein tapaukset ovat etumaksupetoksia, joissa yrityksiä pyydetään maksamaan maksu etukäteen. Tilattua tuotetta ei kuitenkaan koskaan toimiteta.

• myyjään kohdistuvat tilauspetokset

Tapauksissa on yleensä kyse siitä, että toisen henkilön henkilötiedoilla erehdytetään yritystä tilaamaan tavaraa tai tilataan tavaraa, jota ei makseta.

Ulkopuolinen taho tilasi tuotteita sähköpostitilauksella ja esiintyi toisen henkilön ja yrityksen nimissä. Petoksen yritys havaittiin ennen tavaroiden toimittamista eikä vahinkoa tapahtunut.
(50-249 henkilöä työllistävä teollisuusyritys)

Yrityksemme ohjattiin maksamaan maksu väärälle tilille eli alkuperäinen vastaanottaja ei koskaan saanut suoritusta. Kysymyksessä oli sähköpostitilin kaappaus
(Alle 50 henkilöä työllistävä teollisuusyritys)

• valelaskut, laskuvääreennökset ja harhaanjohtava markkinointi

Harhaan johtavassa markkinoinnissa yrityksiä houkutellaan epäasiallisin markkinointikeinoin sitoutumaan ei toivottuun sopimukseen. Huijauslasku näyttää usein erehdyttävästi oikealta laskulta, vaikka kyseessä on tarjous. Tapauksia on usein kesäaikaan. Yrityksen kannattaa kouluttaa ja ohjeistaa henkilöstöä tapausten varalle, koska esimerkiksi sopimusten irtisanominen on osoittautunut vaikeaksi.

Laskuväärennöksessä viestin lähettäjätiedot väärennetään muistuttamaan oikean toimittajan sähköpostiosoitetta. Yrityksen kannattaa olla varuillaan myös silloin, kun yritystä lähestytään viestillä, jossa ilmoitetaan toimittajan yhteystietojen muuttuneen ja annetaan uusi tilinumero, jonne laskut tulisi maksaa. Osa laskuväärennöksistä on tehty myös niin, että alkuperäiset laskut on varastettu kirjelaatikosta ja oikean laskuttajan tilinumero on korvattu huijarin tilinumerolla.

Nettinäkyvyyttä myyvä yritys on yrittänyt kiristää yritystämme maksamaan puolen vuoden näkyvyydestä yli 7000 €. Asiaa on hoidettu asianajotoimiston avulla ja asiasta on tulossa rikosilmoitus.
(Alle 50 henkilöä työllistävä yritys, muu toimiala)

Väärennetty tilinumero alihankkijan laskussa.
(Alle 50 henkilöä työllistävä teollisuusyritys).

Sähköisen asioinnin kanssa oltava tarkkana - mihin vastaa tai mitä lähettää.
(Alle 50 henkilöä työllistävä palvelualan yritys)

• toimitusjohtajahuijaukset

Toimitusjohtajahuijauksilla on huijattu suurten suomalaisyritysten tytäryhtiöistä jopa miljoonia euroja. Tapauksissa väärennetystä tai joskus jopa aidosta hakkeroidusta sähköpostiosoitteesta lähetetään yrityksen johtohenkilön nimissä maksukehotus taloushallintoon, josta maksu suoritetaan rikollisten tilille. Huijausyrityksiä voidaan tehostaa puhelinsoitoilla, jossa huijari esiintyy esimerkiksi yrityskauppaa hoitavana lakimiehenä.

Toimitusjohtajahuijauksena tunnettu laskutushuijaus, mutta se jäi yritykseksi.
(Alle 50 henkilöä työllistävä palveluyritys)

Försök att få betalning gjort genom e-mail från VD.
(50-249 henkilöä työllistävä teollisuusyritys)

Hävikki myymälöissä, tuotannossa, kuljetuksissa tai varastoinnissa

Hävikki voi johtua tilausvirheistä tai esimerkiksi tuotteiden vioittumisesta tai pilaantumisesta, mutta epätavalliseen hävikkiin voi olla syynä varkaudet. Epätavallisesta hävikistä myymälöissä, tuotannossa, kuljetuksissa tai varastoinnissa raportoivien yritysten osuus oli vuoden 2017 ja 2012 kyselyissä lähes sama (13 %-->12 %).

Eri vuosien kyselyjen tuloksia verratessa voidaan havaita, että hävikin määrä on vähentynyt yli viisi henkilöä työllistävissä yrityksissä vuodesta 2005 alkaen. Vuonna 2005 hävikistä raportoi 17 prosenttia yli viisi henkilöä työllistävistä yrityksistä. Vuosina 2008, 2012 ja 2017 hävikistä raportoivien yli viisi henkilöä työllistävien yritysten osuus on vakiintunut 12 ja 14 prosentin välille. Kaikilla mittauskerroilla epätavallista hävikkiä on ollut eniten kaupan ja rakennusalan yrityksissä.

Vuoden 2017 kyselyssä epätavallisesta hävikistä ilmoitti joka kymmenes teollisuuden ja palvelualan yritys. Rakennusalla epätavallista hävikkiä oli selvästi vähemmän kuin edellisellä mittauskerralla. Rakennusalan yrityksistä vain 14 prosenttia raportoi epätavallisesta hävikistä, kun vuonna 2012 joka viides (20 %) raportoi epätavallisesta hävikistä.

Kaupan alalla epätavallisen hävikin vähentäminen on ollut hitaampaa kuin rakennusalalla. Lainsäädäntö on kuitenkin viimein vastannut kauppiaiden huoleen. Vuonna 2012 tehdyssä selvityksessä kaupan alan yritykset raportoivat myymälävarkauksien ja näpistysten määrän kasvusta ja yleisestä välinpitämättömyyden signaalista tilanteessa, jossa poliisin määräämiä sakkoja ei vuoden 2008 jälkeen muunnettu vankeudeksi. Sakon muuntorangaistus kuitenkin palautettiin vuoden 2017 alusta. Sakon muuntorangaistus tarkoittaa sitä, että myymälävarkaalle määrätty sakko voidaan muuntaa vankeudeksi, jos sakkoa ei saada perityksi rahana.

Vuonna 2017 hävikistä raportoivien kaupan alan yritysten osuus on laskenut prosentilla edelliseen mittauskertaan verrattuna (26 % –25 %). Todennäköisesti epätavallisesta hävikistä raportoivien kaupan alan yritysten osuus tulee edelleen tippumaan lainsäädännön muutoksen myötä.

Työkalu ja tavarahävikki
(Yli 250 henkilöä työllistävä palvelualan yritys)

Henkilökunnan tahalliset väärinkäytökset ja myymälävarkaudet.
(Yli 250 henkilöä työllistävä kaupan alan yritys)

Pimeä työvoima toimialalla

Harmaan talouden kannalta riskitoimialoja ovat työ- ja elinkeinoministeriön mukaan rakennusala ja majoitus- ja ravitsemusala sekä kuljetusala. Majoitus- ja ravitsemusala ja kuljetusala ovat mukana yritysturvallisuuskyselyssä palvelualan vastaajaryhmässä.

Yritysturvallisuuskyselyyn vastanneista kaikista yrityksistä 15 prosenttia on kohdannut toimialalla pimeää työvoimaa. Kaikkien yritysten osuus oli sama myös edellisellä mittauskerralla vuonna 2012.

Vuoden 2017 yritysturvallisuuskyselyssä teollisuusyrityksistä vain kahdeksan prosenttia ja kaupan alan yrityksistä kuusi prosenttia raportoi pimeästä työvoimasta toimialalla. Palvelualalla pimeästä työvoimasta toimialalla raportoivien yritysten osuus on kuitenkin ollut viime vuosina selvässä kasvussa. Palvelualalla osuus oli 22 prosenttia vuoden 2017 mittauksessa, 18 prosenttia vuoden 2012 mittauksessa ja 12 prosenttia vuoden 2005 mittauksessa. Palvelualalla harmaata taloutta on pyritty kitkemään muun muassa kuitinantovelvollisuudella. Palvelualan vastaajista myös osa edustaa kuljetusalaa. Harmaan talouden ilmiöitä kuljetusalalla ovat muun muassa pimeän työvoiman käyttö ja pimeiden kuljetuspalveluiden myynti. Kuljetusyritykset ovat katsoneet, että alalla on harmaata taloutta erityisesti ulkomaisen kuljetusliikenteen vuoksi. Ravintola-alan harmaa talous on tyypillisimmillään pimeästi maksettua palkkoja, veronkiertoa ja ohimyyntiä.

Rakennusala on ollut harmaalle taloudelle otollista kasvualaa, koska työ on projektimaista, alihankintaketjut ovat tavallisia ja työvoiman tarve vaihtelee paljon. Pimeää työvoimaa esiintyy alan omien arvioiden mukaan erityisesti yksityisillä pienrakennustyömailla. Rakennusalan yrityksistä 38 prosenttia raportoi pimeästä työvoimasta toimialalla. Osuus on suuri, mutta se on pudonnut selvästi edellisestä, vuoden 2012 mittauskerrasta. Vuonna 2012 joka toinen (54 %) rakennusalan yritys oli havainnut pimeää työvoimaa toimialalla. Edellisen mittauskerran jälkeen rakennusalalla on otettu käyttöön lukuisia toimia, jolla alan harmaata taloutta kitketään:

- velvollisuus pitää esillä työmailla kuvallista henkilötunnistetta veronumeroineen (2012)
- rakentamispalvelujen tilaajan velvollisuus ilmoittaa Verohallinnolle kuukausittain
- tiedot työmaalla käytettävistä yrityksistä sekä näille maksetuista vastikkeista (2014)
- yhteisen rakennustyömaan pääurakoitsijan tai muun päätoteuttajan velvollisuus
- toimittaa Verohallinnolle verovalvontaa varten tarpeelliset tiedot yhteisellä työmaalla
- työskentelevistä työntekijöistä ja itsenäisistä työn suorittajista (2014)

Toimet ovat yritysturvallisuuskyselyn tulosten valossa tuoneet hyviä tuloksia harmaan talouden määrään. Toisaalta samalla on otettava vakavasti alan yritysten huoli siitä, että yritysten hallinnollinen taakka on voimakkaasti lisääntynyt erityisesti runsaasti työtä teettävän ilmoitusvelvollisuuden vuoksi. Osa hallinnollisesta taakasta on liittynyt siihen, että tieto ei ole välittynyt viranomaisten välillä ja yritys on joutunut täyttämään tietoja moneen paikkaan.

Lahjonta

Lahjonnalla tarkoitetaan valta-aseman väärinkäyttöä yksityisen edun saavuttamiseksi. Julkisella sektorilla korruption esiintymisessä on yleensä kyse virka- ja lahjusrikoksista, kun taas yksityisellä sektorilla se voi ilmetä muun muassa elinkeinoelämän lahjusrikoksina, yritys-salaisuusrikoksina, luottamusaseman väärinkäyttönä sekä petos- ja kavallusrikoksina. Kauppakamarien kyselyssä tarkastellaan sekä viranomaisasioinnissa että yritysten välisessä yhteistyössä esiintyvää lahjontaa. Yritystoiminnassa ilmenevä lahjonta jää yleensä tilastoimattomaksi piilorikollisuudeksi.
Vastanneista yrityksistä kolme prosenttia oli kohdannut lahjontaa viranomaisten kanssa asioidessa ja viisi prosenttia yritysten välisessä yhteistyössä.

• Viranomaisasioinnissa kohdattu lahjonta

Edelliseen vuoden 2012 kyselyyn verrattuna viranomaisasioinnissa kohdattu lahjonta on kasvanut kaikkien yritysten ja yli viisi henkilöä työllistävien yritysten osalta kahdella prosenttiyksiköllä (1 %-->3 %). Yritysten osuus, jotka olivat kohdanneet lahjontaa viranomaisasioinnissa, kasvoi kaikilla toimialoilla useilla prosenttiyksiköllä vuosina 2012 - 2017. Vuonna 2017 kaupan alan yrityksistä neljä prosenttia (1 %-->4 %), rakennusalan yrityksistä kolme prosenttia (2 %-->3 %) ja palvelualan yrityksistä kolme prosenttia (1 %-->3 %) ja teollisuusyrityksistä kaksi prosenttia (1 %-->2%) oli kohdannut lahjontaa viranomaisasioinnissa.

• Yritysten välisessä yhteistyössä kohdattu lahjonta

Edelliseen vuoden 2012 kyselyyn verrattuna niiden yritysten osuus, jotka raportoivat yritysten välisestä lahjonnasta nousi kahdella prosenttiyksiköllä (3 %-->5 %). Yli viisi henkilöä työllistävien yritysten tarkastelussa lahjonnasta raportoivien yritysten osuus ja muutos olivat samoja.

Yritysten välisessä yhteistyössä lahjontaa kohtasivat eniten rakennusalalla toimivat yritykset. Lahjonnasta raportoivien rakennusalan yritysten osuus nousi vuoden 2012 kyselyyn verrattuna (6 %-->9 %). Kaupan ja palvelualan yrityksistä kuusi prosenttia raportoi yritysten välisessä yhteistyössä kohdatusta lahjonnasta. Kaupan alalla lahjonnasta yritysten välisessä yhteistyössä raportoivien yritysten osuus nousi neljästä prosentista kuuteen prosenttiin ja palvelualalla kahdesta kuuteen prosenttiin. Teollisuudessa muutos oli kolmesta neljään prosenttiin.

Taloushallintoon liittyvät sisäiset väärinkäytökset

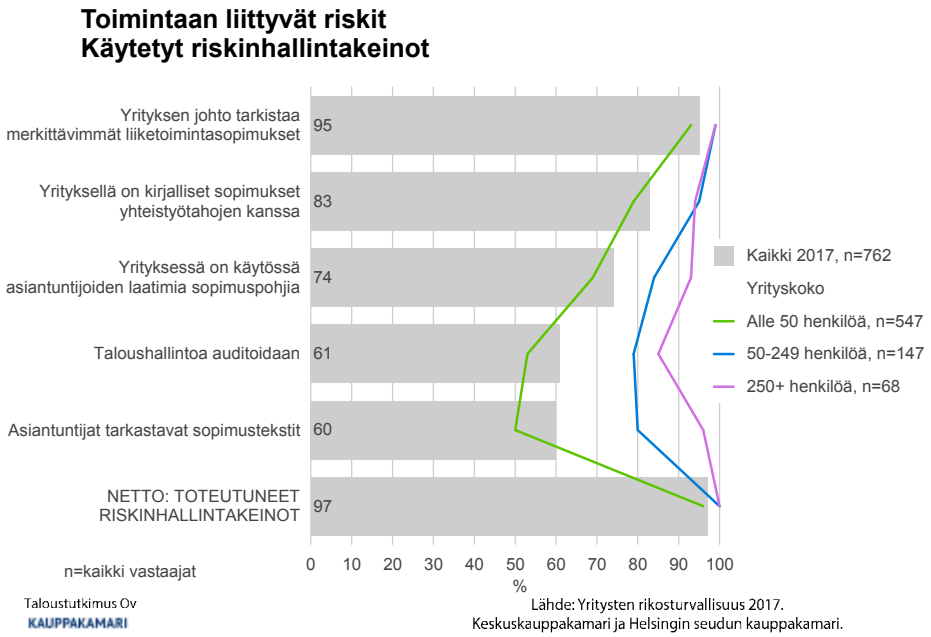
Sisäisen valvonnan puutteet esim. erään rahaliikenteestä vastanneen henkilön kohdalla.
(Yli 250 henkilöä työllistävä kaupan alan yritys)

Työntekijä kavalsi päivärahoja ja palkkaa vilpillisillä matkaselvityksillä tekemättä työtä ollenkaa.
(Alle 50 henkilöä työllistävä kaupan alan yritys)

Taloushallintoon liittyviä sisäisiä väärinkäytöksiä oli havainnut vain kolme prosenttia vastanneista. Suurista yrityksistä kymmenesosa (10 %) raportoi väärinkäytöksistä. Taloushallintoon liittyviä sisäisiä väärinkäytöksiä ei juuri havaittu pienissä ja keskisuurissa yrityksissä. Pienistä yrityksistä kaksi prosenttia ja keskisuurista yrityksistä kolme prosenttia ilmoitti taloushallinnon väärinkäytöksistä.

Vahingollisella tiedolla kiristäminen

Vahingollisella tiedolla kiristäminen oli yrityksissä erittäin harvinaista. Vastaajista vain kaksi prosenttia ilmoitti rikoksesta. Suurista yrityksistä kuitenkin kuusi prosenttia raportoi vahingollisella tiedolla kiristämisestä.



Lähde: Yritysten rikosturvallisuus 2017.
Keskuskauppakamari ja Helsingin seudun kauppakamari.

Yleisimmät riskienhallintakeinot toiminnan suojaamiseksi

Yritysturvallisuuskyselyyn vastanneet yritysjohtajat kertoivat yrityksen tavoista suojata toimintaa sopimusten ja auditoinnin avulla. Sopimuksilla ja auditoinnilla voidaan myös suojata yritysten asiakkaiden omaisuutta ja tietoa ja näitä on käsitelty tarkemmin luvussa viisi.

1. Lähes kaikissa yrityksissä johto tarkistaa merkittävimmät liiketoimintasopimukset (95 %).
Rakennusalalla johto tarkistaa hieman keskimääräistä harvemmin merkittäviä sopimuksia. Osuus on rakennusalalla 89 prosenttia, kun se muilla toimialoilla on keskimääräisellä tasolla

2. Kirjalliset sopimukset yhteistyötahojen kanssa ovat yleisesti käytössä (83 %)
Sekä vuonna 2012 että 2017 yrityksistä 15 prosenttia ilmoitti, että yritys ei tee kirjallisia sopimuksia yhteistyötahojen kanssa. Tilanne on heikkoerityisesti alle 50 henkilöä työllistävissä yrityksissä, joista 20 prosenttia ei käytä kirjallisia sopimuksia. Kirjallisia sopimuksia yhteistahojen kanssa ei käytä myöskään joka neljäs kaupan alan yritys ja joka kuudes rakennusalan ja teollisuusalan yritys. Keskisuurista ja suurista yrityksistä sekä palvelualan yrityksistä valtaosa tekee sopimukset yhteistahojen kanssa kirjallisesti.

3. Asiantuntijoiden laatimat sopimuspohjat antavat suojaa toiminnalle (74 %)
Pienistä yrityksistä keskimääräistä harvempi, 69 prosenttia käyttää asiantuntijoiden laatimia mallisopimuksia. Keskisuurista yrityksistä 84 prosenttia ja suurista yrityksistä 93 prosenttia käyttää sopimuspohjia ja käytöaste on varsin hyvä. Sopimuspohjien käyttö on keskimääräistä (74 %)) harvinaisempaa kaupan alalla ja rakennusalalla, keskimääräisellä tasolla teollisuudessa ja keskimääräistä yleisempää palvelualalla.

4. Taloushallintoa auditoidaan (61 %)
Auditoinnilla tarkoitetaan säännöllistä, riippumatonta ja dokumentoitua tarkastusta tai arviointia, jossa toimintaa verrataan annettuihin vaatimuksiin tai ohjeisiin. Taloushallinnon väärinkäytösten ehkäisyssä tärkeässä asemassa on myös taloushallintoa hoitavien henkilöiden luotettavuuden ja pätevyyden arviointi. Taloushallintoon liittyviä väärinkäytöksiä voidaan ehkäistä työnkierrolla ja työtehtäviä eriyttämällä sekä käyttämällä ammattitaitoista tilintarkastusta, sisäistä valvontaa ja auditointia. Yrityksissä on myös syytä olla erityisen tarkkana laskujen hyväksymisessä, sillä esimerkiksi huijauslaskut ja petokset ovat kasvava ongelma.

Kolmannes yrityksistä ei ole auditoinut taloushallintoaan. Auditointi on keskimääräistä (61 %) yleisempää teollisuudessa, muulla toimialalla sekä yli viisi henkilöä työllistävissä yrityksissä. Suurista yrityksistä vain joka kymmenes ja keskisuurista yrityksistä alle viidennes ei ole auditoinut taloushallintoaan.

5. Asiantuntijat tarkistavat sopimustekstit (60 %)
Pienistä yrityksistä puolet, keskisuurista yrityksistä 80 prosenttia ja suurista yrityksistä lähes kaikki (96 %) turvautui sopimusten laadinnassa asiantuntijan apuun.

Teollisuudessa ja palvelualalla riskienhallintakeinon käyttö oli lähes yhtä yleistä (61 % - 63 %), rakennusalalla ja kaupan alalla vain puolet yrityksistä ilmoitti, että asiantuntijat tarkistavat sopimustekstit.

Turvallisuus-johtaminen

7 TURVALLISUUSJOHTAMINEN

Turvallisuusjohtamisen kehittyminen

Turvallisuusjohtamisen kautta yritys toteuttaa turvallisuuspolitiikkaa ja turvallisuuden kehittämistä. Turvallisuus kuuluu turvallisuusjohtajan lisäksi kaikille työntekijöille ja esimiesasemassa olevilla henkilöillä on erityinen vastuu huomioida turvallisuus työssään ja osoittaa näin alaisilleen sen tärkeys osana arkityöskentelyä. Jos yrityksellä ei ole palkattua turvallisuusjohtajaa, sitä suurempi vastuu turvallisuusjohtamisesta on yrityksen johdolla.

Verrattaessa tämän vuoden kyselyn tuloksia vuosina 2012, 2008 ja 2005 tehtyjen kyselyjen tuloksiin, lähes kaikkien turvallisuusjohtamisen osa-alueiden osalta on tapahtunut näkyvää myönteistä kehitystä. Tämä kertoo turvallisuuden ankkuroitumisesta osaksi yritysten toimintaa ja johtamista.

Omassa organisaatiossani haasteena on resursointi turvallisuustehtävien hoitamiseksi ja ylimmän johdon selkeän tuen puuttuminen työlle. Turvallisuusorganisaatioon kuuluu kyllä edustaja ylimmästä johdosta, mutta siitä miten asiat päätyvät johtoryhmälle tiedoksi, ei ole täyttä varmuutta. Yleisesti haasteena on myös tietoturva- ja turvallisuusohjeistuksien jalkautuksen puutteet, eli koko henkilöstö ei ole tietoinen käytännöistä ja periaatteista.
(Yli 250 henkilöä työllistävä palvelualan yritys)

Turvallisuusjohtamisen tavat ja muodot

Johdon osallistuminen ja turvallisuusasioiden käsittely henkilökunnan kanssa

Yrityksen johdon asenne turvallisuuteen ohjaa merkittävällä tavalla sitä, miten henkilökunta suhtautuu turvallisuuteen. Turvallisuuteen vähättelevästi suhtautuva henkilökunta voi tehdä tarkoittamattaan tyhjäksi sen, mitä yritys on tavoitellut panostaessaan turvallisuuteen. Jos henkilökunta päästää yritykseen tuntematttomia henkilöitä, voi sinänsä hyvää tarkoittava henkilökunta tehdä tyhjäksi sijoitukset ovien lukitukseen, hälytysjärjestelmiin ja vartiointiin. Henkilökunnan koulutus on tehokkain tapa kertoa henkilökunnalle, miten yritys haluaa henkilökunnan toimivan turvallisesti.

Yhdeksän kymmenestä vastaajayrityksestä (91 %) kertoi johdon osallistuvan turvallisuuden kehittämiseen. Tuloksissa ei ollut juuri eroa yrityksen koon perusteella. Eri toimialoilla johto osallistui turvallisuuden kehittämiseen seuraavasti: teollisuus 92 %, palveluala 90 %, kaupan ala 90 % ja rakennusala 88 %. Korkeat vastausprosentit kertovat yritysten johdon mieltäneen turvallisuuden osaksi yrityksen toimintaa yrityksen kokoluokasta tai toimialasta riippumatta. Johdon osallistuminen turvallisuuden kehittämiseen on yleistynyt selvästi yli viisi henkilöä työllistävissä yrityksissä vuosien 2005 ja 2017 välillä (80 %-->91 %).

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

Kaikista yrityksistä 87 prosenttia käsitteli turvallisuusasioita henkilöstön kanssa. Osuus oli hieman pienempi pienissä yrityksissä, 84 prosenttia. Suurista vastaajayrityksistä kaikki käsitteli turvallisuusasioita henkilöstön kanssa ja keskisuuristakin valtaosa (92 %). Eri toimialoilla turvallisuusasioita käsiteltiin henkilökunnan kanssa seuraavasti: kaupan ala 90 %, palveluala 87 %, teollisuus 85 % ja rakennusala 82 %.

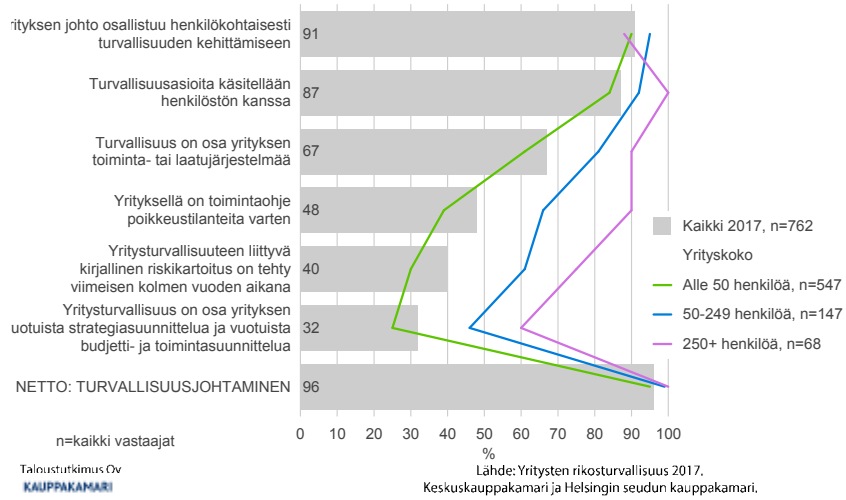
Turvallisuusasioiden käsittely henkilökunnan kanssa on yleistynyt yli viisi henkilöä työllistävissä yrityksissä vuosien 2005 ja 2017 välillä (82 %-->87 %).

Turvallisuusjohtaminen osana toiminta- tai laatujärjestelmää

Kytkemällä turvallisuus laatuun tai toimintaan yritys yhdistää turvallisuuden osaksi yrityksen laatujärjestelmän auditointeja. Samalla tarve erilliselle turvallisuuden arvioimiselle voi jäädä vähäisemmäksi.

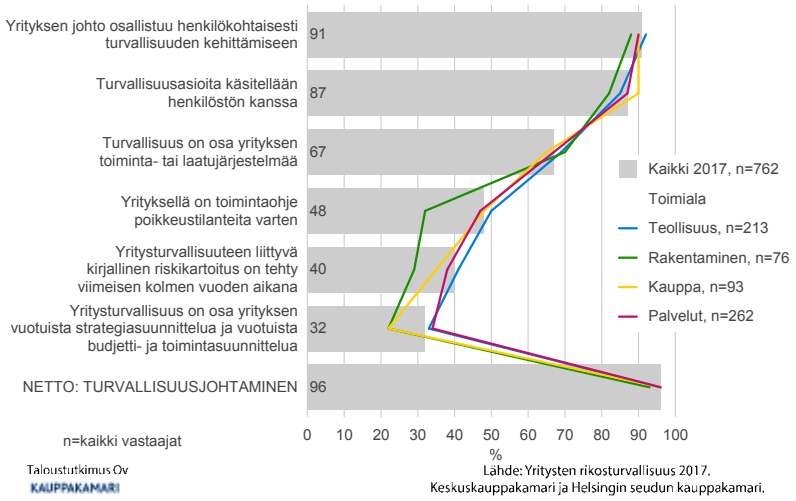
Kahdella kolmasosalla (67 %) yrityksistä turvallisuus on osa yrityksen toiminta- tai laatujärjestelmää. Suurista vastaajayrityksistä yhdeksällä kymmenestä (90 %), keskisuurista kahdeksalla kymmenestä (81 %) ja pienistä yrityksistä alle kahdella kolmasosalla (61 %) turvallisuus on osa yrityksen toiminta- ja latujärjestelmää. Eri toimialoilla turvallisuusasioita käsiteltiin henkilökunnan kanssa seuraavasti: rakennusala (70 %), teollisuus (69 %), palveluala (67 %) ja kaupan ala (65 %).

Turvallisuusjohtaminen



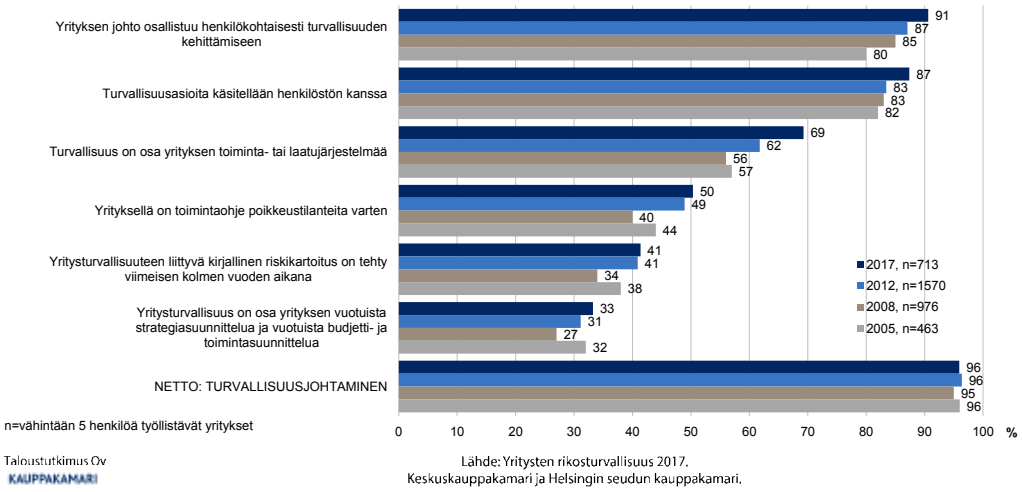
Lähde: Yritysten rikosturvallisuus 2017, Keskuskauppakamari ja Helsingin seudun kauppakamari.

Turvallisuusjohtaminen



Lähde: Yritysten rikosturvallisuus 2017, Keskuskauppakamari ja Helsingin seudun kauppakamari.

Selvitykset 2005 - 2017: Turvallisuusjohtaminen



Lähde: Yritysten rikosturvallisuus 2017, Keskuskauppakamari ja Helsingin seudun kauppakamari.

Turvallisuus on yhä useammin osa yrityksen turvallisuus- ja laatujärjestelmiä. Vuosien 2005 ja 2017 välillä osuus on kasvanut 12 prosenttiyksikköä yli viisi henkilöä työllistävissä yrityksissä (57 % – 69 %).

Kirjallinen toimintaohje poikkeustilanteisiin ja riskikartoitus

Kun yritys tekee toimintaohjeen poikkeustilanteita varten varautuu yritys samalla myös jatkuvuuttaan tavalla tai toisella uhkaaviin tilanteisiin. Jatkuvuutta uhkaavan tilanteen käynnistyessä ensimmäinen toimenpide on käynnistää poikkeustilanteen toimintaohjeiden mukainen toiminta keräämällä poikkeustilanteiden johtoryhmä koolle.

Puolet kaikista yrityksistä (48 %) on laatinut poikkeustilanteen toimintaohjeen. Suurista vastaajayrityksistä yhdeksän kymmenestä (90 %) on tehnyt niin ja keskisuurista kaksi kolmasosaa (66 %). Pienistä neljä kymmenestä (39 %) on laatinut ohjeen. Eri toimialoilla oli toimintaohje poikkeustilanteita varten seuraavasti: teollisuus 50 %, kaupan ala 48 %, palveluala 47 % ja rakennusala 32 %.

Yli viisi henkilöä työllistävissä yrityksissä toimintaohjeet poikkeustilanteisiin ovat yleistyneet kuudella prosenttiyksiköllä vuosien 2005 ja 2017 välillä (44 %-->50 %).

Omien resurssien puute edes siihen, että tietää mihin syytä panostaa ja mitä voi jättää vähemmälle. (Alle 50 henkilöä työllistävä palvelualan yritys)

Riskikartoituksen tekeminen on tehokas tapa selvittää, millaisia uhkia yritykseen kohdistuu. Tällöin yritys saa paljon tietoa siitä, mihin uhkiin sen kannattaa ensisijaisesti varautua ja mihin resurssit kannattaa kohdistaa.

Kaikista vastaajayrityksestä 40 prosenttia oli tehnyt kirjallisen riskikartoituksen. Yrityksistä enemmistö, 57 prosenttia, ei ollut tehnyt riskikartoitusta ja pieni osa yrityksistä ei tiennyt, onko yrityksessä tehty riskikartoitusta. Suurista yrityksistä kolme neljäsosaa (75 %), keskisuurista kuusi kymmenesosaa (61 %) ja pienistä yrityksistä alle kolmasosa (30 %) ilmoitti tehneensä kirjallisen riskikartoituksen. Eri toimialoilla kirjallinen riskikartoitus oli tehty seuraavasti: teollisuus 41 %, palveluala 38 %, kaupan ala 35 % ja rakennusala 29 %.

Yli viisi henkilöä työllistävissä yrityksissä riskikartoitusten tekeminen on yleistynyt vuosien 2005 ja 2017 välillä vain hieman (38 %-->41 %).

Yritysturvallisuus osana strategiasuunnittelua ja vuotuista budjetti- ja toimintasuunnittelua

Jos yritys ei liitä yritysturvallisuutta osaksi yrityksen muuta vuotuista toiminnan suunnittelu- ja rahoitusprosessia, vaan yritysturvallisuus saa rahaa sen ulkopuolelta tapauskohtaisesti, on vaikea nähdä yrityksen kehittävän yritysturvallisuutta tosissaan ja pitkäjänteisesti.

Kaikista vastanneista yrityksistä vain kolmasosa (32 %) oli kytkenyt yritysturvallisuuden osaksi vuotuista suunnittelua. Suurista yrityksistä kaksi kolmasosaa (60 %), keskisuurista alle puolet (46 %) ja pienistä yrityksistä neljännes (25 %) oli tehnyt näin. Eri toimialoilla osuudet vaihtelivat seuraavasti: palveluala 34 %, teollisuus 33 %, kaupan ala 22 % ja rakennusala 22 %.

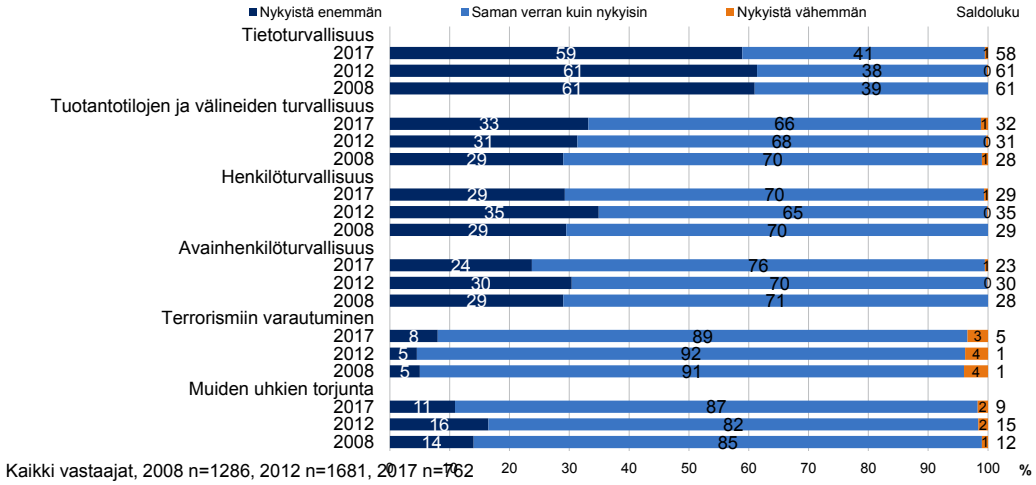
Yli viisi henkilöä työllistävissä yrityksissä osuus on pysynyt lähes samana vuosien 2005 ja 2017 välillä (32 %-->33 %). Tämä tarkoittaa sitä, että edelleen kaksi kolmasosaa vastaajista ei budjetoi turvallisuutta vuotuiseen suunnitteluun. Yrityksen turvallisuus on kuitenkin aivan samalla tavalla vuotuista kehitystä ja budjetointia vaativa yrityksen toiminnan osa-alue kuten esimerkiksi myynti tai tuotanto.

Ei ehkä tarpeeksi tiedosteta turvallisuusuhkia. Asenne turvallisuusasioita kohtaan tuntuu kohenevan vasta kun jotain on jo tapahtunut. Yritysjohto ei täysin tunnista tai tunnusta turvallisuuden merkitystä liiketoimintaan. (Yli 250 henkilöä työllistävä palvelualan yritys

Turvallisuus-panostukset jatkossa

8 TURVALLISUUSPANOSTUKSET JATKOSSA

Turvallisuuden kehittäminen
Yritys panostaa seuraaviin yritysturvallisuuden osa-alueisiin



Taloustutkimus Oy
KAUPPAKAMARI

Lähde: Yritysten rikosturvallisuus 2017.
Keskuskauppakamari ja Helsingin seudun kauppakamari.

Kyselyyn vastanneet yritykset arvioivat tulevaisuuden painopisteitä turvallisuuden kehittämisessä. Keskimääräistä korkeampi saldoluku (enemmän panostuksia – vähemmän panostuksia) kertoo siitä, että yritykset panostavat keskimääräistä useammin tähän osa-alueeseen. Yritysturvallisuuden kehittämisessä tulevaisuuden painopistealueina nähdään erityisesti:

1. Tietoturvallisuus (saldoluku 58)
2. Tuotantotilojen ja –välineiden turvallisuus (saldoluku 32)
3. Henkilöturvallisuus (saldoluku 29)

Kuten aikaisemmissa kyselyissä, myös tässä kyselyssä turvallisuuden kehittäminen painottuu tietoturvallisuuteen. Tämä kertoo sekä tietoriskien kasvusta että siitä, että yritykset ovat riippuvaisia tietojärjestelmistä. Yrityksistä 59 prosenttia vastasi, että tietoturvallisuuteen panostetaan yrityksessä jatkossa nykyistä enemmän. Keskisuurista yrityksistä 71 prosenttia ja suurista yrityksistä 78 prosenttia aikoo panostaa tietoturvallisuuteen nykyistä enemmän. Pienissä yrityksissä osuus on keskimääräistä pienempi, 53 prosenttia.

Tietoturvallisuuteen aikoo panostaa nykyistä enemmän 63 prosenttia palvelualan yrityksistä, 60 prosenttia teollisuusyrityksistä, 58 prosenttia kaupan alan yrityksistä ja 49 prosenttia rakennusalan yrityksistä.

Kaikki yritykset	Teollisuus	Rakentaminen	Kauppa
+58	+53	+71	+76

Turvallisuuspanostukset tietoturvallisuuteen jatkossa (punaisella keskimääräistä suuremmat panostukset)

Yritykset osaavat melko hyvin 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. Rakennusalan korkeaan osuuteen vaikuttaa todennäköisesti rakennusalan yritysten kokemat varkaustapaukset.

Kaikki yritykset	Teollisuus	Rakentaminen	Kauppa	Palvelut	Muu toimiala
+32	+37	+42	+22	+31	+28

Turvallisuuspanostukset tuotantotilojen ja välineiden turvallisuuteen jatkossa (punaisella keskimääräistä suuremmat panostukset)

Henkilökunnan turvallisuudesta huolehtiminen on osa vastuullisen työnantajan toimintaa. Lähes kaikki yritykset pitävät panostuksensa siihen samalla tasolla kuin aiemmin. Seitsemän kymmenestä (70 %) yrityksestä aikoo panostaa henkilöturvallisuuteen saman verran kuin nykyisin ja lähes kolmasosa (29 %) nykyistä enemmän. Edelliseen mittauskertaan verrattuna lisäpanostuksia suunnittelevien vastaajien määrä on laskenut kuusi prosenttiyksikköä ja panostukset samalla tasolla pitävien määrä on kasvanut viisi prosenttiyksikköä. Henkilöturvallisuuteen panostaa keskimääräistä useampi keskisuuri ja suuri yritys. Nykyistä enemmän henkilöturvallisuuteen panostaa joka neljäs (26 %) pieni yritys, reilu kolmannes (37 %) keskisuurista yrityksistä ja neljä kymmenestä 41 %) suuresta yrityksestä. Toimialojen kesken eroa ei juuri ole. Henkilöturvallisuuteen panostaa aiempaa enemmän 30 prosenttia teollisuuden ja palvelualan yrityksistä ja 26 prosenttia kaupan ja rakennusalan yrityksistä.

Kaikki yritykset	Teollisuus	Rakentaminen	Kauppa
+29	+25	+37	+40

Turvallisuuspanostukset henkilöturvallisuuteen jatkossa (punaisella keskimääräistä suuremmat panostukset)

Kaikista yrityksistä neljännes (24 %) aikoo panostaa avainhenkilöturvallisuuteen nykyistä enemmän. Kolme neljäsosaa (76 %) pitää avainhenkilöturvallisuuteen liittyvät panostukset ennallaan. Edelliseen mittauskertaan verrattuna panostuksia lisäävien määrä on laskenut kuusi prosenttiyksikköä ja panostukset ennallaan pitävien määrä noussut kuusi prosenttiyksikköä. Nykyistä enemmän avainhenkilöturvallisuuteen aikoo panostaa 28 prosenttia palvelualan yrityksistä, 26 prosenttia rakennusalan yrityksistä, 22 prosenttia teollisuusyrityksistä ja 14 prosenttia kaupan alan yrityksistä.

Kaikki yritykset	Teollisuus	Rakentaminen	Kauppa	Palvelut	Muu toimiala
+23	+22	+26	+14	+27	+24

Turvallisuuspanostukset avainhenkilöturvallisuuteen jatkossa (punaisella keskimääräistä suuremmat panostukset)

Kaikista yrityksistä kahdeksan prosenttia vastasi, että yritys aikoo varautua nykyistä enemmän terrorismiin tulevaisuudessa. Terrorismiin torjuntaan varaudutaan hieman enemmän kuin vuonna 2012 (saldoluku 1 – 5). Terrorismista on viimeisten vuosien aikana tullut riski, jonka vaikutukset voivat kohdistua yrityksen toimintaan myös kotimaan toiminnoissa. Yhdeksän kymmenestä (89 %) pitää varautumisen kuitenkin silla tasolla kuin se on ollut.

Erityisesti suuret yrityksistä varautuvat terrorismiin. Viidennes suurista yrityksistä aikoo varautua terrorismiin nykyistä enemmän. Kolme prosenttia vastaajista aikoo varautua nykyistä vähemmän terrorismiin. Toimialoittain aiempaa enemmän terrorismin varautumiseen panostaa kymmenen prosenttia palvelualan yrityksistä, seitsemän prosenttia teollisuusyrityksistä, kuusi prosenttia kaupan alan yrityksistä ja kolme prosenttia rakennusalan yrityksistä.

Kaikki yritykset	Teollisuus	Rakentaminen	Kauppa
+5	+3	+4	+19

Turvallisuuspanostukset terrorismiin varautumiseen jatkossa (punaisella keskimääräistä suuremmat panostukset)

Kymmenesosa (11 %) yrityksistä ilmoitti varautuvansa turvallisuuden kehittämisessä muihin turvallisuuden kehittämisen osa-alueisiin. Yritysten avoimissa vastauksissa mainittiin muun muassa varautuminen luonnonilmiöiden aiheuttamiin riskeihin ja matkustusturvallisuuteen. Yritysten mainitsemissa muissa uhkissa nousi esille myös uusiin tietoturvariskeihin kuten kyberuhkiin ja tiedon urkintaan varautuminen.

Jatkuvuus-suunnittelu

9 JATKUVUUSSUUNNITTELU

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.

Huolimatta kaikista varautumistoimenpiteistä riski voi toteutua ja aiheuttaa yrityksen toiminnan keskeytymisen tai jopa toiminnan loppumisen. Esimerkiksi naapuriyritykselle voi tapahtua jotain, mikä estää pääsyn omaan yritykseen tai vaikuttaa muuten yritykseen. Yritys ei voi aina vaikuttaa toisen toimijan varautumiseen. Joskus riskit vain toteutuvat yrityksen varautumisesta riippumatta.

Jos riskeihin ei ole varauduttu ennalta, voivat ne aiheuttaa merkittäviä taloudellisia vahinkoja ja uhata yrityksen toiminnan jatkumista. Käydessään läpi toimintansa kriittiset prosessit voi yritys saada jatkuvuuden varmistamisen lisäksi tietoa, jolla se voi tehostaa toimintaansa. Tällaisena seikkana voisi olla esimerkiksi tulipaloriskejä ja seurauksia kartoitettaessa havaittu liian suuren varaston ylläpitäminen ja siitä seuraava vahinko- ja liiketoiminnan keskeytysriski varaston tuhoutuessa.

Jatkuvuutta uhkaavan tilanteen synnyttyä voidaan tarvita poikkeustilanteiden johtamista tilanteen hallitsemiseen. Käytännössä tämä tarkoittaa ryhmää, joka on harjoitellut etukäteen toimintaa erilaisissa liiketoiminnan jatkuvuutta uhkaavissa tilanteissa. Tällainen ryhmä voi harjoitella toimintaansa neuvotteluhuoneharjoituksella, jolloin mitään käytännön toimia ei tehdä, vaan reagointi ja päätökset voidaan tehdä ryhmätyönä ja niistä käydään tarvittava keskustelu harjoituksen päätteeksi. Samalla voidaan arvioida omien suunnitelmien toimivuutta.

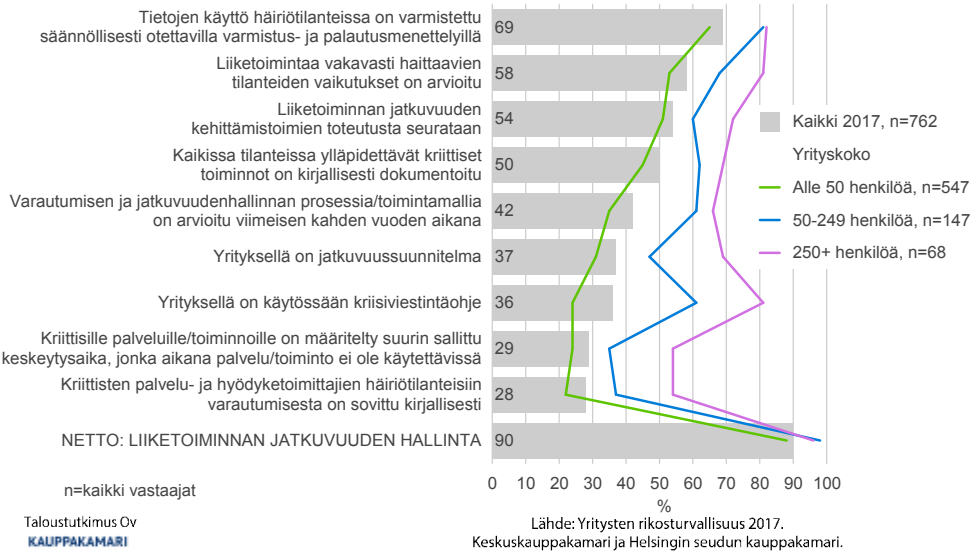
Mistä apua jatkuvuudenhallintaan?

Jatkuvuudenhallinnan systemaattisen kehittämisen avulla vähennetään toimintakatkoista aiheutuvia kustannuksia, luodaan organisaation johdolle varmuutta vastuuhenkilöiden kyvystä toimia häiriötilanteissa, tehostetaan toimintaa häiriötilanteissa ja nopeutetaan tilanteesta toipumista, lisätään vastuuhenkilöiden osaamista toiminnan kehittämisessä ja parannetaan organisaation mainetta luotettavana kumppanina.

Huoltovarmuuskeskus on kehittänyt useita työkaluja, joita yritykset voivat käyttää apuna jatkuvuudenhallinnassa. Huoltovarmuuskeskuksen sivuilla yritys voi muun muassa testata jatkuvuudenhallintaa kypsyysanalyysilla, josta saa myös yrityksen toiminnan nykytila- ja kehittämisraportit.

Lue lisää: https://www.huoltovarmuuskeskus.fi/tietoa-huoltovarmuudesta/jatkuvuudenhallinta/

Liiketoiminnan jatkuvuuden hallinta
Käytetyt riskinhallintakeinot



Lähde: Yritysten rikosturvallisuus 2017.
Keskuskauppakamari ja Helsingin seudun kauppakamari.

Yritystoiminnan jatkuvuutta tukevat toimenpiteet

Tietojen käytettävyyden varmistaminen häiriötilanteissa

Kaikki IT-asiat. Jos se pettää varautumisesta huolimatta, yritys on vakavissa ongelmissa toiminnan jatkuvuuden suhteen. Olemme liian riippuvaisia yhdestä it-henkilöstä. Tämä riski on työn alla.
(Alle 50 henkilöä työllistävä yritys, muu toimiala)

Yritykset ovat riippuvaisia tiedoistaan, niiden luottamuksellisuudesta, muuttumattomuudesta ja käytettävyydestä. Jos yritys menettäisi kaikki tietonsa tai luottamukselliset tiedot, olisi sillä väistämättä negatiivista taloudellista vaikutusta sen toimintaan. Niin pitkään kuin tiedot eivät ole yrityksen käytettävissä, vaikuttaisi se toimintaa hidastavasti ja jokainen tuottamaton päivä vaikuttaa tulokseen. Esimerkkinä tällaisesta uhista ovat lunnasohjelmahyökkäykset, joissa hyökkääjä salaa ja lukitsee yrityksen tiedostoja estäen niiden käyttämisen. Olennaisena varautumiskeinona lunnasohjelmahyökkäyksiin ovat tiedon varmistus- ja palautusmenettelyt.
Yli kaksi kolmasosaa kaikista vastaajayrityksistä (69 %) teki säännöllisesti varmistus- ja palautusmenettelyjä. Keskisuurissa ja suurissa yrityksissä osuudet olivat kaikkein korkeimmat (81 - 82 %). Pienistä vastaajista kaksi kolmasosaa (65 %) teki näin. Tämä jättää kolmasosan pienistä yrityksistä haavoittuvaksi tietojen menettämiselle. Samalla nämä yritykset asettavat itsensä hyvin heikkoon asemaan rikollisen toiminnan suhteen. Yleisintä varautuminen tiedon menettämiseen oli teollisuudessa ja palvelualalla 72 %. Perässä tuli kaupan ala 67 % ja rakennusala 54 %.

Liiketoimintaa vakavasti haittaavien tilanteiden vaikutusten arvioiminen

Kyetäkseen varautumaan liiketoiminnan jatkuvuutta uhkaaviin uhkiin, yrityksen on tunnistettava vakavimmat uhat ja arvioitava, millaisia seurauksia näillä on liiketoimintaan. Yrityksen johto vastaa toiminnan jatkuvuudesta ja siitä, miten jatkuvuutta uhkaaviin uhkiin on varauduttu. Tilanne, jossa omistajataho kysyy keskeytyksen tapahduttua, miksi jatkuvuutta ei ollut varmistettu, ei ole yrityksen kannalta suotuisa tilanne.

Yli puolet (58 %) kaikista vastaajayrityksistä oli arvioinut liiketoimintaa vakavasti haittaavien tilanteiden vaikutuksia. Vain puolet (53 %) pienistä yrityksistä oli arvioinut vaikutuksia, kun taas keskimääräistä selvästi useampi, kaksi kolmasosaa (68 %) keskisuurista yrityksistä arvioi tilanteita. Arviointeja tehtiin eniten (81 %) suurissa yrityksissä. Suuri joukko (36 %) kaikista vastaajayrityksistä ei ole arvioinut lainkaan näitä vaikutuksia. Esimerkiksi alihankintaketjuissa on usein pieniä ja keskisuuria yrityksiä. Näissä vastaajaryhmissä oli edelleen melko yleistä, ettei vaikutuksia arvioitu lainkaan. Alihankintaketjussa saattaa pienelläkin yrityksellä olla merkittävä rooli päämiehen toimitusten häiriöttömän toteutumisen kannalta. Siksi taloudellisesti merkittävissä hankkeissa mukana olevien pientenkin yritysten olisi hyvä arvioida, millaisia vaikutuksia eri tilanteissa voi syntyä. Sen jälkeen voisi olla hyvä suunnitella varatumista ja käydä keskustelua vakuutusyhtiön kanssa
Kuusi kymmenestä (59 – 60 %) palvelualan ja teollisuuden vastaajista oli arvioinut vaikutuksia. Kaupan alalla joka toinen (56 %) vastaajista oli tehnyt arvioinnin ja rakennusalalla alle puolet (45 %) oli tehnyt arvioinnin.

Jatkuvuuden kehittämistoimien toteutuksen seuraaminen

Kehittämistoimien onnistumista ja tehokkuutta on seurattava, jo senkin vuoksi, että yritys on sijoittanut niihin resursseja. Toteutuksen jälkeen toimivuutta ja suunnitelmia on hyvä testata. Jos yritys on sijoittanut resursseja jatkuvuuden kehittämiseen ja laiminlyö seurannan ja testaamisen, on varautumisen toimivuus huonoimmassa tilanteessa sattumanvaraista.

Puolet (54 %) yrityksistä seuraa kehittämistoimien toteutusta. Mikäli kehittämistoimia ei seurata, on vaarana, ettei niitä tehdä riittävän hyvin ja suunnitellusti. Myönteistä on, että ne, jotka ovat arvioineet vaikutuksia, seuraavat kehittämistoimien toteutusta. Samalla varmistuu, että kehittämiseen suunnatut resurssit on käytetty tehokkaasti ja suunnitellun mukaisesti.

Suurista yrityksistä seitsemän kymmenestä (72 %), keskisuurista kuusi kymmenestä (60 %) ja pienistä yrityksistä puolet (51 %) seuraa jatkuvuutta edistävien kehittämistoimien toteutusta.

Kaikissa tilanteissa ylläpidettävien kriittisten toimintojen kirjallinen dokumentointi

Yrityksen tehdessä toimintansa kannalta kriittisistä toiminnoista kirjalliset asiakirjat, syntyy samalla työkalu käytettäväksi niille henkilöille, jotka vastaavat jatkuvuudesta. Asiakirja antaa johdolle kuvan siitä, mistä toiminnoista yritys on riippuvainen ja samalla perusteen resurssien antamiselle kehittämistoimintaan. Sen kautta on myös helppo kontrolloida, miten jatkuvuutta on kehitetty.

Puolet kaikista yrityksistä (50 %) on kirjannut kriittiset toiminnot. Suurissa yrityksissä osuus on suurin, 69 prosenttia ja keskisuurissakin 61prosenttia. Pienistä yrityksistä alle puolet (45 %) on kirjannut kriittiset toiminnot. Viidennes suurista yrityksistä, kolmannes keskisuurista sekä puolet pienistä yrityksistä ei ole kirjannut eikä mahdollisesti ole tunnistanut kriittisiä toimintojaan. On vaikea tehdä jatkuvuussuunnittelua, mikäli ei tiedä mi-

hin pitää keskittää voimavaroja ja varmistustoimenpiteitä. Kohtasi yritystä sitten tulipalo tai kyberhyökkäys, varautumaton yritys kärsii aina kovemmin seurauksista ja selviää hitaammin tai ei selviä niistä lainkaan.

Yleisimmin kriittiset toiminnot oli kirjattu teollisuudessa (51 %) ja palvelualalla (50 %). Kaupan alalla melkein puolet (47 %) ja rakennusalalla kolmasosa (36%) oli tehnyt näin.

Jatkuvuudenhallintaprosessin tai toimintamallin arviointi

Olennainen osa jatkuvuuden kehittämistä on ulkopuolisen tahon tekemä arviointi, auditointi, esimerkiksi osana laadunvalvontaa tai turvallisuusauditointia. Tällöin yritys saa paljon tietoa siitä, mitä on kehitettävä ja mitkä asiat ovat jo kunnossa. Ulkopuolinen taho on riippumaton ja siksi annettu raportti on arvokkaampi yrityksen kannalta kuin itseauditoinnin raportti. Samalla johto saa arvion siitä, onko yrityksen siihenastinen oma varautumistoiminta ollut tarkoituksenmukaista.

Kaikista yrityksistä 42 prosenttia oli auditoitu jatkuvuudenhallinnan tiimoilta. Suurista yrityksistä 66 prosenttia, keskisuurista 61 prosenttia ja pienistä yrityksistä 35 prosenttia ilmoitti olleensa auditoinnin kohteena. Suurista ja keskisuurista yrityksistä jää kuitenkin noin kolmasosa ja pienistä 59 prosenttia, joita ulkopuolinen ei ole auditoinut kahden viime vuoden aikana.

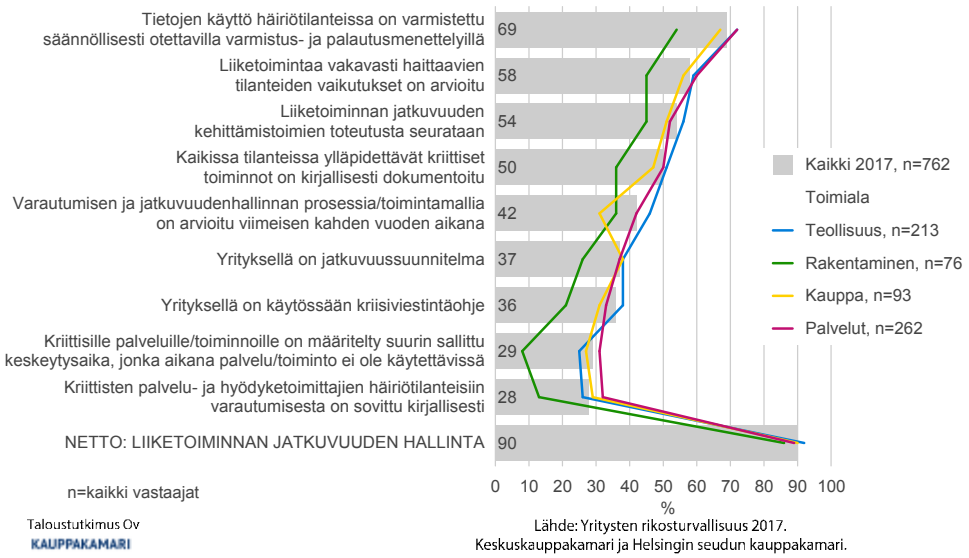
Eniten auditointien kohteena oli ollut teollisuusalan (46 %) ja palvelualan (42 %) vastaajayrityksiä. Kolmasosa rakennusalan ja kaupan alan yrityksistä oli ollut auditoinnin kohteena.

Jatkuvuussuunnitelma

Toimialasta johtuva jatkuvuussuunnitelman moninaisuus ja sen ylläpito kaikkien eri osapuolten suhteen luo haasteita.
(Alle 50 henkilöä työllistävä yritys, muu ala)

Ilman suunnitelmaa on mahdoton varautua jatkuvuutta vaarantavien uhkien varalle. Suunnitelmassa määritellään muun muassa, mitkä toiminnot ovat kriittisiä ja miten pitkään ne voivat olla keskeytyneenä. Jatkuvuussuunnitelma ohjaa yritystä tekemään pitkäjänteistä kehitystyötä ja auttaa suuntamaan resursseja tehokkaalla tavalla.

Liiketoiminnan jatkuvuuden hallinta
Käytetyt riskinhallintakeinot



Taloustutkimus Oy
KAUPPAKAMARI

Lähde: Yritysten rikosturvallisuus 2017.
Keskuskauppakamari ja Helsingin seudun kauppakamari.

Mikään suunnitelma ei ole toimintavarma, mikäli sitä ei ole jollan tavalla testattu. Siksi jatkuvuussuunnitelman toimivuutta tulisi kokeilla vähintään neuvotteluhuoneharjoituksena. Neuvotteluhuoneharjoitus on harjoitus, jossa ei toteuteta toimenpiteitä käytännössä, vaan etukäteen käsikirjoitettuun tarinaan liittyviin kysymyksiin vastataan sitä mukaa kuin tilanne kehittyy. Kysymyksiin vastaamisen lisäksi osallistujat tekevät erilaisia tilanteen vaatimia päätöksiä liiketoiminnan turvaamiseksi ja tilanteen hallitsemiseksi tai sen vaikutusten minimoimiseksi.

Miten jatkuvuussuunnitelma laaditaan?

- Jokaisen yrityksen on tehtävä omasta jatkuvuussuunnitelmastaan itsensä näköinen. Suunnitelmat ovat aina yrityskohtaisia eikä niitä voida sisällöllisesti koskaan kopioida suoraan toisen yrityksen käyttöön.
- Suunnitelman voi jakaa esimerkiksi kolmeen osaan: pelastussuunnitelmaan, poikkeustilanteiden johtamiseen ja toipumissuunnitelmaan. Nämä taas voidaan jakaa pienempiin osa-alueisiin kuten toipumissuunnitelmat koskien liiketoiminnan eri osa-alueita, varatoimipaikkasuunnitelma, sidosryhmien tiedottamis- ja yhteistyösuunnitelma (alihankkijat, tavarantoimittajat, palveluidentuottajat) ja vaikkapa tuotantomateriaalin hankintasuunnitelma.
- Jatkuvuussuunnitteluprosessin merkittävimpiä vaiheita on harjoittelu.
- Jatkuvuussuunnitelmaa pitäisi päivittää säännöllisesti ja aina kun yritykselle tulee uutta merkittävää liiketoimintaa, joka saattaa edellyttää aiempaa laajempia varautumistoimia.

Kaikista vastanneista yrityksistä vain hieman yli kolmasosalla (37 %) oli jatkuvuussuunnitelma. Suurista vastaajista kahdella kolmasosalla (69 %), keskisuurista alle puolella (47 %) ja pienistä vastaajayrityksistä kolmasosalla (31 %) oli jatkuvuussuunnitelma. Yli puolet (56 %) kaikista vastaajayrityksistä tiesi, ettei yrityksessä ole tehty jatkuvuussuunnitelmaa ja seitsemän prosenttia ei tiennyt, onko suunnitelmaa tehty. Suuristakin vastaajista peräti neljäsosa ei ole tehnyt suunnitelmaa. Yrityksillä on merkittävä rooli koko yhteiskunnan häiriöidensietokyvyssä. Siksi jatkuvuussuunnitelmien määrää on saatava lisättyä kaikissa yrityskokoluokissa.

Teollisuuden ja kaupan yrityksistä 38 prosenttia ja palvelualan yrityksistä 37 prosenttia oli tehnyt jatkuvuussuunnitelman. Osuus oli tätäkin heikompi rakennusalalla, jossa vain neljäsosa (26 %) yrityksistä oli tehnyt jatkuvuussuunnitelman.

Yrityksellä on käytettävissään kriisiviestintäohje

Kriisiviestintäohje liittyy käytännössä aina tilanteisiin, joissa yrityksen liiketoiminnan jatkuvuus on uhattuna. Huonosti viestitetty kriisitilanne voi antaa asiakkaille ja yhteistyökumppaneille kuvan siitä, ettei yritys ole onnistunut selviytymään tilanteesta hyvin. Henkilökunnan on esimerkiksi tiedettävä, kuka saa antaa lausuntoja tai tietoa yrityksen ulkopuolisille tahoille. Näin tiedonkulkua voidaan hallita ja välttää tilanteet, joissa tietoa päätyy hallitsemattomasti julkisuuteen.

Kaikista vastanneista yrityksistä vain hieman yli kolmasosalla (36 %) oli kriisiviestintäohje. Suurista vastaajista kahdeksalla kymmenestä (81 %), keskisuurista kahdella kolmasosalla (61 %) ja pienistä vastaajayrityksistä neljäsosalla (24 %) oli kriisiviestintäohje.

Noin kolmasosa teollisuuden (38 %), palvelualan (33 %) ja kaupan (31 %) yrityksistä, mutta vain viidesosa (21 %) rakennusalan yrityksistä oli tehnyt jatkuvuussuunnitelman.

Kriittisille palvelujen ja toimintojen on määritelty suurin sallittu keskeytysaika

Suurimman sallitun keskeytysajan määrittäminen antaa johdolle käsityksen siitä, mitä kriittiset toiminnot ja palvelut ovat ja miten pitkään ne voivat olla pysähtyneenä. Joillakin yrityksillä saattaa olla toimintoja, jotka eivät voi olla lainkaan tai vain lyhyen aikaa keskeytyneenä. Sen vuoksi yrityksen ainoaksi vaihtoehdoksi saattaa jäädä varajärjestelmien ylläpito.

Jos suurinta sallittua keskeytysaikaa ei ole määritetty, saattaa käydä niin, ettei yritys kykene pitämään sopimusvelvoitteistaan kiinni. Suurimman sallitun keskeytysajan jälkeen häiriö alkaa vaikuttaa sietokyvyn ylittävällä haitallisella tavalla liiketoimintaan. Yritys voi varautua keskeytysvakuutuksella, mutta niissäkin on omavastuunsa. Yrityksen on hyvä selvittää, mitä vakuutus korvaa. Vakuutuksetkin edellyttävät yritykseltä jonkinasteisia varautumistoimia.

Kaikista vastanneista yrityksistä vain kolme kymmenestä (29 %) oli määritellyt suurimman sallitun keskeytysajan. Suurista yrityksistä yli puolet (54 %), keskisuurista kolmasosa (35 %) ja pienistä yrityksistä neljäsosa (24 %) oli määritellyt suurimman sallitun keskeytysajan.

Noin kolmasosa (31 %) palvelualan yrityksistä, neljäsosa (25 - 27 %) kaupan ja teollisuuden yrityksistä ja kymmenesosa (8 %) rakennusalan yrityksistä oli määrittänyt suurimman keskeytysajan.

Kriittisten palvelu- ja hyödyketoimittajien häiriötilanteisiin varautumisesta sopiminen

Nykyisin yhteistyökumppaniverkostolla ja alihankintaketjuilla on merkittävä rooli yrityksen toiminnan onnistumisessa. Jos tavarat eivät saavu ajallaan ja palveluita ei toteuteta sovitusti sen vuoksi, että joku verkoston tai alihankintaketjun toimijoista on kohdannut jatkuvuuden keskeyttäneen tilanteen, saattaa se vaikuttaa suoraan asiakassuhteessa vastuussa olevan yrityksen toimitusvarmuuteen ja asiakassuhteisiin.

Alihankintaketjun jatkuvuuden varmistaminen on yleistynyt viime vuosikymmenen aikana. Suurien ja keskisuurien yritystenkin joukossa on vielä paljon yrityksiä, jotka eivät ole huomioineet alihankintaketjun jatkuvuuden varmistamista, vaikka ovat riippuvaisia alihankkijoidensa ja yhteistyökumppaneidensa toimitusvarmuudesta. Näiden yritysten omaa riskiarvioita ei ole tehty huolellisesti tai sitten tätä riskiä ei ole osattu ottaa huomioon.

Kaikista vastanneista yrityksistä vain yli neljäsosa (28 %) oli sopinut kirjallisesti toimittajien kanssa häiriötilanteisiin varautumisesta. Suurista vastaajista yli puolet (54 %), keskisuurista kolmasosa (37 %) ja pienistä vastaajayrityksistä viidesosa (22 %) oli sopinut kirjallisesti toimittajien kanssa häiriötilanteisiin varautumisesta.

Palvelualan yrityksistä 32 prosenttia, kaupan yrityksistä 29 prosenttia ja teollisuuden yrityksistä 26 prosenttia oli sopinut kirjallisesti toimittajien kanssa häiriötilanteisiin varautumisesta. Niiden yritysten osuus, jotka olivat sopineet kirjallisesti toimittajien kanssa häiriötilanteisiin varautumisesta jäi rakennusalalla vain 13 prosenttiin.

Yrityksissä ei tarpeeksi paneuduta näihin riskeihin eikä yrityksillä ole suunnitelmia kuinka jatketaan, kun ongelma tulee eteen.
(50-249 henkilöä työllistävä teollisuusalan yritys)

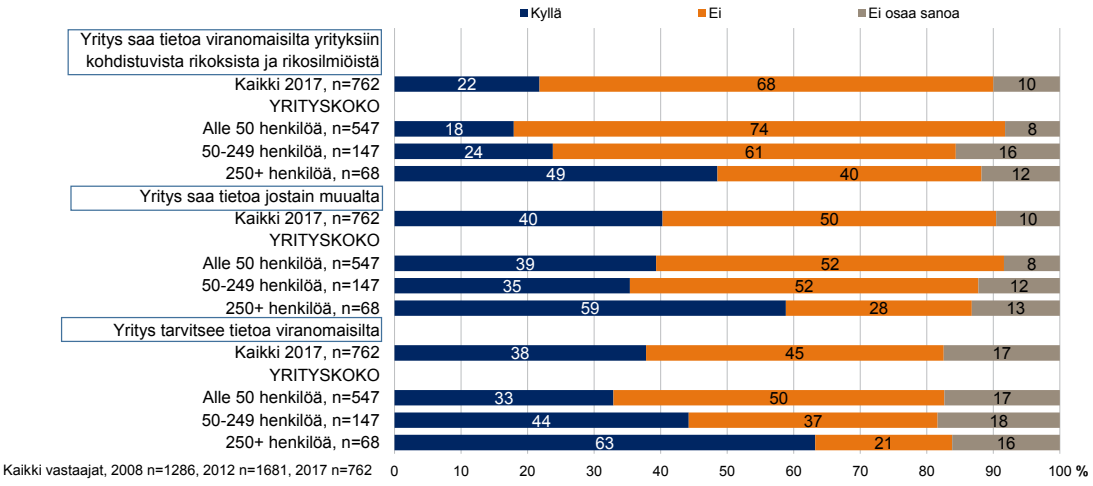
Kaikki IT-asiat. Jos se pettää, varautumisesta huolimatta yritys on vakavissa ongelmissa toiminnan jatkuvuuden suhteen. Olemme liian riippuvaisia yhdestä it-henkilöstä. Tämä riski on työn alla.
(Alle 50 henkilöä työllistävä yritys, muu ala)

Todellisen jatkuvuuden aikaansaaminen erittäin haasteellisin toimitusaikatauluin ei ole mahdollista saavuttaa tai se luo suuria haasteita.
(Alle 50 henkilöä työllistävä yritys, muu ala)

Tiedonsaanti rikosilmiöistä

10 TIEDONSAANTI RIKOSILMIÖISTÄ

Turvallisuuden kehittäminen
Rikosriskeihin liittyvä tiedonsaanti viranomaisilta



Taloustutkimus Oy
KAUPPAKAMARI

Lähde: Yritysten rikosturvallisuus 2017.
Keskuskauppakamari ja Helsingin seudun kauppakamari.

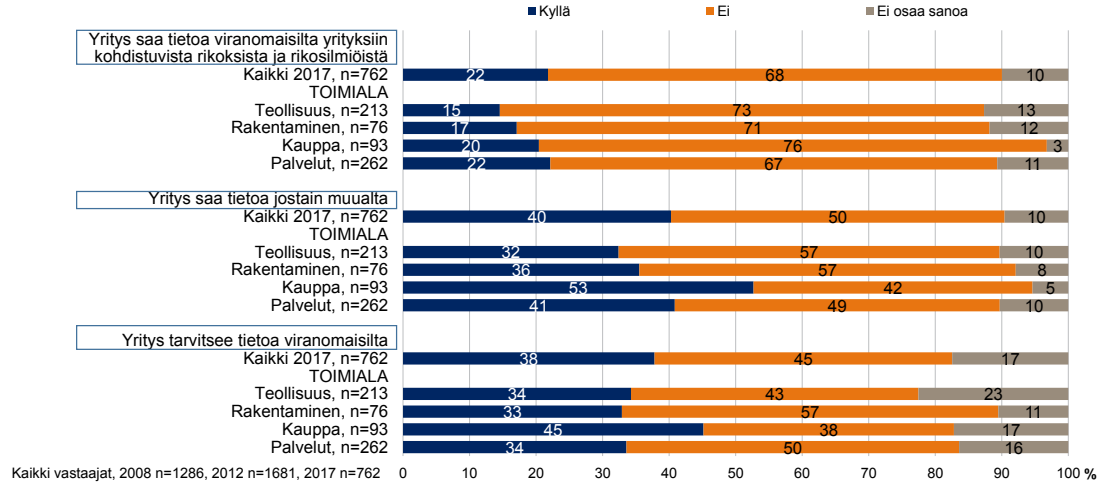
Erikokoisten yritysten rikosriskeihin liittyvä tiedonsaanti ja tarve saada tietoa

Kaikista vastanneista yrityksistä viidesosa (22 %) sai tietoa rikoksista ja rikosilmiöistä viranomaisilta. Seitsemän kymmenestä (68 %) vastaajasta ilmoitti, ettei ole saanut tietoa viranomaisilta rikoksista ja rikosilmiöistä. Pienistä yrityksistä peräti kolme neljästä (74 %) ei ole saanut tietoa. Keskisuurista yrityksistä kuusi kymmenestä (61 %) ja suurista yrityksistä neljä kymmenestä (40 %) ei saanut tietoa viranomaisilta. Suurten vastaajien tiedonsaanti on edelleen keskimääräistä yleisempää, mutta kehitys on huolestuttava. Vuoden 2012 selvityksessä kolmasosa (33 %) niistä ei ollut saanut tietoa viranomaisilta ja vuonna 2017 tietoa saamattomien osuus oli kasvanut seitsemän prosenttiyksikköä.

Kaikista kyselyyn vastanneista yrityksistä neljä kymmenestä (40 %) oli saanut tietoa rikosilmiöistä muuta kautta. Puolet (50 %) vastaajista ei ollut kuitenkaan saanut tietoa muistakaan lähteistä. Vastaukset vaihtelivat merkittävästi yrityskoon mukaan. Kun suurista yrityksistä vain 28 prosenttia ei ollut saanut tietoa muualta, niin keskisuurissa ja pienissä yrityksissä osuus oli 52 prosenttia. Vastausten osalta yllättävää oli pienten vastaajien tietoa saavien osuuden kasvu yhdeksällä prosenttiyksiköllä edelliseen mittauskertaan verrattuna. Suurien vastaajien osalta taas kasvua oli viisi prosenttiyksikköä.

Vastanneilta yrityksiltä kysyttiin, onko yrityksellä tarvetta saada viranomaisilta tietoa rikoksista ja rikosilmiöistä. Kaikista yrityksistä 38 prosenttia ilmoitti vuonna 2017 tarvitsevansa tietoa viranomaisilta. Vuonna 2012 osuus oli kuusi prosenttiyksikköä suurempi. Kolmasosa (33 %) pienistä yrityksistä ilmoitti tarvitsevansa tietoa. Keskisuurista yrityksistä 44 prosenttia ja suurista yrityksistä kaksi kolmasosaa (66 %) ilmoitti tiedontarpeesta. Kaikissa yrityskokoluokissa tiedontarve oli edellisellä mittauskerralla hieman suurempi.

Turvallisuuden kehittäminen
Rikosriskeihin liittyvä tiedonsaanti viranomaisilta



Taloustutkimus Oy
KAUPPAKAMARI

Lähde: Yritysten rikosturvallisuus 2017.
Keskuskauppakamari ja Helsingin seudun kauppakamari.

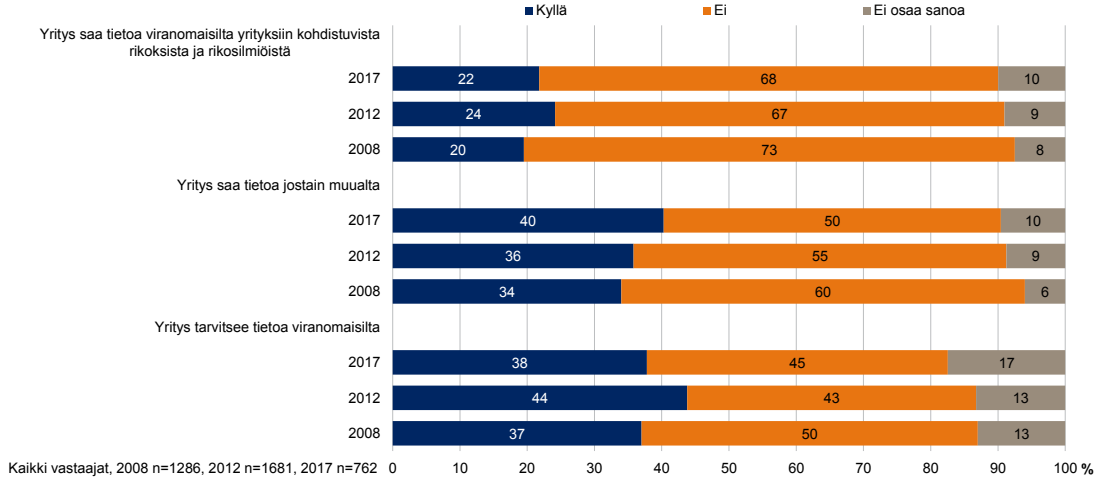
Eri toimialoilla toimivien yritysten rikosriskeihin liittyvä tiedonsaanti ja tarve saada tietoa

Viranomaisilta tietoa saaneiden yritysten osuudet jakaantuivat varsin tasaisesti eri toimialojen kesken. Palvelualalla 22 prosenttia ja kaupan alalla 20 prosenttia yrityksistä sai tietoa viranomaisilta. Tiedonsaanti oli hieman vähäisempää rakennusalalla, jossa tietoa sai 17 prosenttia yrityksistä. Vähiten tietoa saatiin teollisuudessa, jossa vain 15 prosenttia yrityksistä sai tietoa viranomaisilta.

Muualta tietoa saaneiden määrässä oli selvää toimialakohtaista vaihtelua. Tietoa muualta sai puolet (53 %) kaupan alan yrityksistä, neljä kymmenestä (41 %) palvelualan yrityksistä ja kolmasosa sekä rakennusalan (36 %) että teollisuuden yrityksistä (32 %). Eräs selitys kaupan alan tietoa saavien melko korkeaan osuuteen voi olla kaupan alan ketjuuntuminen ja tiedonvaihto Kaupan liiton jäsenten keskuudessa.

Tarve saada tietoa viranomaisilta vaihteli toimialoittain. Lähes puolet (45 %) kaupan alan yrityksistä ja kolmasosa (34 %) palvelualalta ja teollisuudesta sekä kolmasosa (33 %) rakennusalalta ilmoitti tarvitsevansa tietoa rikosriskeistä. Kaupan alan muita suurempaa tarvetta saada tietoa saattaa selittää kaupan alaa vaivaava jokapäiväinen omaisuusrikollisuus ja häiriköinti.

Turvallisuuden kehittäminen
Rikosriskeihin liittyvä tiedonsaanti viranomaisilta



Taloustutkimus Oy
KAUPPAKAMARI

Lähde: Yritysten rikosturvallisuus 2017.
Keskuskauppakamari ja Helsingin seudun kauppakamari.

Tarkistuslistat riskienhallinnan tukena

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).

Johtopäätökset

12 JOHTOPÄÄTÖKSET

Suuriin yrityksiin kohdistuva rikollisuus kasvussa

Yrityksistä 44 prosenttia arvioi, että rikosten määrä on kasvanut viimeisen kolmen vuoden aikana ja tästä seitsemän prosenttia arvioi, että rikosten määrä on lisääntynyt paljon.

Joka toinen suuri yritys näkee kasvua yrityksiin kohdistuvien rikosten ja väärinkäytösten määrässä viimeisen kolmen vuoden aikana. Edelliseen mittauskertaan verrattuna osuus on selvässä kasvussa (34 %-->52%). Kaikissa neljässä kyselyssä (2017, 2012, 2008 ja 2005) suuret yritykset kokevat joutuvansa keskimääräistä useammin rikosten ja väärinkäytösten kohteeksi.

Kaupan ja rakennusalan arviot turvallisuustilanteesta muita aloja synkemmät

Yritysrikosten kehitystä pidettiin synkimpänä kaupan alalla ja rakennusalalla. Rakennusalalla vaihtuvien työmaiden suojaaminen on vaikeaa ja riittävä suojaus tulee yrityksille liian kalliiksi. Rakennusalan vastaajista peräti 58 prosenttia ilmoitti työväline- ja laitevarkauksista. Kauppa kohtaa myös entistä enemmän uudenlaisia tieto- ja petosriskejä.

Turvallisuustilannetta pidetään kaikilla aloilla selvästi heikompana kuin edellisellä mittauskerralla. Viisi vuotta sitten tehdyssä selvityksessä viidennes rakennusalan ja teollisuusalan yrityksistä, neljännes palvelualan yrityksistä ja kolmannes kaupan alan yrityksistä arvioi rikosten määrän olevan kasvussa. Vuonna 2017 puolet rakennusalan ja kaupan yrityksistä ja neljä kymmenestä teollisuuden ja palvelualan yrityksistä arvioi rikosten määrän olevan kasvussa.

Joka kolmannessa kaupan ja palvelualan yrityksessä uhkatilanteita – varautumisessa vielä puutteita

Joka kolmannessa kaupan ja palvelualan yrityksessä on ollut uhkatilanteita. Ohjeet väkivalta- ja uhkatilanteiden hallintaan puuttuvat edelleen monelta kaupan (44 %) ja palvelualan (38 %) yritykseltä. Näissä yrityksissä ohjeiden teko on tarpeellisempaa kuin muiden alojen yrityksissä, jossa uhkailun tai väkivallan riski on vähäisempää.

40 prosenttia ei ole varautunut EU:n tietosuoja-asetukseen

EU:n uuden tietosuoja-asetuksen soveltaminen alkaa 25.5.2018. EU:n tietosuoja-asetus tuo lisää velvoitteita rekisterinpitäjälle ja henkilötietojen käsittelijälle. Yrityksistä 40 prosenttia ei ole varautunut tietosuoja-asetukseen, ja vajaa viidesosa ei osaa ottaa kantaa asiaan. Keskimääräistä heikompaa varautuminen on henkilömäärältään pienissä yrityksissä. Pienistä, alle 50 henkilöä työllistävistä yrityksistä vajaa kolmannes, keskisuurista yrityksistä puolet ja suurista yrityksistä kolme neljästä on varautunut asetukseen.

Salassapitosopimusten ja luokittelu- ja käsittelyohjeiden puute lisää pienten yritysten haavoittuvuutta

Salassapitosopimuksia tai -sitoumuksia ei ole tehnyt viidennes yrityksistä. Salassapitosopimusten teko on pienissä yrityksissä huomattavasti harvinaisempaa kuin suurissa yrityksissä. Tämä lisää pienten yritysten haavoittuvuutta. Pienistä yrityksistä 23 prosenttia ei käytä salassapitosopimuksia. Suurissa yrityksissä osuus on kolme prosenttia. Pienten yritysten haavoittuvuutta tietoturvaloukkaustapauksissa lisää myös se, että yli puolet pienistä yrityksistä ei ollut tehnyt ohjeita liike- ja ammattisalaisuuksien käsittelyyn. Verrattuna viisi vuotta aiemmin tehtyyn mittauskertaan, käsittelyohjeet ovat yleistyneet erityisesti suurissa yrityksissä, kun taas muissa yrityksissä muutokset ovat olleet melko pieniä.

Identiteettikaappaukset kasvussa

Vuoden 2017 yritysturvallisuuskyselyssä tietoon kohdistuvista riskeistä nousi esille lukuisat tapaukset, joissa yrityksen identiteetti on kaapattu tai yritetty kaapata. Yleensä yritystä on haluttu erehdyttää maksamaan pieniä tai isoja summia rikollisen tilille. Suuret yritykset näyttävät valikoituvan usein rikoksen kohteeksi. Pienistä yrityksistä viisi prosenttia, keskisuurista yrityksistä 11 prosenttia ja suurista yrityksistä peräti 28 prosenttia ilmoitti, että yrityksen identiteetti on kaapattu tai yritetty kaapata.

Vertailu eri kyselyjen välillä kuvaa ilmiön kasvua. Kun vuonna 2012 kolme prosenttia kaikista yrityksistä ja neljä prosenttia yli viisi henkilöä työllistävistä yrityksistä ilmoitti, että yrityksen identiteetti on kaapattu tai yritetty kaapata, vuonna 2017 osuus nousi molemmissa kohderyhmissä kahdeksan prosenttiin. Vuonna 2017 osuudet vaihtelivat toimialasta riippuen seitsemän ja kymmenen prosentin välillä, kun osuudet viisi vuotta aiemmin olivat kolmen ja viiden prosentin välillä. Sekä vuonna 2017 että 2012 osuudet olivat korkeimmat kaupan alalla (vuonna 2017: 10 % ja vuonna 2012: 5 %). Kyselyssä ilmennyt ilmiön laajuus ja lukuisat tapaukset antavat vahvan viestin. Yritysten pitää ottaa riskienhallinnassaan ja henkilöstölle annettavassa ohjeistuksessa vakavasti ilmiö.

Tiedon luvattomat urkintatapaukset kaupan alalla kasvussa, teollisuudessa tunnistetaan paremmin suojattava tietopääoma

Kaupan alan yritykset ilmoittivat toteutuneista tietoriskeistä kaikkein useimmin ja rakennusalan yritykset muiden toimialojen yrityksiä harvemmin. Kaupan alalla yritystiedon luvattomasta urkinnasta ilmoittaneiden osuus, 15 prosenttia, oli niin suuri, että riskienhallintaan on syytä alalla erityisesti panostaa. Muilla aloilla osuudet olivat 7- 8 prosentin tasolla. Urkintatapauksista huolimatta kaupan alan yrityksistä vain kolmannes tunnistaa, että niillä on kilpailijaa kiinnostavaa tietoa. Teollisuudessa oli eniten (50 %) yrityksiä, jotka tunnistavat, että niillä on tietoa, joka saattaisi olla laittoman tiedustelun tai yritysvakoilun kohteena.

Joka kolmas yritys on törmännyt epäluotettavaan yhteistyökumppaniin

Joka kolmannella yrityksellä oli huonoja kokemuksia yhteistyökumppaneista. Vuoden 2017 kyselyssä epäluotettavasta yhteistyökumppanista raportoivia oli eniten kaupan alalla, jossa 40 prosenttia raportoi epäluotettavasta yhteistyökumppanista. Vuoden 2017 kyselyssä rakennusalan yrityksistä 38 prosentilla oli ollut epäluotettava yhteistyökumppani viimeisen kolmen vuoden aikana. Yhteistyökumppaniin tyytymättömien yritysten osuus rakennusalalla on kuitenkin jatkuvasti pienentynyt. Osuudet olivat keskimääräisellä kolmanneksen tasolla palvelualalla ja teollisuudessa. Kaikilla toimialoilla on kuitenkin niin paljon yrityksiä, jotka ovat kohdanneet epäluotettavia kumppaneita, että yhteistyökumppanin luotettavuuden arviointiin pitäisi käyttää yrityksissä selvästi nykyistä enemmän aikaa. Yrityksistä reilu puolet arvioi yhteistyökumppanin luotettavuutta.

Petokset kohdistuvatkin useammin suurempiin yrityksiin

Petokset ovat voimakkaassa kasvussa ja niitä tehdään yhä useammin tietoverkkojen avustuksella. Yrityksistä 13 prosenttia ilmoitti joutuneensa ulkopuolisen aiheuttaman petoksen kohteeksi viimeisen kolmen vuoden aikana. Monia petosyrityksiä pidetään julkisuudessa lähinnä pienten yritysten ongelmina. Yrityskokoluokkavertailussa ilmeni kuitenkin se, että pienissä ja keskisuurissa yrityksissä petosten kohtaaminen oli keskimääräisellä tasolla (12 - 13 %), kun taas suurista yrityksistä peräti neljännes (25 %) ilmoitti ulkopuolisen tekemistä petoksista. Petoksia voidaan kohdistaa tarkoituksella suuriin yrityksiin, joiden työntekijät eivät voi käytännössä aina tuntea toisiaan. Tämä helpottaa petoksen tekoa, mikäli henkilökunta ei ole varautunut petosyritysten mahdollisuuteen.

Lahjonnasta raportoidaan aiempaa enemmän, osuudet kuitenkin vielä pieniä

Vastanneista yrityksistä kolme prosenttia (1 %-->3 %) oli kohdannut lahjontaa viranomaisten kanssa asioidessa ja viisi prosenttia (3 %-->5 %) yritysten välisessä yhteistyössä. Lahjontaa havaitaan aikaisempaa enemmän, mutta osuudet ovat vielä keskimäärin melko pieniä. Yritysten osuus, jotka olivat kohdanneet lahjontaa viranomaisasioinnissa, kasvoi kaikilla toimialoilla useilla prosenttiyksiköllä vuosina 2012 - 2017.

Yritysten välisessä yhteistyössä lahjontaa kohtasivat eniten rakennusalalla toimivat yritykset. Lahjonnasta raportoivien rakennusalan yritysten osuus nousi yhdeksään prosenttiin (6 %-->9 %). Lahjonnasta yritysten välisessä yhteistyössä raportoivien kaupan alan yritysten osuus nousi neljästä prosentista kuuteen prosenttiin ja palvelualalla kahdesta kuuteen prosenttiin. Teollisuudessa muutos oli kolmesta neljään prosenttiin.

Yrityksen jatkuvuuden turvaamiseksi vielä tehtävää

Kaikista vastanneista yrityksistä vain hieman yli kolmasosalla oli jatkuvuussuunnitelma. Suuristakin vastaajista peräti neljäsosa ei ole tehnyt suunnitelmaa. Yrityksillä on merkittävä rooli koko yhteiskunnan häiriöidensietokyvyssä. Siksi jatkuvuussuunnitelmien määrää on saatava lisättyä kaikissa yrityskokoluokissa.

Suurimman sallitun keskeytysajan määrittäminen antaa johdolle käsityksen siitä, mitä kriittiset toiminnot ja palvelut ovat ja miten pitkään ne voivat olla pysähtyneenä. Joillakin yrityksillä saattaa olla toimintoja, jotka eivät voi olla lainkaan tai vain lyhyen aikaa keskeytyneenä. Kaikista vastanneista yrityksistä vain kolme kymmenestä (29 %) oli määritellyt suurimman sallitun keskeytysajan.

Nykyisin yhteistyökumppaniverkostolla ja alihankintaketjuilla on merkittävä rooli yrityksen toiminnan onnistumisessa. Suurien ja keskisuurien yritystenkin joukossa on vielä paljon yrityksiä, jotka eivät ole huomioineet alihankintaketjun jatkuvuuden varmistamista, vaikka ovat riippuvaisia alihankkijoidensa ja yhteistyökumppaneidensa toimitusvarmuudesta. Kaikista vastanneista yrityksistä vain yli neljäsosa oli sopinut kirjallisesti toimittajien kanssa häiriötilanteisiin varautumisesta.

Yrityksistä merkittävä osa ei saa tarvitsemaansa tietoa

Vain viidennes yrityksistä saa viranomaisilta rikosilmiöihin liittyvää tietoa. Tilanne on heikoin teollisuudessa, jossa 15 prosenttia saa tietoa. Erityisesti tietoa tarvitsee kaupan ala, johon kohdistuu keskimääräistä enemmän omaisuus-, henkilö- ja tietoriskejä. Kaupan alalla tietoa tarvitsee 45 prosenttia yrityksistä ja muilla toimialoilla kolmannes.

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 (2010) Innovaatioiden ja tiedon suojaaminen.

Helsingin seudun kauppakamari (2016). Yrityksiin kohdistuvat kyberuhat.

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

Huoltovarmuuskeskus (2013). PK-yrityksen kyberturvallisuuden kehittäminen.

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

Keskuskauppakamari (2006) Avainhenkilöriskit- opas yritysten avainhenkilöriskien hallintaan. Opas on laadittu Keskuskauppakamarin ja Keskusrikospoliisin yhteistyönä.

Keskusrikospoliisi (2011). Katsaus korruptiorikollisuuteen 2011.

Keskusrikospoliisi. Yrityksiin kohdistuvan rikollisuuden ja niitä hyödyntävän rikollisuuden tilannekuvat ja teematilannekuvat. Keskusrikospoliisin sivuilla on myös elinkeinoelämän ja viranomaisten yhteistyönä laadittu rikosten torjunnan toimintamalli ja tarkistuslista riskien kartoituksen avuksi. http://www.poliisi.fi/krp

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

Lehtonen, Jaakko (1999) Kriisiviestintä.

Mustatulevaisuus-verkkosivusto. http://www.mustatulevaisuus.fi. Harmaan talouden torjumiseksi laadittu verkkosivusto. Sivusto on laadittu viranomaisten ja järjestöjen yhteistyönä.

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

OP Ryhmä (2015). Artikkeli. Kyberturvallisuus – yrityksiä erehdytetään ovelilla sähköpostihuijauksilla
https://taloudessa.fi/2015/09/kyberturvallisuus-yrityksia-erehdytetaan-ovelilla-sahkopostihuijauksilla-2/

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

Siiki. Pertti (2010) Työturvallisuuslaki. Teos on työturvallisuusasioiden opas yrityksille ja työntekijöille. Teoksessa kuvataan työturvallisuusajattelun lähtökohdat ja työturvallisuuslain pääsisältö. Teos on kommentaari työnantajan ja työntekijän oikeuksista ja velvollisuuksista työturvallisuusasioissa.

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

Sisäasiainministeriön turvallisuusalan neuvottelukunta (2007) Palvelutyöpisteiden turvallisuussuunnitteluopas. Sisäasiainministeriön julkaisuja 47 / 2007.

Suomen toimitila- ja rakennuttajaliitto RAKLI ry ja Turva-alan yrittäjät (2004) Toimitilaturvallisuus ja sähköiset turvallisuusjärjestelmät.

Työsuhdeneuvonta.fi http://tyosuhdeneuvonta.fi

Tampereen teknillinen yliopisto, Turvallisuustekniikan laitos (2004) Kokonaisturvallisuuden edistäminen yrityksessä. Tutkimusraportti 17.8.2004.

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

Toimitilaturvallisuus ja sähköiset turvallisuusjärjestelmät -opas (2004)
http://www.turva-alanyrittajat.fi/doc/toimitilaturvallisuus.pdf

Työ- ja elinkeinoministeriö (2016). Selvitys harmaan talouden ja talousrikollisuuden torjunnan tehostamiseksi tarvittavista toimenpiteistä. Loppuraportti 22.3.2016.

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

Viestintävirasto (2016). Ohje 3/2016 Palvelunestohyökkäysten ehkäisy ja torjunta.

Elinkeinoelämän keskusliiton sivuilla on tietoa yritysturvallisuuden edistämisestä http://www.ek.fi

YRITYSTEN RIKOSTURVALLISUUS 2017-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 henkilöstöön kohdistuvat turvallisuusriskit viimeisen kolmen vuoden aikana…
lisääntyneet paljon
lisääntyneet jonkin verran
pysyneet ennallaan
vähentyneet jonkin verran
vähentyneet paljon

Toteutuneet riskit /uhat

Onko yrityksessänne viimeisen kolmen vuoden aikana…
Kyllä / Ei/ Ei osaa sanoa
työntekijä on joutunut työssään väkivallan uhriksi?
työntekijää on työssään uhkailtu /häiritty?
tapahtunut muuta työhön liittyvää rikosta työntekijää kohtaan?
avainhenkilöitä tai heidän läheisiään on uhattu työhön liittyen?
työntekijä syyllistynyt rikokseen / väärinkäytökseen yritystänne kohtaan?
työntekijä syyllistynyt rikokseen / väärinkäytökseen asiakastanne kohtaan?

Riskienhallintakeinot

Onko yrityksenne käyttänyt seuraavia riskienhallintakeinoja?
Kyllä / Ei/ Ei osaa sanoa

Taustaselvitykset työntekijöistä
Taustaselvitykset avainhenkilöistä
Yhteistyökumppanien luotettavuusselvitykset/arviointi
Asiakkaiden luottokelpoisuusselvitykset
Alihankkijoiden referenssien tarkastaminen
Salassapitosopimus on käytössä
Kilpailukieltosopimus on käytössä

Miten yrityksenne on varautunut ihmisiin kohdistuviin rikosriskeihin työtehtävissä?
Kyllä / Ei/ Ei osaa sanoa

Työympäristön teknisillä ratkaisuilla
Ohjeet mahdollisiin väkivalta- ja uhkatilanteisiin
Avainhenkilöille on varamiesjärjestelmä
Henkilötietojen suojaus on määritelty
Matkustamisesta on annettu turvallisuusohjeet
Työntekijöille annetaan turvallisuuskoulutusta
Työntekijöitä kannustetaan kertomaan havaitsemistaan turvallisuuspuutteista
Turvallisuusasiat ovat osa perehdyttämiskoulutusta

Onko yrityksenne varautunut 25.5.2018 voimaan tulevaan EU:n tietosuoja-asetukseen?
Kyllä/ Ei /Ei osaa sanoa

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

Kriittisistä yritysasioista kertominen luvatta kolmannelle osapuolelle
Luottamuksellista yritysasiaa sisältävän asiakirjan luovuttaminen luvatta kolmannelle osapuolelle
Yritystiedon (sisällön) luvaton urkkiminen / vakoilu
Tietojen luvaton kopiointi ennen siirtymistä pois yrityksen palveluksesta
Tietoverkkoon murtautuminen tai hakkerointi
Tietoverkkoon murtautumisen tai hakkeroinnin yritys
Tiedostojen tahallinen tuhoaminen
Identiteetti kaapattu tai yritetty kaapata rikolliseen toimintaan

Riskienhallintakeinot

Varautuminen tiedon väärinkäytöksiin (tiedon suojaus)

Kyllä / Ei/ Ei osaa sanoa

Onko yrityksellänne tärkeitä tietoja (liike- ja ammattisalaisuudet) koskeva luokittelu- ja käsittelyohje?
Onko yrityksellänne muita tietoja koskeva luokittelu- ja käsittelyohje?
Onko yrityksen tärkeimmät tiedot suojattu rajatuilla käyttöoikeuksilla?
Onko henkilökuntaa koulutettu salaisten / luottamuksellisten tietojen käsittelyyn?
Onko yrityksellänne erikseen ohjeet viranomaisten ja yhteistyökumppanien luovuttamille luottamuksellisille asiakirjoille ja tiedoille?
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

Myymälöissä, tuotannossa, kuljetuksissa tai varastoinnissa on ollut epätavallista hävikkiä
Tahallinen perättömän tiedon levittäminen yrityksestä
Yhteistyökumppani on ollut epäluotettava
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)
Vahingollisella tiedolla kiristäminen
Yrityksen tuotteita tai tavaramerkkejä on tietoisesti plagioitu

Riskienhallintakeinot

Miten yrityksenne on varautunut yrityksen toimintaan kohdistuviin rikosriskeihin työtehtävissä?
Kyllä/ Ei /Ei osaa sanoa

Yrityksellä on kirjalliset sopimukset yhteistyötahojen kanssa
Asiantuntijat tarkastavat sopimustekstit
Yrityksessä on käytössä asiantuntijoiden laatimia sopimuspohjia
Yrityksen johto tarkistaa merkittävimmät liiketoimintasopimukset
Taloushallintoa auditoidaan

Kuuluvatko yrityksen turvallisuusjohtamiseen seuraavat osat?
Kyllä/ Ei /Ei osaa sanoa

Yrityksen johto osallistuu henkilökohtaisesti turvallisuuden kehittämiseen
Turvallisuusasioita käsitellään henkilöstön kanssa
Yritysturvallisuuteen liittyvä kirjallinen riskikartoitus on tehty viimeisen kolmen vuoden aikana
Yrityksellä on toimintaohje poikkeustilanteita varten
Yritysturvallisuus on osa yrityksen vuotuista strategiasuunnittelua ja vuotuista budjetti- ja toimintasuunnittelua
Turvallisuus on osa yrityksen toiminta- tai laatujärjestelmää

5. LIIKETOIMINNAN JATKUVUUDENHALLINTA

Miten yrityksenne on varautunut liiketoiminnan jatkuvuudenhallintaan?
Kyllä/ Ei /Ei osaa sanoa

Kaikissa tilanteissa ylläpidettävät kriittiset toiminnot on kirjallisesti dokumentoitu.
Kriittisille palveluille/toiminnoille on määritelty suurin sallittu keskeytysaika, jonka aikana palvelu/toiminto ei ole käytettävissä.
Liiketoimintaa vakavasti haittaavien tilanteiden vaikutukset on arvioitu.
Liiketoiminnan jatkuvuuden kehittämistoimien toteutusta seurataan.
Kriittisten palvelu- ja hyödyketoimittajien häiriötilanteisiin varautumisesta on sovittu kirjallisesti.
Yrityksellä on jatkuvuussuunnitelma (yritys on määritellyt toimenpiteet liiketoiminnan turvaamiseksi eri tilanteissa).

Jos kyllä, Jatkuvuussuunnitelmassa esitetyt keskeiset toimintaohjeet on koulutettu henkilöstölle.
Yrityksellä on käytössään kriisiviestintäohje.
Tietojen käyttö häiriötilanteissa on varmistettu säännöllisesti otettavilla varmistus- ja palautusmenettelyillä.
Varautumisen ja jatkuvuudenhallinnan prosessia / toimintamallia on arvioitu viimeisen kahden vuoden aikana (esim. osana laadunvalvontaa, turvallisuusauditointia)

6. OMAISUUTEEN LIITTYVÄT RISKIT

Ovatko yrityksen omaisuuteen 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
Asiakkaan edustaja on auditoinut yrityksemme toimintatapoja
Yhteistyösopimukseen on kirjattu toimintatavat asiakkaan omaisuuden / 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
Ilkivalta yrityksen muuhun omaisuuteen
Työväline- tai laitevarkaus

Riskienhallintakeinot

Onko omaisuuden suojaamiseksi tehty seuraavia toimia?
Tuotanto- ja toimitilojen suojaus:
Kyllä/ Ei /Ei osaa sanoa
Eriytetyt tuotanto-, toimisto – ja tuotekehitystilat
Murtohälytys
Kulunvalvonta
Videovalvonta
Vierailujen ohjeistus
Vartiointi
Henkilöstön koulutus
Valvontajärjestelmien säännöllinen toimivuustestaus

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
Avainhenkilöturvallisuus
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?

KAUPPAKAMARI