



**YRITYSTEN RIKOSTURVALLISUUS 2005**  
RISKIT JA NIIDEN HALLINTA

*Julkaistavissa 7.11.2005 klo 11*

**KESKUSKAUPPAKAMARI  
JA  
HELSINGIN SEUDUN KAUPPAKAMARI**

YRITYSTEN RIKOSTURVALLISUUS 2005:  
**Riskit ja niiden hallinta**

Marraskuu 2005

Keskuskauppakamari, Aleksanterinkatu 17, PL 1000, 00101 Helsinki  
puh. (09) 696 969, faksi (09) 650 303  
[www.chamber.fi](http://www.chamber.fi)

ISBN 952-5620-00-X

## SAATTEEKSI

Suojautuminen rikoksilta ja väärinkäytöksiltä ja niihin varautuminen on yhä tärkeämpää suomalaisille yrityksille ja niiden henkilökunnalle. Rikosturvallisuus on yritysturvallisuuden olennainen osa.

Turvallisuuteen kuuluvien asioiden merkityksen korostumiseen on useita syitä. Suomalaiset yritykset toimivat yhä kansainvälisemmin, jopa maailmanlaajuisesti. Tietoverkot yhdistävät suomalaiset yritykset osaksi koko maailman kattavaa taloudellisen toimeliaisuuden verkkoa. Yritysten toimintaympäristö on voimakkaasti muuttunut. Yritysten rikosturvallisuutta heikentävien tekijöiden uhka on kasvamassa järjestäytyneen rikollisuuden, huumeiden, tietojärjestelmien vaurioittamisen sekä laittoman muuttoliikkeen vuoksi.

Keskuskauppakamari ja Helsingin kauppakamari osallistuvat aktiivisesti sisäasianministeriössä työn alla olevan yritysturvallisuusstrategian suunnitteluun ja sen toteuttamiseen. Yritysten rikosturvallisuuden lisäämiseen tähtäävien toimenpiteiden perustaksi Keskuskauppakamari ja Helsingin kauppakamari ovat laatineet oheisen koko maan kattavan selvityksen yritysten rikosturvallisuuden riskeistä ja niiden hallinnasta. Selvitys on jatkoa Helsingin seudun kauppakamarin ja Uudenmaan liiton vuonna 2004 julkaisemalle selvitykselle pääkaupunkiseudun yritysten liiketoiminnan riskeistä.

Lähes viidensadan suomalaisyrityksen johto on tähän selvitykseen antanut luottamuksellisesti arvokkaita tietoja ja näkemyksiä yrityksiin kohdistuvien rikos- ja väärinkäytösuhkien luonteesta ja vakavuudesta sekä suojautumis- ja varautumiskeinoista. Olemme kiitollisia yritysjohton merkittävästä panoksesta sekä siitä luottamuksesta, jota he ovat osoittaneet kauppakamarijärjestölle antamalla monessa suhteissa herkkää yritys kohtaista turvallisuustietoa selvityksen käyttöön.

Helsingissä 4.11.2005



Kari Jalas  
toimitusjohtaja  
Keskuskauppakamari



Heikki Perälä  
toimitusjohtaja  
Helsingin kauppakamari

## SISÄLLYS

|   |  |    |
|---|--|----|
| 1 | JOHDANTO .....   | 5  |
| 2 | YRITYSRIKOSTEN MÄÄRÄN KEHITYS .....  | 7  |
| 3 | IHMISET YRITYSRIKOSTEN UHREINA JA TEKIJÖINÄ .....  | 9  |
|   | 3.1 Työntekijään tai asiakkaaseen kohdistuvat rikosriskit.....   | 9  |
|   | 3.2 Riskienhallintakeinot ihmisiin kohdistuvien riskien vähentämiseksi .....                           | 11 |
|   | 3.3 Työntekijän, asiakkaan tai yhteistyökumppanin tekemät yritysririkokset ja<br>väärinkäytökset ..... | 13 |
|   | 3.4 Rikosten ja väärinkäytösten torjuminen.....  | 13 |
| 4 | TIETOOON KOHDISTUVAT RIKOKSET JA VÄÄRINKÄYTÖKSET.....  | 17 |
|   | 4.1 Tietoon kohdistuneet toteutuneet riskit ja uhkat .....   | 17 |
|   | 4.2 Riskienhallintakeinot: Miten yritykset varautuvat tiedon väärinkäyttöihin? .....                   | 21 |
| 5 | OMAISUUTEEN KOHDISTUVAT RIKOKSET JA VÄÄRINKÄYTÖKSET .....  | 25 |
|   | 5.1 Yrityksen hallussa oleva asiakkaan omaisuus, tieto ja suojaustarpeet.....                          | 26 |
|   | 5.2 Toteutuneet riskit ja uhkat.....   | 28 |
|   | 5.3 Riskienhallintakeinot: Onko omaisuuden suojaamiseksi tehty seuraavia toimia? ..                    | 30 |
|   | 5.4 Omaisuuteen liittyvät riskit: Irtaimen omaisuuden suojaus .....                                    | 34 |
| 6 | TOIMINTAAN KOHDISTUVAT RIKOKSET JA VÄÄRINKÄYTÖKSET.....  | 36 |
|   | 6.1 Toteutuneet riskit ja uhkat.....   | 36 |
|   | 6.2 Riskienhallintakeinot: Miten yritys on varautunut toimintaan kohdistuviin<br>rikosriskeihin?.....  | 39 |
| 7 | TURVALLISUUSJOHTAMINEN.....  | 41 |
| 8 | TURVALLISUUDEN KEHITTÄMINEN.....   | 44 |
|   | 8.1 Turvallisuuden kehittämisen painopisteet.....  | 44 |
|   | 8.2 Rikosriskeihin liittyvä tiedonsaanti.....  | 45 |
| 9 | JOHTOPÄÄTÖKSET.....  | 47 |
|   | LÄHTEITÄ JA LISÄTIETOA .....   | 49 |



## YRITYSTEN RIKOSTURVALLISUUS 2005

### 1 JOHDANTO

Selvitys käsittelee suomalaisten yritysten rikosturvallisuutta ja yrityksiin kohdistuvien rikosten ja väärinkäytösten torjuntaa. Selvitys perustuu 463 suomalaisen yrityksen sähköpostitse antamiin vastauksiin.

Taloustutkimus toteutti kyselyn Keskuskauppakamarin ja Helsingin seudun kauppakamarin toimeksiannosta. Yritykset vastasivat kyselyyn syyskuussa 2005. Yritysturvallisuuskyselyyn vastanneita yrityksiä ei mainita nimeltä selvityksessä, koska vastaukset ovat luottamuksellisia. Tutkimustulokset on esitetty taulukkoina ja kuviaina, joista yksittäisen vastaajan mielipide ei käy ilmi.

Selvityksen ovat laatineet asiamies Kaisa Saario Keskuskauppakamarista ja projektipäällikkö Panu Vesterinen Helsingin kauppakamarista. Selvitys on osa kauppakamarijärjestön yritysturvallisuustoimintaa.

Rikosturvallisuuskyselyyn vastanneista 463 yrityksestä 43 prosenttia edustaa palveluita ja liikennettä, 35 prosenttia teollisuutta ja energiaa ja 15 prosenttia kauppaa. Rakennusalan yrityksistä on vastaajista 7 prosenttia.

Vastaajaryhmien muodostaminen noudattaa läänijakoa. Vastaajista suurin osa on Etelä-Suomesta (43 %) ja Länsi-Suomesta (27 %), mikä vastaa kohtuullisen hyvin yritysten toimipaikkojen sijoittumista Suomessa. Itä-Suomea edustaa tutkimuksessa 5 prosenttia vastaajista. Oulun ja Lapin läänin vastaajia (6 %) käsitellään tutkimuksessa yhtenä kokonaisuutena, jotta vastaajajoukko on riittävän suuri vertailtavaksi.

Puolet (54 %) vastanneista yrityksistä on henkilömäärältään pieniä yrityksiä, jotka työllistävät alle 50 henkilöä. Neljännes (28 %) vastaajista on keskisuuria yrityksiä, joiden palveluksessa on 50 - 250 työntekijää. Suuret yritykset, jotka työllistävät yli 250 henkilöä, muodostavat viidenneksen (18 %) vastaajista.

Rikosturvallisuusselvityksen vastaajat olivat yritysten toimitusjohtajia (43 %), talous- tai hallintojohtajia (32 %) ja turvallisuuspäälliköitä (9 %). Kuudennes vastaajista (16 %) oli muita johtajia tai asiantuntijatehtävissä olevia.

Selvitys on jaettu lukuihin yrityksen suojattavien kohteiden (ihmiset, tieto, omaisuus ja yrityksen toiminta) perusteella. Jokaisessa luvussa on käsitelty sekä toteutuneita rikoksia ja väärinkäytöksiä että riskejä alentavia toimenpiteitä. Riskienhallintaa on käsitelty selvityksessä laajasti. Riskienhallinta suojaa yrityksen henkilöitä, omaisuutta, tietoa tai

toimintaa sisäisiltä ja ulkoisilta uhkilta. Lukujen loppuun on koottu riskienhallintaan liittyviä keskeisiä asioita. Niillä ei kuitenkaan korvata yrityksen omista lähtökohdista tehtävää riskikartoitusta. Selvityksen lähdeluetteloon on koottu lisätietoa yrityksen turvallisuusjohtamisen tueksi.

Selvityksessä on lisäksi tarkasteltu vastaajayritysten turvallisuusjohtamista ja turvallisuuskulttuuria sekä tiedonsaantia rikosilmiöistä. Vastaajayritykset ovat arvioineet rikosten määrän kehityssuuntaa sekä yrityksen turvallisuustyön lähivuosien kehittämiskohteita.

Selvityksessä on kursivilla lainauksia yritysten vapaamuotoisista vastauksista.

Selvityksessä käytetään netto- prosenttiosuutta. Luku ilmaisee, kuinka suuri osa vastaajista on ilmoittanut, että ainakin yksi mainituista riskeistä on toteutunut. Riskien hallintaa kuvaavissa kaavioissa osuus ilmaisee vastaavasti sen, kuinka monella vastaajalla on käytössä ainakin yksi esitellyistä riskienhallintakeinoista.

Koko maan kattava rikosturvallisuusselvitys on jatkoa Helsingin seudun kauppakamarin ja Uudenmaan liiton vuonna 2004 julkaisemalle selvitykselle pääkaupunkiseudun yritysten liiketoiminnan riskeistä. Tutkimusten tuloksia on verrattu soveltuvin osin toisiinsa.

## YRITYSTEN RIKOSTURVALLISUUS 2005

### 2 YRITYSRIKOSTEN MÄÄRÄN KEHITYS

Suomessa ei ole käytettävissä luotettavaa tietoa yritykseen kohdistuvasta rikollisuuden kokonaismäärästä. Tämä johtuu siitä, että yrityksiin kohdistuvaa rikollisuutta ei yleensä erikseen tilastoida. Yrityksillä ei myöskään ole lakisääteistä velvollisuutta ilmoittaa viranomaisille niihin kohdistuneista rikoksista. Suuri osa yrityksiin kohdistuvista rikoksista jää piilorikollisuudeksi. Tehokas rikollisuuden vähentäminen ja rikoshyödyn takaisinsaaminen edellyttäisivät kuitenkin rikoksien ilmoittamista viranomaisille.

Keskuskauppakamarin ja Helsingin seudun kauppakamarin yritysturvallisuuskyselyyn vastanneista 463 yrityksistä kolmasosa (34 %) arvioi, että rikosten määrä on kasvanut viimeisen kolmen vuoden aikana. Kaksi kolmasosaa (60 %) arvioi rikosten määrän pysyneen ainakin ennallaan. Vain viisi prosenttia yrityksistä vastasi, että rikosten määrä on vähentynyt viimeisen kolmen vuoden aikana.

Vastauksissa oli selviä eroja yrityksen kokoluokan mukaan. Vajaa kolmannes (31%) pienistä, alle 50 hengen yrityksistä, vastasi, että rikosten määrä on kasvanut viimeisen kolmen vuoden aikana. Keskiisuuret, 50 - 250 henkilön yritykset pitivät kasvua suurempana (36 %). Suurista, yli 250 henkilön yrityksistä, jopa neljä kymmenestä (41 %) arvioi rikosten määrän lisääntyneen.

Yritysten turvallisuusjohtajat arvioivat toimitusjohtajia useammin, että yritykseen kohdistuvat rikokset ovat olleet kasvussa viimeisen kolmen vuoden ajan. Turvallisuusjohtajista 40 prosenttia arvioi rikosten määrän kasvaneen, kun toimitusjohtajien kohdalla luku oli alhaisempi, 31 prosenttia.

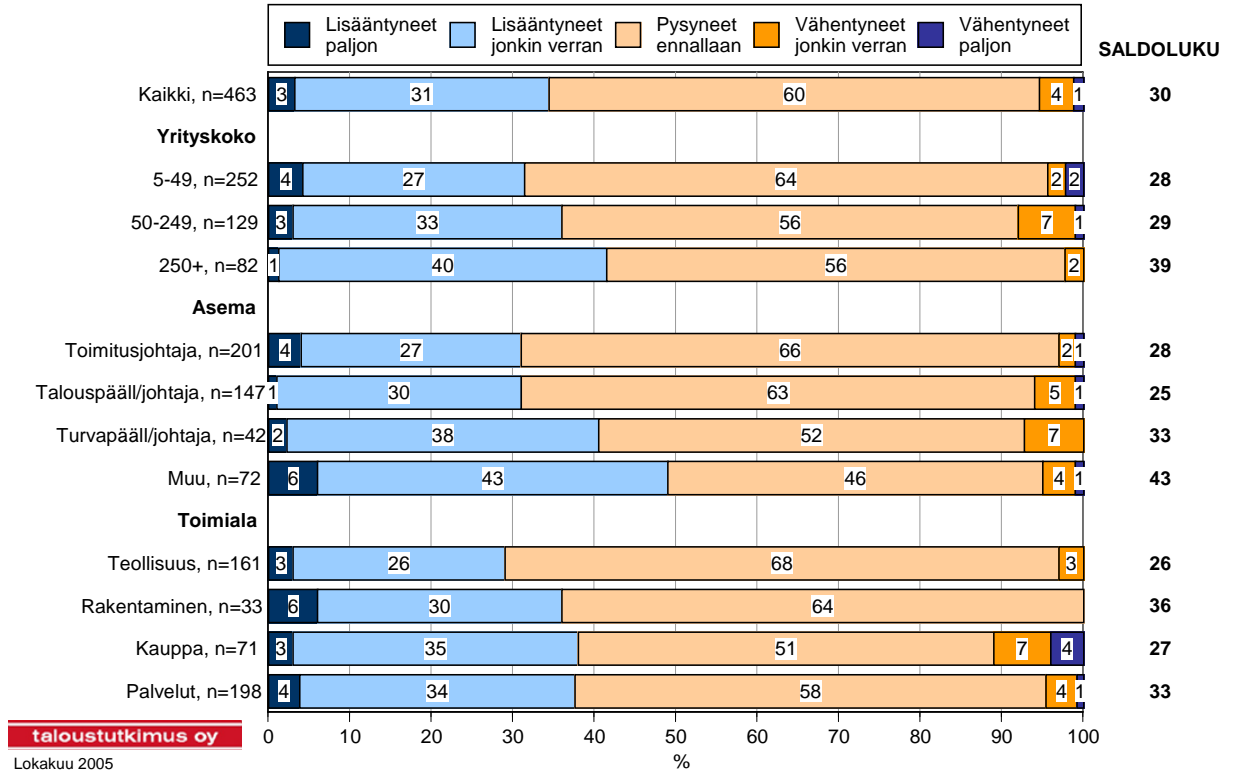
Vastauksissa ei ollut merkittäviä toimialakohtaisia eroja. Teollisuudessa vajaa kolmannes (29 %) vastaajista arvioi rikosten määrän kasvaneen, seitsemän kymmenestä (68 %) pysyneen ennallaan ja 3 prosenttia vähentyneen. Rakennusala erottui muista toimialoista siinä, että yksikään alan yritys ei nähnyt kehitystä myönteisenä. Yli kolmannes (36 %) vastasi rikosten määrän kasvaneen ja valtaosa (64 %) vastasi määrän pysyneen ennallaan.

Kaupan alalla vastauksissa oli eniten hajontaa. Jopa neljä kymmenestä (38 %) kaupan yrityksestä vastasi, että rikosten määrä on lisääntynyt kolmen vuoden aikana. Puolet (51 %) toimialan yrityksistä katsoi rikosten määrän pysyneen ennallaan. Yrityksissä oli eniten niitä, jotka arvioivat yrityksiin kohdistuvien rikosten määrän laskeneen.

Palvelualan vastaukset olivat lähellä kaikkien vastausten keskiarvoa. Palvelualalla valtaosa arvioi, että rikosten määrä on joko kasvanut (38 %) tai pysynyt ennallaan (58 %). Rikoksien määrän laskua oli havainnut 5 prosenttia vastaajista.

## YRITYSRIKOSTEN MÄÄRÄN KEHITYS

Onko yritykseen kohdistuneet rikosriskit ja väärinkäytökset viimeisen kolmen vuoden aikana...  
n=kaikki vastaajat



### 3 IHMISET YRITYSRIKOSTEN UHREINA JA TEKIJÖINÄ

#### 3.1 Työntekijään tai asiakkaaseen kohdistuvat rikosriskit

##### Väkivalta ja uhkailu

Vain harva työntekijä joutuu työssään yrityksen ulkopuolelta tulevan väkivallan kohteeksi. Kaikista yrityksistä 7 prosenttia vastasi työntekijän joutuneen väkivallan kohteeksi. Väkivalta oli huomattavasti keskimääräistä todennäköisempää kaupan alalla, jossa joka seitsemäs yritys (14 %) arvioi työntekijänsä joutuneen väkivallan kohteeksi viimeisen kolmen vuoden aikana. Myös palvelualan yrityksissä työntekijät joutuivat keskimääräistä useammin (8 %) väkivallan kohteeksi. Teollisuudessa ja rakentamisessa työntekijät joutuivat harvoin väkivallan kohteeksi. Näiden toimialojen yrityksistä vain 3 prosenttia arvioi työntekijänsä joutuneen väkivallan uhriksi.

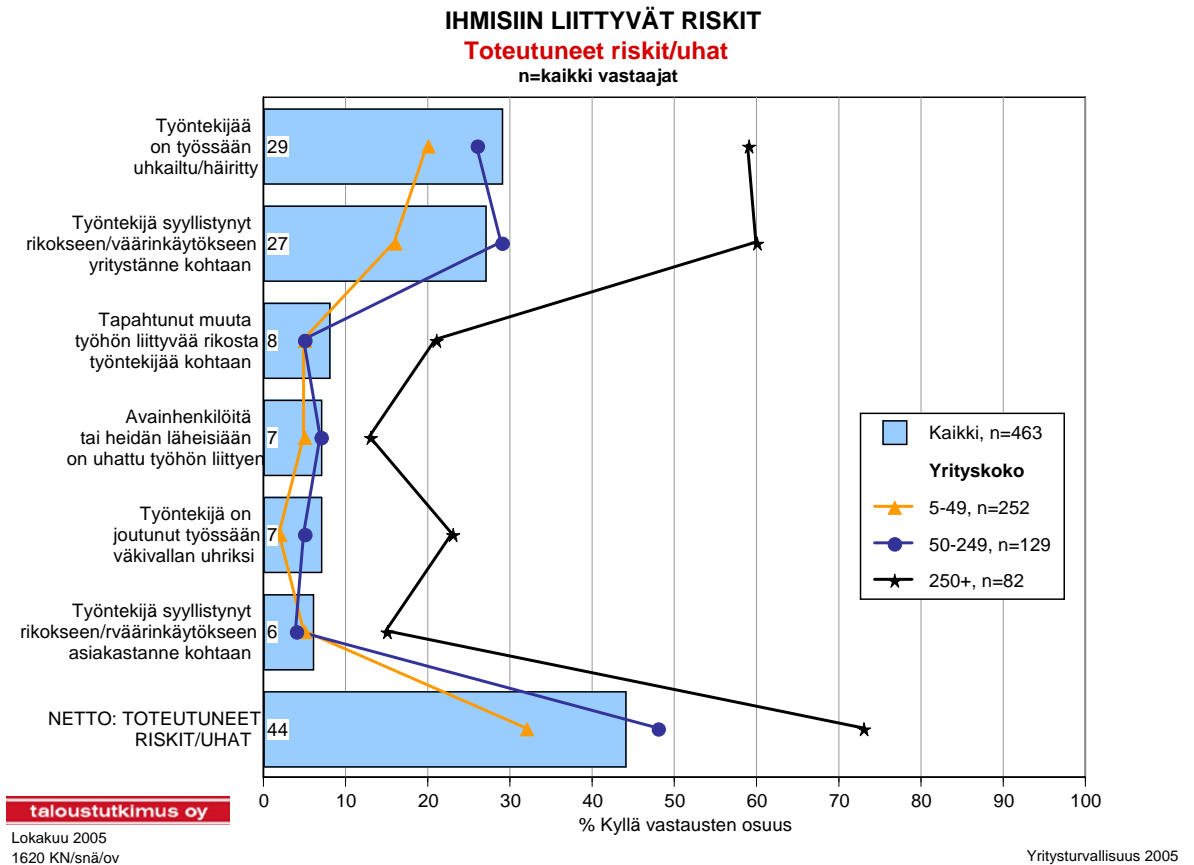
Henkilömäärältään suurimmissa, yli 250 henkilön yrityksissä joka viides vastaaja (23 %) arvioi työntekijän joutuneen väkivallan kohteeksi, kun taas pienissä, alle 50 henkilön yrityksistä vain 2 prosenttia työntekijöistä oli joutunut väkivallan kohteeksi. Keskisuurista yrityksistä 7 prosenttia oli kohdannut työväkivaltaa kolmen vuoden aikana.

Vastaajan asema yrityksessä vaikutti huomattavasti vastauksiin. Vajaa kolmannes (29 %) kyselyyn vastanneista turvallisuusjohtajista arvioi, että yrityksen työntekijä on joutunut työväkivallan kohteeksi kolmen vuoden aikana. Toimitusjohtajista vain 2 prosenttia oli havainnut työntekijöihin kohdistuvaa väkivaltaa.

Väkivallalla uhkailu oli vastaajayrityksissä varsinaista väkivaltaa yleisempää. Kaikista vastaajista vajaa kolmannes (29 %) ilmoitti työntekijöihin kohdistuneesta uhkailusta. Uhkailua oli keskimääräistä vähemmän pienissä ja keskisuurissa yrityksissä. Joka viidennen (20 %) pienen ja joka neljännen (26 %) keskisuuren yrityksen työntekijät olivat joutuneet uhkailun kohteeksi. Jopa kuusi kymmenestä (59 %) suuresta yrityksestä ilmoitti uhkailusta. Toimitusjohtajista valtaosa (85 %) ilmoitti, että yrityksen työntekijää ei ole uhkailtu, kun taas turvallisuusjohtajista vain kolmannes (33 %) ei ollut havainnut uhkailua.

Vaikka varsinaista väkivaltaa oli eniten kaupan alalla, niin väkivallalla uhkailu oli yleisintä palvelualan yrityksissä, joista joka kolmas (33 %) ilmoitti, että työntekijää on uhkailtu väkivallalla. Kaupassa (28 %), rakentamisessa (24 %) ja teollisuudessa (24 %) uhkailua oli hieman keskimääräistä vähemmän.

Yrityksen avainhenkilöllä tarkoitetaan yrityksen toiminnan kannalta vaikeasti korvattavaa henkilöä. Yrityksen avainhenkilöihin kohdistuu yleensä turvallisuushkia heidän asemansa, varallisuutensa, näkyvyytensä tai yrityksen toiminnan ja toimialan vuoksi.



Yrityksen avainhenkilöihin tai heidän läheisiinsä kohdistuva uhkailu ei ollut vastaajayrityksissä tuntematonta. Vastaajista 7 prosenttia kertoi, että yrityksen avainhenkilöjä tai heidän läheisiään oli uhattu viimeisen kolmen vuoden aikana. Valtaosassa (88 %) yrityksissä avainhenkilöä ei ollut uhkailtu. Uhkailu oli yleisintä suuremmissa yrityksissä.

Avainhenkilöt tai heidän läheisensä olivat joutuneet uhatuiksi joka kahdeksannessa (13 %) suuressa yrityksessä. Pienissä yrityksissä osuus oli selvästi pienempi, 5 prosenttia, ja keskiuurissa yrityksissä 7 prosenttia. Vastauksissa ei ollut merkittäviä toimialakohtaisia eroja. Avainhenkilöiden uhkailu oli hieman keskimääräistä harvinaisempaa (6 %) teollisuudessa ja yleisempää rakentamisessa (9 %) , kaupassa (8 %) ja muissa palveluissa (8 %).

### 3.2 Ihmisiin kohdistuvien riskien vähentäminen

Työnantajalla on velvollisuus huolehtia työntekijöiden turvallisuudesta. Työnantajan kannalta on tärkeää turvata liiketoiminnan jatkuvuus tilanteissa, joissa avainhenkilöön tai hänen läheiseensä on kohdistunut liiketoimintaan vaikuttava rikos tai onnettomuus.

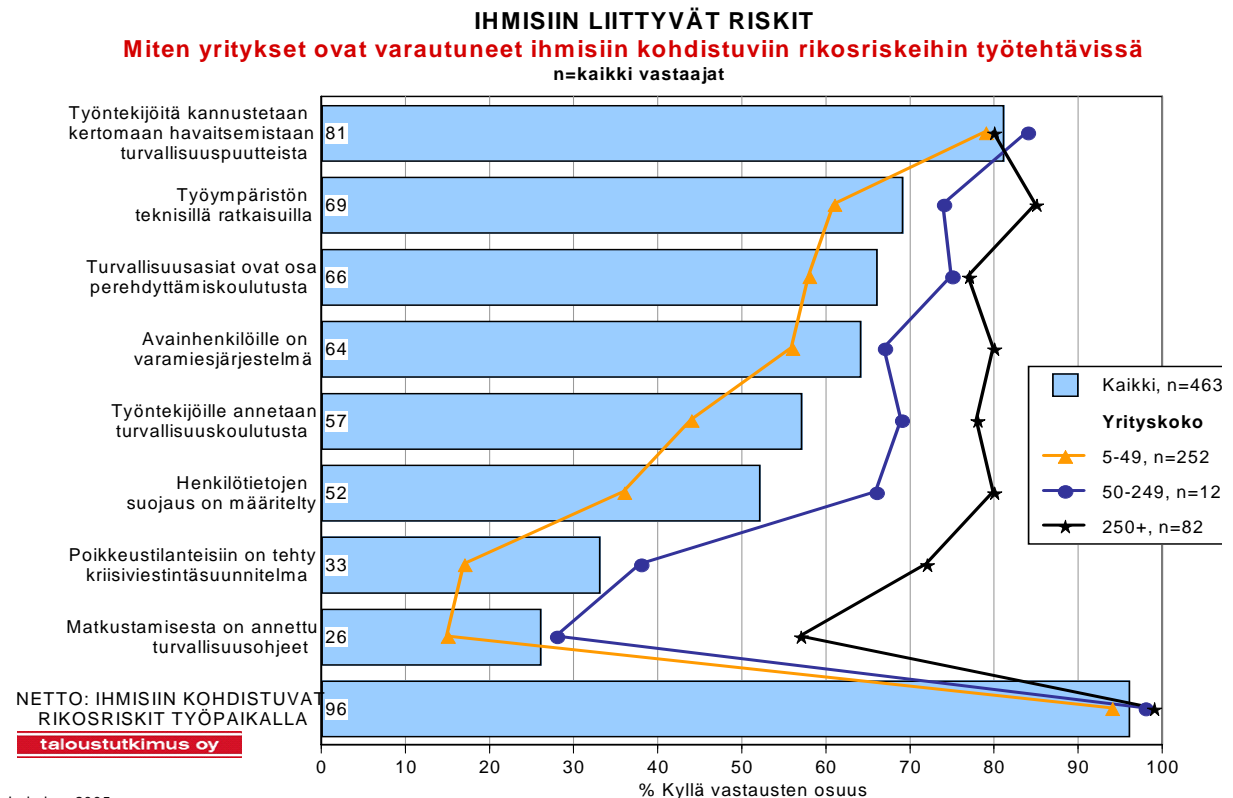
#### Työympäristön tekniset ratkaisut

Kyselyyn vastanneissa yrityksissä työhön liittyvä väkivalta liittyi muun muassa päihtyneiden tai huumautuneiden asiakkaiden kohtaamiseen tai erilaisiin murto-, anastus- ja näpistystilanteisiin. Väkivaltaa voidaan jossain määrin vähentää teknisillä turvatoimilla. Valvontalaitteet helpottavat myös väkivaltarikoksien selvittämistä.

Suurin osa vastanneista yrityksistä (69 %) on varautunut ihmisiin kohdistuviin rikosriskeihin työympäristön teknisillä ratkaisuilla. Teknisiin ratkaisuihin turvaututaan keskimääräistä yleisemmin keskisuurissa ja suurissa yrityksissä sekä kaupassa ja muualla palvelualalla.

#### Avainhenkilöiden varamiesjärjestelmä

*"Pienessä organisaatiossa avainhenkilöiden merkitys on suuri. Varamiesjärjestelmää ei pystytä helposti luomaan"*



Lokakuu 2005

Yrityksen avainhenkilöihin kohdistuu yleensä muuta henkilöstöä enemmän turvallisuusriskejä. Avainhenkilöriskien toteutuminen aiheuttaa heti kriisitilanteen yrityksessä. Avainhenkilöriskien vaikutusta yrityksen toimintaan voidaan pienentää siirtämällä ajoissa avainhenkilöillä olevaa tietoa ja osaamista useammalle henkilölle. Vastaajayritykset ovat varautuneet avainhenkilöihin kohdistuviin turvallisuusriskeihin melko hyvin. Kuudella kymmenestä (64 %) vastanneesta yrityksestä on avainhenkilöiden varamiesjärjestelmä. Pienissä yrityksissä avainhenkilöt ovat vaikeammin korvattavissa kuin suurissa. Pienistä yrityksistä vain puolella (56 %) oli avainhenkilöiden varamiesjärjestelmä. Suurista yrityksistä neljä viidestä (80 %) oli varautunut avainhenkilöiden korvaamiseen.

### **Kriisiviestintäsuunnitelma**

Usein yritysten kriisit ovat luottamuskriisejä: tukijat, rahoittajat, asiakkaat tai kansalaiset menettävät luottamuksensa yritykseen. Yrityksen henkilöstöön liittyvät ongelmat, esimerkiksi avainhenkilöiden joutuminen kielteisen julkisuuden kohteeksi, voivat aiheuttaa kriisin yrityksessä. Hyvin hoidetusta kriisiviestinnästä voi olla merkittävää hyötyä yritykselle.

Useimmissa vastaajayrityksissä ei ole kriisiviestintäsuunnitelmaa. Pienistä yrityksistä kahdeksan kymmenestä (79 %), keskisuurista puolet (57 %) ja suurista yrityksistä neljännes (24 %) ei ollut laatinut kriisiviestintäsuunnitelmaa. Teollisuusyrityksissä on useammin kriisiviestintäsuunnitelmia kuin muiden alojen yrityksissä.

### **Henkilötietojen suojaus**

Kyselyyn vastanneista pienistä yrityksistä vain reilu kolmannes (36 %) ilmoitti, että henkilötietojen suojaus on määritelty yrityksessä. Keskisuurissa yrityksissä luku oli selvästi korkeampi, 66 prosenttia, ja suurissa yrityksissä 80 prosenttia. Vastauksissa ei ollut merkittäviä eroja toimialoittain.

### **Matkustusohjeet**

Matkustusohjeet alentavat yrityksen henkilöstöön liittyviä riskejä yrityksen toimipaikan ulkopuolella. Matkustusohjeeseen olisi myös hyvä liittää kohta tiedonkäsittelystä matkojen aikana.

Vain harva yritys on antanut matkustusohjeita henkilöstölleen. Matkustusohjeet on joka kuudennella pienellä (15 %), joka neljännellä (28 %) keskisuurella ja joka toisella (57 %) suurella yrityksellä.

### **Turvallisuuskoulutus**

Motivoitunut, turvallisuustietoinen henkilöstö on tärkeä osa yrityksen rikosturvallisuutta. Yli puolet (57 %) vastaajayrityksistä on antanut työntekijöilleen turvallisuuskoulutusta. Turvallisuuskoulutusta ei ole järjestänyt 54 prosenttia pienistä, 29 prosenttia keskisuurista ja 18 prosenttia suurista yrityksistä. Turvallisuusasiat ovat osa perehdyttämiskoulutusta valtaosassa (66 %) yrityksistä. Turvallisuuskoulutus ja turvallisuusasioiden käsittely perehdyttämisvaiheessa olivat yleisimpiä teollisuudessa ja palvelualalla toimivissa yrityksissä.

### **Työntekijöiden vaikutusmahdollisuudet**

Työntekijöiden vaikutusmahdollisuudet turvallisuusasioihin ovat vastaajien mukaan hyvät. Neljä viidestä yrityksestä vastasi, että yrityksen työntekijöitä kannustetaan kertomaan havaitsemistaan turvallisuuspuutteista. Yrityksen koko tai toimiala eivät vaikuta työntekijän vaikutusmahdollisuuksiin. Turvallisuusjohtajat vastasivat muita vastaajia useammin, että työntekijöitä on kannustettu kertomaan puutteista.

### 3.3 Työntekijän, asiakkaan tai yhteistyökumppanin tekemät yritysrikokset ja väärinkäytökset

Kyselyyn vastanneista 463 yrityksestä 27 prosenttia vastasi, että yrityksen työntekijä on syyllistynyt rikokseen tai väärinkäytökseen omaa yritystä kohtaan. Työntekijän rikokset ja väärinkäytökset olivat keskimääräistä yleisempiä Etelä- (31 %) ja Länsi-Suomessa (28 %) ja keskimääräistä harvinaisempia Oulun läänin ja Lapin alueilla (23 %) sekä Itä-Suomessa (16 %).

Työntekijän tekemät rikokset yleistyvät yrityksen koon kasvaessa. Työntekijän tekemiä rikoksia ja väärinkäytöksiä oli ollut joka kuudennessa (16 %) pienessä yrityksessä, lähes joka kolmannessa (29 %) keskisuudessa yrityksessä ja kuudessa kymmenestä (60 %) suuresta yrityksestä. Työntekijän tekemät rikokset keskittyivät selvästi kaupan alalle, jossa 41 prosenttia vastaajista ilmoitti työntekijän rikoksesta tai väärinkäytöksestä. Rakennusalan yrityksissä työntekijän yritystä kohtaan tekemiä väärinkäytöksiä oli muita yrityksiä vähemmän.

Työntekijän tekemät rikokset tai väärinkäytökset kohdistuivat harvoin asiakkaaseen. Valtaosa (86 %) yrityksistä ilmoitti, että työntekijä ei ole tehnyt rikosta tai muuta väärinkäytöstä asiakasta kohtaan. Osuus oli muita yrityksiä vähäisempi suurissa yrityksissä (71 %).

### 3.4 Rikosten ja väärinkäytösten torjuminen

Työnantajan tehtävänä on suojata yritystä ja sen toimintaa myös oman henkilöstön aiheuttamilta tahallisilta tai tahattomilta uhkilta. Turvallisuustoimenpiteiden pitää olla lain mukaisia ja myös eettisesti hyväksyttäviä. Tässä käsiteltyjen riskienhallintatoimenpiteiden lisäksi turvallisuustietoisuuden lisäämisellä voidaan ehkäistä sitä, että turvatoimet pettävät työntekijän tahattoman toiminnan vuoksi.

#### Työntekijöiden ja avainhenkilöiden taustaselvitykset

*”Tuli palkattua töihin väärä henkilö, joka ongelmien tullen muodostui vakavaksi turvallisuusriskiksi.”*

*”Henkilöstöön päässyt epärehellinen henkilö voi tehdä paljonkin haittaa.”*

Uuden henkilön palkkaamiseen liittyy usein riskejä. Huolellisella rekrytoinnilla ja henkilöiden taustaselvityksillä yritys pystyy vähentämään merkittävästi henkilökuntaan liittyviä turvallisuusriskejä ja varmistamaan, että palkattava henkilö sopii yritykseen.

Kolmannes (33 %) yrityksistä selvittää palkattavan henkilön taustan. Taustaselvitysten tekeminen ei ollut yleistä missään kokoluokassa. Pienistä yrityksistä vain vajaa kolmannes (29 %), keskisuurista yrityksistä kolmannes (35 %) ja suurista yrityksistä neljä kymmenestä (44 %) oli tehnyt taustaselvityksiä. Kaupan ja muun palvelualan yritykset tekivät keskimääräistä yleisemmin taustaselvityksiä.

Yritykset selvittävät avainhenkilöidensä taustat huolellisemmin kuin muun henkilökunnan taustat. Vastanneista yrityksistä puolet (49 %) oli tarkastanut avainhenkilöiden taustatietoja. Pienistä yrityksistä neljä kymmenestä (42 %), keskisuurista yrityksistä puolet (51 %) ja suurista yrityksistä seitsemän kymmenestä (67 %) oli selvittänyt avainhenkilöiden taustoja. Vastauksissa ei ollut toimialakohtaisia eroja.

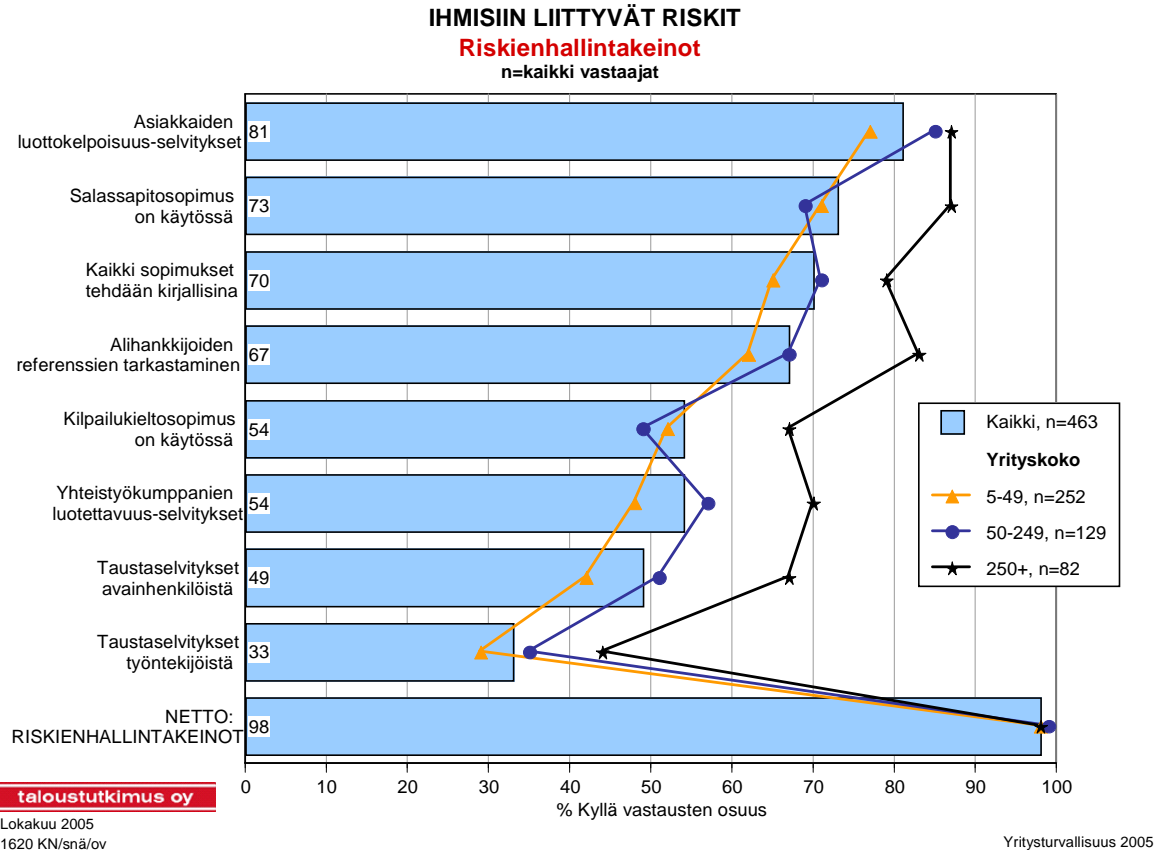
## Salassapito- ja kilpailukieltosopimukset

*"Yritysturvallisuuden suurimpana riskinä ovat poislähtevät henkilöt."*

*"Henkilöt voivat siirtyä suoraan kilpailijalle ja viedä asiakastiedot dokumentteina tai ainakin päässään."*

*"Työntekijän luotettavuudesta on kiinni, pysyykö tieto yhtiön omaisuutena vai ei."*

*"Meillä ei ollut kilpailukieltosopimusta ja kahden edustajan lähtö vei meiltä yllättäen edustuksia ja meillä tehdyt tarjoukset tehtiin uudelleen toisen yrityksen nimissä."*



Yrityssalaisuutta suojaavat laki sopimattomasta menettelystä elinkeinotoiminnassa, työsopimuslaki ja rikoslaki. Yritysten kannalta on ongelmallista erityisesti se, että lait eivät ole tässä suhteessa samansisältöisiä. Vain rikoslakiin on tehty lisäys siitä, että työsuhteen päättymisen jälkeen työntekijä ei saa ilmaista yrityssalaisuuksia kahteen vuoteen. Salassapitosopimukset ovatkin yleistyneet lainsäädännön ja immateriaalisuojan puutteellisuuden sekä yritysten kansainvälistymisen vuoksi. Salassapitosopimus voidaan solmia esimerkiksi yritysneuvotteluiden, projektin tai työ- tai toimeksiantosuhteen alkaessa tai salassa pidettävää tietoa luovutettaessa. Salassapitosopimus (NDA, Non Disclosure Agreement) tai sitoumus korostaa yrityssalaisuuksien ja tietotaidon huolellisen säilyttämisen merkitystä ja selkiyttää rikkomistapauksissa työsuhteen päättämisen ja vahingonkorvausvelvollisuuden edellytyksiä.

Vastanneet yritykset käyttävät melko yleisesti salassapitosopimuksia.

Salassapitosopimukset ovat käytössä kolmella neljästä (73 %) yrityksessä. Suurten yritysten kohdalla luku on vielä korkeampi, 87 prosenttia. Yleisimmin salassapitosopimusta käytetään palvelualalla (80 %), kaupassa (75 %) ja teollisuudessa (69 %). Salassapitosopimusten käyttö on vähäisintä rakennusalaalla (45 %). Vastaajilta ei kysytty salassapitosopimusten sisällöstä.

Kilpailukieltosopimusta käytetään salassapitosopimusta harvemmin. Kilpailukieltosopimuskin on käytössä joka toisella yrityksellä (54 %). Kilpailukieltosopimuksen käytössä ei ole suuria eroja toimialojen ja yrityskoon suhteen. Yleisintä kilpailukieltosopimuksen käyttö on kuitenkin suurissa yrityksissä sekä kaupassa ja muualla palvelualalla.

### **Yhteistyökumppanien luotettavuus ja asiakkaiden luottokelpoisuus**

*"Ajan tasalla olevien tietojen saanti esimerkiksi yritys- ja luottotietorekisteristä on osoittautunut ongelmalliseksi, yritysten tilinpäätöstiedot ovat vanhentuneita, yksityisistä on vähän tietoa saatavilla."*

*"Aliurakoitsijoiden ja vuokratyövoiman kontrollointi on ongelmallista "*

Puolet (54 %) vastanneista yrityksistä tarkastaa yhteistyökumppaninsa luotettavuuden. Pienissä ja keskisuurissa yrityksissä riskienhallintatoimet ovat tässä asiassa keskimääräisellä tasolla, kun taas suurista yrityksistä lähes kolme neljästä (70 %) tarkistaa yhteistyökumppaninsa luotettavuuden. Yhteistyökumppanien taustojen tarkistaminen on yleisintä rakentamisessa (67 %) ja kaupassa (61 %). Yhteistyökumppanien luotettavuus tarkistetaan useimmin Etelä-Suomessa ja muita vertailualueita harvemmin Itä-Suomessa.

Asiakkaiden luottokelpoisuus selvitysten tekeminen on vastaajayrityksissä hyvin yleistä. Valtaosa (81 %) yrityksistä selvittää asiakkaan luottokelpoisuuden. Toimialoista luottokelpoisuuden selvittäminen oli yleisintä kaupan alalla (93 %).

### **Alihankkijoiden referenssien tarkistaminen**

Yrityksen alihankkijat ja palveluntuottajat voivat olla yrityksen rikosturvallisuuden heikkoja kohtia, mikäli yritys laiminlyö turvallisuusnäkökohtia. Palveluntoimittajan toiminta tapahtuu kuitenkin usein yrityksen tiloissa. Palveluntuottajan työntekijöillä on laajat oikeudet liikkua ja toimia tilaajayrityksen tiloissa. Heidän ulottuvillaan on usein runsaasti yritystä koskevaa tietoa. Alihankkijat ja palveluntuottajat voivat myös tahattomasti aiheuttaa riskitilanteita, mikäli näiden yritysten työntekijöitä ei ole perehdytetty turvallisuusasioihin.

Neljännes (25 %) kaikista yrityksistä ei ole tarkistanut alihankkijoiden referenssejä. Pienissä ja keskisuurissa yrityksissä riskienhallintatoimet ovat lähes samalla tasolla. Suurista yrityksistä vain 5 prosenttia ei ole tarkistanut alihankkijoiden referenssejä. Teollisuudessa ja rakentamisessa toimivat yritykset tarkastavat muiden alojen yrityksiä useammin alihankkijoiden referenssit.

### **Kirjalliset sopimukset**

Suurin osa (70 %) yrityksistä tekee kaikki sopimukset kirjallisina. Vastauksissa ei ole merkittäviä eroja yrityksen koon suhteen. Turvallisuusjohtajat vastasivat selvästi muita vastaajaryhmiä useammin, että yrityksen kaikki sopimukset tehdään kirjallisina. Kirjalliset sopimukset olivat yleisimmin käytössä kaupassa ja palvelualalla.

**Tarkistuslista 1: Ihmisiin liittyviin rikosriskeihin ja väärinkäytöksiin varautuminen**

- Taustaselvitykset työntekijöistä
- Taustaselvitykset avainhenkilöistä
- Yhteistyökumppanien luotettavuusselvitykset
- Asiakkaiden luottokelpoisuusselvitykset
- Alihankkijoiden referenssien tarkastaminen ja ulkoistuksen turvallisuus
- Kaikki sopimukset kirjallisina
- Salassapitosopimus
- Kilpailukieltosopimus
- Työväkivallan vähentäminen: Työtilan järjestelyt, henkilökunnan koulutus väkivaltatilanteiden hallitsemiseksi ja välttämiseksi, turvalliset toimintatavat, riskinäkökulmien huomioonottaminen, uhkatilanteen jälkiselvittely ja uhrin auttaminen
- Avainhenkilöille on varamiesjärjestelmä
- Liiallisen avoimuuden välttäminen
- Kriisiviestintäsunnitelma
- Henkilötietojen suojaus
- Matkustamisen turvallisuusohjeet
- Työntekijöiden turvallisuuskoulutus
- Työntekijöiden kannustus kertomaan havaitsemistaan turvallisuuspuutteista
- Turvallisuusasiat osaksi perehdyttämiskoulutusta

## YRITYSTEN RIKOSTURVALLISUUS 2005

### 4 TIETOON KOHDISTUVAT RIKOKSET JA VÄÄRINKÄYTÖKSET

Jokaisella yrityksellä koosta tai toimialasta riippumatta on yrityssalaisuudeksi luokiteltavaa tietoa. Yritysten ei ole helppoa tunnistaa suojattavaa tietoaan ja luokitella sitä asianmukaisesti. Tiedon suojaamisen merkitys korostuu myös rikosoikeudellisten seuraamusten arvioinnissa. Yritys ei ole aina saanut oikeussuojaa tilanteissa, joissa on herätty tietoturvallisuuden vasta tietoon kohdistuneen teon jälkeen.

Yrityssalaisuusrikosten selvittämiseksi tiedon suojaamisessa on osoitettava tarve, tahto ja käytännön toimenpiteet tiedon suojaamiseksi. Tämä tarkoittaa vähintään tiedon luokittelua, henkilöstön kouluttamista tiedon oikeaan käsittelyyn ja vaatimusta siitä, että tiedolla on taloudellista arvoa yritykselle.

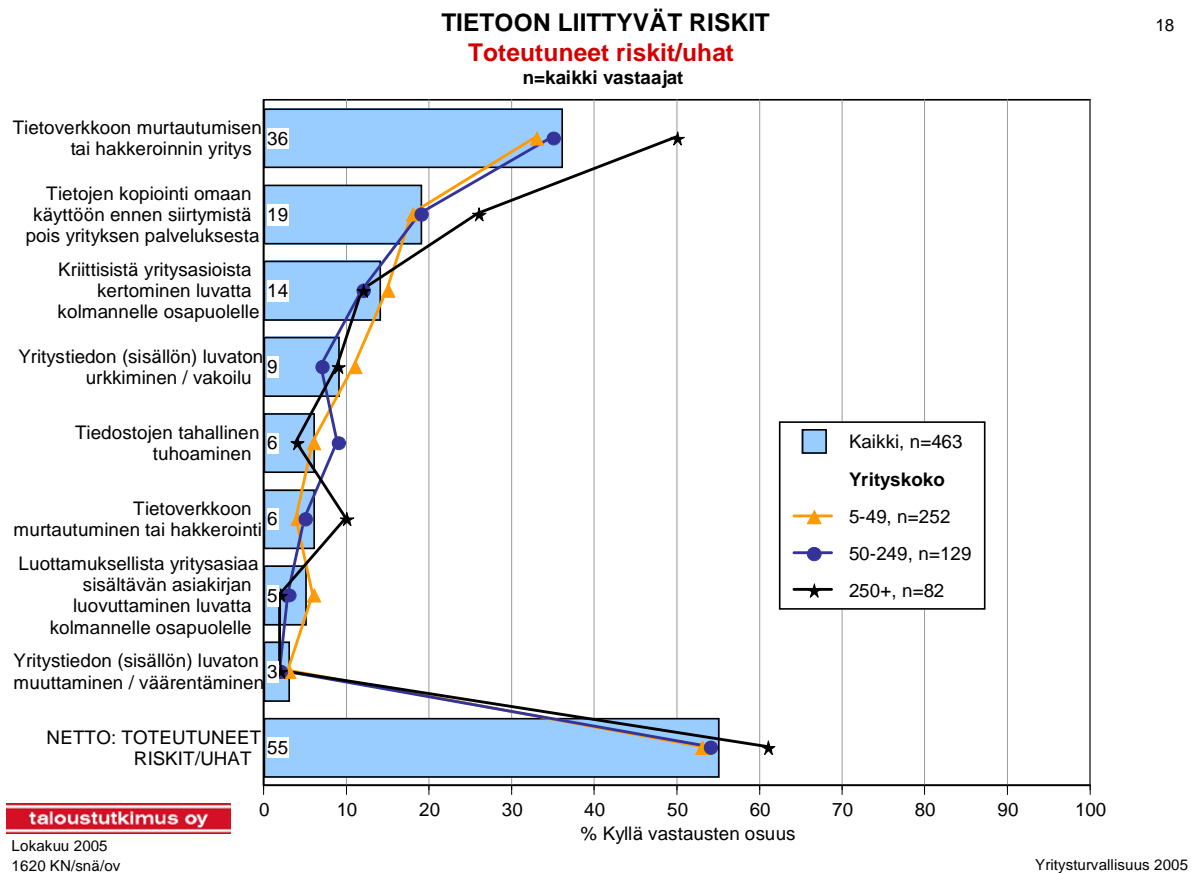
Yrityksen tietoturvassa tekniset välineet kuten palomuuuri ja salausten menetelmät eivät riitä, vaan yrityksen on opastettava henkilöstöä riskienhallintaan. Koulutuksella ehkäistään esimerkiksi sosiaalista krakkerointia (engl. social engineering). Termillä tarkoitetaan sitä, että työntekijää harhautetaan tai taivutellaan antamaan asiattomalle tunkeilijalle pääsy yrityksen tietojärjestelmiin tai sen sisältämään tietoon.

”Ei osaa sanoa” –vastausten suuri osuus tiettyjen kysymysten osalta kertoo siitä, että kyseessä voi olla piiloon jäävä ilmiö, jonka ilmitulo saattaa olla mahdotonta tai sattumanvaraista.

#### 4.1 Tietoon kohdistuneet toteutuneet riskit ja uhat

##### Tietoverkkoon murtautumisen tai hakkeroinnin yritys

Kaikista vastaajista yli kolmannes (36 %) oli havainnut, että ulkopuolinen oli luvattomasti yrittänyt päästä yrityksen tietoverkkoon. Tulosta arvioitaessa on muistettava, ettei kaikilla yrityksillä ole tietotaitoa tunnistaa näitä yrityksiä. Joka toisessa suuressa vastaajayrityksessä oli havaittu luvaton yritys päästä tietoverkkoon. Ero henkilömäärältään pienten (33 %) ja keskisuurten (35 %) vastaajayritysten havaitsemiin murtautumis- tai hakkerointirytyksiin selittyy osin suurien yritysten tunnettavuudella, joka tekee niistä kiinnostavia kohteita. Erot saattavat myös johtua siitä, että pienemmissä yrityksissä ei aina osata tunnistaa murtautumis- tai hakkerointirytyksiä. Kaikista vastaajaryityksistä joka viides (20 %) ei osannut sanoa, onko heidän tietoverkkonsa yritetty murtautua. Suurimpien vastaajaryitysten osalta tämä osuus oli 27 prosenttia.



Palvelualan yrityksistä 42 prosenttia oli joutunut tietoverkkoon murtautumisen tai hakkeroinnin yrityksen kohteeksi. Harvinaisinta se oli rakennusallalla (21 %).

### Tietoverkkoon murtautuminen tai hakkerointi

*"Hakkerointi konsultin koneeseen, vaikka suojajärjestelmät olivat toiminnassa. Suojausta parannettiin. Päivitykset tehdään ajallaan. Koko suojaamiseen kiinnitettiin huomiota julkisuutta saaneen lehtijutun jälkeen. Yrityksemme lienee jatkuvan sosiaalisen hakkeroinnin kohteena ja kilpailijaseurannan alaisena."*

Murtautumiset tai hakkeroinnit noudattivat suunnilleen samanlaista suhdetta kuin havaitut yritykset murtautua tai hakkeroida. Kokonaisuutena noin joka kahdeskymmenes vastaajayritys oli joutunut tietoverkkoon murtautumisen tai hakkeroinnin kohteeksi. Suurimmissa yrityksissä joka kymmenes tietomurto tai hakkerointi oli onnistunut. Pienimmistä ja keskisuurista vastaajayrityksistä vain joka kahdeskymmenes oli joutunut vastaavan teon kohteeksi. Kaikista vastaajayrityksistä joka seitsemäs (14 %) ei osannut sanoa, onko heidän tietoverkkoonsa murtauduttu. Suurimmista vastaajayrityksistä näin vastasi noin joka viides (21 %) vastaaja.

### Yritystiedon luvaton urkkiminen tai vakoilu

*"Avotoimistot, henkilöstön vapaa liikkuminen eri työpisteissä, salakuuntelu, juoruilu ja perättömien huhujen levittäminen, tietojen kertominen esimerkiksi perheelle."*

*"Alihankkijan edustaja otti kamerakännykällä kuvan asiakkaan tuotteesta, vaikka se oli erikseen kielletty."*

Turvallisuustietoisuuden lisääminen on yksinkertaisin tapa torjua laitonta tiedonkeruuta. Mikäli ilmiötä ja sen eri muotoja ei tunneta, torjuminen on vaikeaa.

Yritystietoon kohdistuvan luvattoman mielenkiinnon kohteeksi oli vastaajayrityksistä joutunut keskimäärin joka kymmenes yritys (9 %). Erot vastaajayritysten välillä olivat pienet. Useimmiten kohteeksi oli joutunut pieni yritys (11 %). Keskisuurista yrityksistä 7 prosenttia oli joutunut luvattoman tiedonkeruun kohteeksi. Lähes joka viides yritys (19%) ei osannut sanoa, onko siihen kohdistunut luvattonta urkintaa tai vakoilua. Suurimmista yrityksistä useampi kuin joka neljäs (27 %) ei osannut sanoa, onko näin tapahtunut.

Yleisintä luvaton urkkiminen tai vakoilu oli palvelualan yritysten keskuudessa, joista noin joka seitsemäs (13 %) oli joutunut sen kohteeksi.

### **Tietojen kopiointi omaan käyttöön ennen siirtymistä pois yrityksen palveluksesta**

*"Avainhenkilön poislähdön yhteydessä tietoa hävisi PC:ltä, varmistukset tältä osin eivät toimineet."*

Lähtevän työntekijän tekemä tiedonkopiointi on ehkä vaikein tiedon suojaamisen haasteista. Työntekijällä on työsuhteensa ajan pääsy työnsä kannalta tarpeelliseen tietoon. Monissa yrityksissä työntekijällä on pääsy myös oman työtehtävänsä kannalta tarpeettomaan, mutta yritykselle tärkeään tietoon. Työntekijän siirtyessä kilpailijan palvelukseen tietoa voi siirtyä uudelle työnantajalle. Samalla työntekijä saattaa viedä myös tietoa omaan toimenkuvaansa liittymättömältä liiketoiminnan alueelta. Esimerkiksi myyntihenkilö saattaa viedä mukanaan tuotekehitystietoa.

Lähes joka viidennessä vastaajayrityksessä (19 %) poislähtevä työntekijä oli kopioinut tietoja. Pienten (18 %) ja keskisuurten (19 %) yritysten välillä ei ollut suurta eroa. Ongelma oli isompi suurissa yrityksissä. Joka neljännes (26 %) suuren vastaajayrityksen työntekijän tiedettiin kopioineen yrityksen tietoja ennen työpaikan vaihtoa. Kaikista vastaajista yli neljännes (27 %) ei osannut sanoa, onko työntekijä kopioinut tietoja ennen poislähtöään. Suurimmista vastaajayrityksistä lähes joka toinen (45 %) ei osannut kertoa, onko näin tapahtunut.

Viidenneksessä palvelualan (22 %) ja neljänneksessä kaupan alan (24 %) yrityksistä oli lähtevä työntekijä kopioinut tietoja itselleen.

Vuonna 2004 Uudellamaalla tehdyssä kyselyssä joka kuudennessa (17 %) yrityksessä lähtevä työntekijä oli kopioinut yrityksen tietoja omaan käyttöönsä ennen pois lähtemistään. Vertailu vuoden 2005 vastaaviin tuloksiin osoittaa, että kopioiminen on yleistynyt.

### **Kriittisistä yritysasioista kertominen luvatta kolmannelle osapuolelle**

*"Sisäinen tietoturvallisuus pitää saada kuntoon jotta voidaan rajata vuodot ulospäin."*

Kriittisen yritystiedon luvaton kertominen on yleistä. Kertominen saattaa perustua esimerkiksi haluun vahingoittaa työnantajaa, oman tärkeiden ja tietämisen korostamisen tarpeeseen tai se saattaa olla tahatonta. Useimmiten tämä tapahtuu tuttujen henkilöiden kesken. Keskusteluilla on kuitenkin monesti myös muita kuulijoita kuin varsinaisen keskustelun osapuolet.

Kriittisten tietojen luvaton kertominen on lähellä yritysvalokailua. Jälkikäteen on hyvin vaikea saada selville, onko tieto keskustelussa paljastunut kuuntelevan osapuolen johdattelemana vai onko kyseessä ollut vain edellä mainittu kertojan oma motiivi.

Noin joka seitsemännessä vastaajayrityksessä (14 %) oli kerrottu kriittisistä yritysasioista luvatta. Kysymyksessä ei ollut eritelty, oliko taho jolle kerrottiin, talon väkeä vai ulkopuolinen. Yleisintä luvaton kertominen oli pienimmissä vastaajayrityksissä (15 %). Ero keskisuuriin (12 %) ja suuriin (12 %) vastaajayrityksiin oli pieni. Joka viides yritys (20 %) ei osaa sanoa, onko

kriittisistä yritysasioista kerrottu luvatta kolmannelle taholle. Suurimmista vastaajista joka kolmas (34 %) vastaa, ettei osaa sanoa, onko näin tapahtunut.

Muista palvelualan yrityksistä useammassa kuin joka kuudennessa (17 %) oli kerrottu luvatta kriittisistä yritysasioista ulkopuoliselle.

### **Luottamuksellista yritysasiaa sisältävän asiakirjan luovuttaminen luvatta kolmannelle osapuolelle**

Luottamuksellisen asiakirjan luovuttamista on usein vaikea saada selville, koska vastaanottaja tai luovuttaja eivät paljasta luovutusta.

Vastaajayrityksistä joka kahdeskymmenes (5%) kertoo, että yrityksen luottamuksellinen asiakirja on luovutettu luvatta. Näissä tapauksissa on täytynyt yrityssalaisuuden luvattoman paljastamisen yritys. Kun huomioidaan, että lähes joka viides (17%) vastaajayritys ei osaa sanoa, onko näin tapahtunut, on ilmeistä, etteivät yritykset aina kykene näyttämään toteen tällaista toimintaa. Suurimmista vastaajayrityksistä lähes joka kolmas (30%) vastaa, ettei osaa sanoa, onko näin tapahtunut.

### **Tiedostojen tahallinen tuhoaminen**

*"En näe suuria uhkia, mutta suurin osa yrityksen tiedoista on kaikkien saatavilla"*

*"Uhka tulee yleensä yrityksen sisältä, tiedon jako ja siihen pääsy yleensä vapaata ja pääsy siihen vaikeasti rajattava. Sisältä tapahtuvaa tuottamuksellista yritysturvallisuuden vahingoittamista on erittäin vaikea estää."*

*"Tietoverkon salasana annettiin tekaistun kertomuksen perusteella ulkopuoliselle."*

Tiedostojen tuhoaminen saattaa liittyä työnantajan toiminnan tahalliseen vahingoittamiseen. Tuhoaminen voi perustua myös haluun hävittää itselle epäedullinen tiedosto työnantajalta tai muulta taholta, kuten viranomaisilta. Työntekijän valvominen ja tiedostojen tuhoamisen estäminen on vaikeaa, koska työntekijällä on oltava pääsy työnsä kannalta tarpeellisiin tiedostoihin. Siksi tuhoamistilanteessa avainasemaan nousee varmuuskopiointi. Mikäli yritys on hoitanut varmuuskopiointin säännöllisesti ja kopiot on sijoitettu turvalliseen paikkaan, on tällaisesta teosta aiheutunut vahinko pieni. Toinen huomioitava seikka näissä tilanteissa on käyttäjäoikeuksien laajuus.

Tuhoamisen voi tehdä myös ulkopuolinen taho tietojärjestelmään tunkeutumalla tai käyttäen välikätenä työntekijää. Varmuuskopiointin lisäksi näissä tilanteissa huomionarvoiseksi seikoiksi nousevat palomuurit ja virustentorjunta sekä näiden jatkuva päivittäminen.

Vastaajista 6 prosenttia ilmoitti, että yrityksen tiedostoja on tuhottu. Vastaajayrityksistä valtaosa, noin neljä viidestä (83%) vastasi, ettei tiedostoja ole tuhottu. Epätietoisia vastauksia oli 11 prosenttia. Suurimpien vastaajayritysten osalta joka neljäs (24 %) vastasi, ettei osaa sanoa.

Kaupan alalla (13%) tiedostojen tuhoaminen oli yleisintä, sillä tuhoamista tapahtui yli kolme kertaa useammin kuin teollisuudessa (4%).

### **Yritystiedon luvaton muuttaminen tai väärentäminen**

Yritystiedon luvaton muuttaminen on usein vaikeammin havaittavissa kuin tiedostojen tuhoaminen. Monisivuisen dokumentin häviäminen on helpommin havaittavissa kuin siinä olleiden tietojen muuttaminen tai väärentäminen.

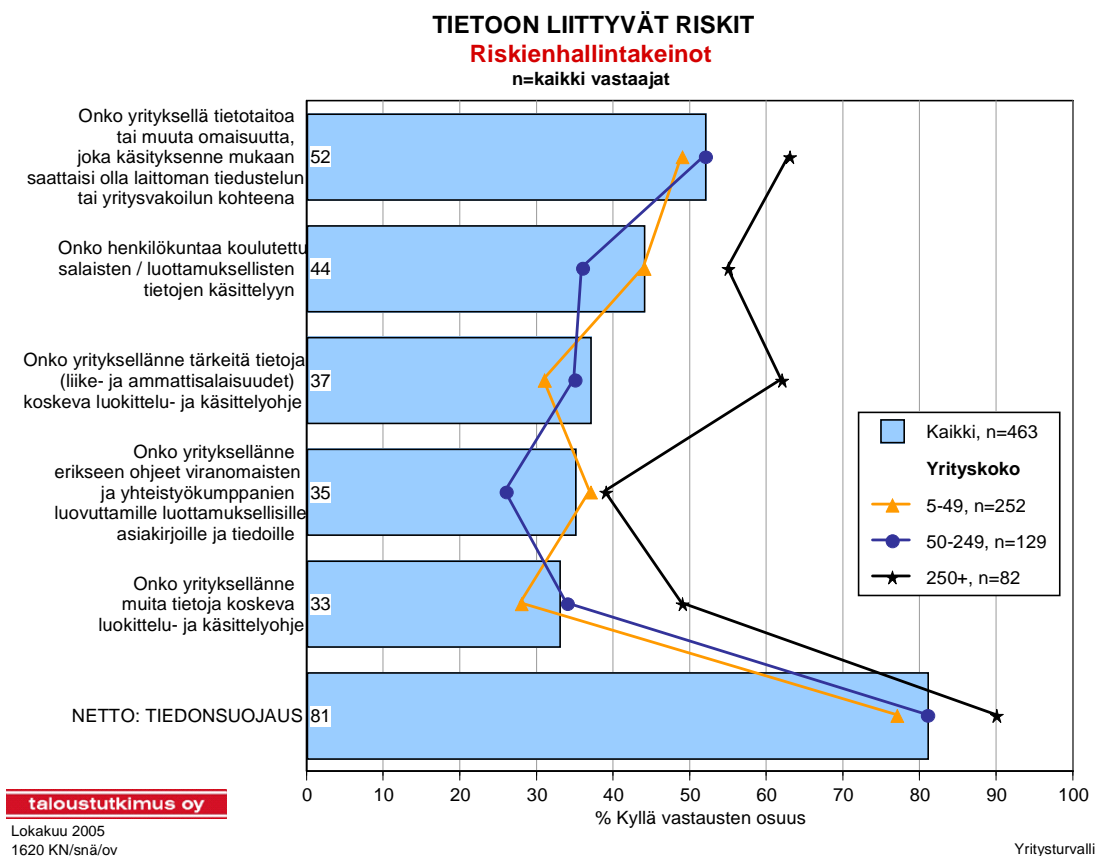
Kaikista vastaajayrityksistä vain 3 prosenttia oli havainnut yritystietojen sisällön muuttamista tai väärentämistä. Noin neljä viidestä vastaajayrityksestä (84%) ilmoitti, ettei näin ole tapahtunut. "Ei osaa sanoa" -vastausten osuus oli 14 prosenttia. Suurimpien

vastaajayritysten osalta joka neljäs (26%) ilmoitti, ettei osannut sanoa onko näin tapahtunut. Asiaan voi osin vaikuttaa tietomäärien suuruus, jolloin tiedoston muutettu tai väärennetty tieto ei tule niin helposti esille kuin pienemmissä yrityksissä, joilla on vähemmän tietoa järjestelmissään.

### Netto: Toteutuneet tietoriskit ja uhat

Tietoturvaa on loukattu (55%) vastaajayrityksistä. Suurista vastaajayrityksistä useampi kuin kuusi kymmenestä (61%) totesi, että tietoon kohdistunut riski tai uhka oli toteutunut. Hallussaan olevan tiedon osalta yritykset ovat hyvin samassa asemassa koosta tai toimialasta riippumatta. Kaikilla yrityksillä on omaan toimintaansa liittyvää suojattavaa omaa tai asiakkaan tietoa, jota ei saa antaa ulkopuolisille. Epäonnistuminen tiedon suojaamisessa saattaa johtaa kilpailuaseman menetykseen tiedon päätyessä kilpailijan hyödynnettäväksi tai asiakkaan vaihtaessa palvelun- tai tavarantoimittajaa tiedon vuotamisen seurauksena. Tietovuoto saattaa myös johtaa maineen menetykseen ja siten välillisesti kilpailuaseman menetykseen asiakkaiden tai mahdollisten asiakkaiden välttäessä epäluotettavaa toimijaa.

## 4.2 Riskienhallintakeinot: Miten yritykset varautuvat tiedon väärinkäyttöihin?



### **Yrityksen tietotaito tai muu omaisuus laittoman tiedustelun tai yritysvakoilun kohteena**

*"Sisällä olevien ihmisten sinisilmäisyys ja `eihän meillä mitään tärkeää ole´-asenne ongelmana."*

Laillisuuden rajat ylittävää tiedonhankintaa tekevät sekä yritykset että eri maiden tiedustelupalvelut, joiden tavoitteena on tukea oman maan yrityksiä. Yritysvakoilun merkitystä ja täyttä mittakaavaa on vaikea arvioida, koska rikoksen uhri ei välttämättä huomaa tapahtunutta. Kielteisen julkisuuden pelossa moni yritys ei halua kertoa havaitsemistaan vakoilutapauksista. Vakoilun kohteeksi voivat joutua hyvin monenlaiset yritykset. Koolla ei ole juuri merkitystä, hyvinkin pieni yritys voi tuottaa mielenkiintoista tietotaitoa. Mielenkiinnon kohteena voi olla yhtä hyvin jo patentointiprosessissa oleva huipputuote kuin joku perustutkimuksen tuottama tulos.

Vastaaajayrityksistä joka toisella (52 %), on hallussaan laittoman tiedustelun tai yritysvakoilun kohteeksi mahdollisesti valikoituvaa tietotaitoa tai omaisuutta. Suurimpien vastaaajayritysten joukosta lähes kaksi kolmesta (63 %), pienistä lähes joka toinen (49 %) ja joka toinen keskisuurista (52 %) oli tätä mieltä.

Yleisintä laittoman tiedustelun tai yritysvakoilun kohteena olevan tietotaidon tai omaisuuden hallussapito oli palvelualalla (59 %).

### **Henkilökunnan koulutus salaisten tai luottamuksellisten tietojen käsittelyyn**

*"Tietoturvallisuuteen liittyvä ohjeistus ja käyttöoikeudet ovat hieman vaillinaisia ja ohjeistus puuttuu."*

Työnantajan on koulutettava työntekijänsä, jotta he tietäisivät, onko tieto julkista vai salaista. Muussa tapauksessa voi tekijän saaminen rikosvastuuseen olla vaikeaa tai mahdotonta. Työnantajan on osoitettava tärkeimmät käytännön toimenpiteet tiedon suojaamiseksi. Muita ovat esimerkiksi ohjeiden laatiminen tiedon käsittelystä, merkitsemisestä, säilyttämisestä, jakelusta ja hävittämisestä.

Vastaaajayrityksistä joka toinen (53 %) ei ole kouluttanut henkilökuntaansa salaisten tai luottamuksellisten tietojen käsittelyyn. Yli puolet (55 %) suurimpien vastaaajayritysten ryhmään kuuluvasta on kouluttanut henkilökuntaansa, kun taas pienimpien vastaaajayritysten joukossa alle puolet (44 %) on kouluttanut henkilökuntaansa.

Palvelualalla (54 %) kouluttaminen oli yleisintä. Vähiten koulutusta oli annettu teollisuudessa (35 %).

Vuonna 2004 Uudellamaalla tehdyssä kyselyssä alle puolet vastaajista oli kouluttanut henkilökuntaansa salaisten tai luottamuksellisten tietojen käsittelyyn. Vuoden 2005 saman alueen vastausten mukaan alle puolet (48 %) on kouluttanut henkilökuntaansa. Huomattavasti useamman yrityksen pitäisi kouluttaa henkilökuntaansa täyttääkseen yrityssalaisuuksien rikosoikeudellisen suojan edellyttämän käytännön toimenpiteiden vaatimuksen.

### **Yrityksen liike- ja ammattisalaisuuksia koskeva luokittelu- ja käsittelyohje**

Työnantajan olisi aiheellista laatia vähintään liike- ja ammattisalaisuuksien käsittelyä koskeva ohje. Työnantajan on määriteltävä liike- ja ammattisalaisuutensa. Työntekijät on koulutettava toimimaan ohjeen mukaisesti ja sen on oltava työntekijöiden saatavilla.

Vastaaajayrityksistä hieman yli kolmasosa (37 %) oli laatinut ohjeen liike- ja ammattisalaisuuksien käsittelystä. Suurimpien vastaaajayritysten joukosta lähes kaksi

kolmesta (62 %) on laatinut ohjeen. Pienimmistä vain hieman alle kolmannes (31 %) ja keskiuurista hieman yli kolmannes (35 %) ovat laatineet ohjeen.

Pienistä yrityksistä 49 prosenttia vastasi, että niillä on tietoa tai omaisuutta, joka voisi olla laittoman tiedustelun tai yritysvakoilun kohteena. Kuitenkin vain 31 prosentissa saman ryhmän vastaajayrityksistä oli laadittu ohje liike- ja ammattisalaisuuksien käsittelystä. Siten ainakin 37 prosenttia niistä vastaajayrityksistä jotka olivat tietoisia riskistä, eivät olleet laatineet ohjetta. Keskiuurista vastaajayrityksistä 52 prosenttia oli tietoisia riskistä ja vain 35 prosenttia oli tehnyt ohjetta. Riskin tiedostaneista siis ainakin 33 prosentilla ei ollut ohjetta. Suurimpien vastaajayritysten ryhmässä oli 63 prosenttia tietoisia riskistä ja 62 prosenttia oli laatinut ohjeen.

Kaksi viidesosaa muun palvelualan yrityksistä (44 %) on laatinut liike- ja ammattisalaisuuksia koskevan ohjeen, kun taas rakennusosalalla vain joka neljännellä (24 %) yrityksellä on sellainen.

Kun otetaan huomioon, että käytännössä lähes jokaisella yrityksellä on jotain tietoa, joka on sen liiketoiminnan kannalta olennaista ja salassa pidettävää, tilannetta voidaan pitää huolestuttavana. Yritykset ovat laiminlyöneet omien yrityssalaisuuksien määrittelyn ja luokittelun sekä koulutuksen.

### **Yrityksen muita tietoja koskeva luokittelu- ja käsittelyohje**

Liike- ja ammattisalaisuuksien käsittelyä koskevan ohjeen lisäksi työnantajan kannattaisi tehdä myös muita tietoja, kuten yrityksen sisäisiä ja julkisia tietoja koskeva käsittelyohje. Muuten tilanne saattaa jäädä epäselväksi, kun yrityksessä on sekä luokiteltua tietoa että luokittelematonta tietoa. Tällainen tilanne luo epätietoisuutta ja saattaa aiheuttaa virheitä tiedon käsittelyssä.

Kaikista vastaajista kolmasosalla (33 %) oli muita tietoja koskeva luokittelu- ja käsittelyohje. Lähes kaksi viidesosaa palvelualan yrityksistä (40 %) on laatinut muita tietoja koskevan ohjeen, kun taas rakennusosalalla vain joka viidennellä (21 %) yrityksellä on sellainen.

### **Yrityksen ohjeet viranomaisten ja yhteistyökumppanien luovuttamille luottamuksellisille asiakirjoille ja tiedoille**

Yritys voi myös saada haltuunsa muiden tahojen luottamuksellista tietoa. Tieto voi olla toisten yritysten tai viranomaisten tietoa. Tieto voi liittyä yritysalaisuuksiin tai yhteiskunnan kannalta tärkeisiin seikkoihin. Tiedon käsittelytavat on hyvä sopia, jotta välttyttäisiin ikäviltä yllätyksiltä. Ohjeet voidaan sisällyttää yrityksen omiin yleisiin ohjeisiin tai sitten niistä voidaan laatia omat erilliset ohjeet vain niille, jotka käsittelevät kyseistä tietoa. Nämä ohjeet laaditaan usein yhdessä tietojen luovuttavan tahon kanssa.

Jokaisen yrityksen pitäisi myös harkita, mitä tietoa se antaa yhteistyökumppaneille ja viranomaisille. Yrityksen on hyvä merkitä tiedon luokitus ja antaa selkeä ohje vastaanottajalle tiedonkäsittelystä

Vastaajayrityksistä yli kolmanneksella (35 %) oli erikseen ohjeet viranomaisten ja yhteistyökumppanien luovuttamille luottamuksellisille asiakirjoille ja tiedoille. Ohjeiden olemassaolo jakaantui: Pienimmillä vastaajayrityksillä luku oli 37 prosenttia, keskiuurilla 26 prosenttia ja suurimmilla 39 prosenttia.

Läheskään kaikilla yrityksillä ei ole toisten tahojen tietoa hallussaan. Siksi lukuja ei lähtökohtaisesti ole pidettävä huolestuttavana.

**Netto: Toteutuneet tietoriskit ja uhat**

Viidesosalla (19%) yrityksistä ei ole mitään kyselyssä käsiteltyjä riskienhallintakeinoja käytössään. Huonoin tilanne on pienimpien vastaajayritysten keskuudessa. Niistä neljäsosa (23%) ei käytä mitään näistä riskienhallintakeinoista.

**Tarkistuslista 2: Tietoon liittyviin rikosriskeihin ja väärinkäytöksiin varautuminen**

- Tietoja koskeva luokittelu- ja käsittelyohje
- Tiedon tekniset suojauskeinot
- Henkilökunnan koulutus salaisten / luottamuksellisten tietojen käsittelyyn
- Liike- ja ammattisalaisuuksia koskeva luokittelu- ja käsittelyohje
- Ohjeet viranomaisten ja yhteistyökumppanien luovuttamille luottamuksellisille asiakirjoille ja tiedoille
- Varautuminen siihen, että yritys voi olla yritysvakoilun kohteena

**Tietoturvan suppea huoneentaulu (Tietoyhteiskunnan kehittämiskeskus TIEKE)**

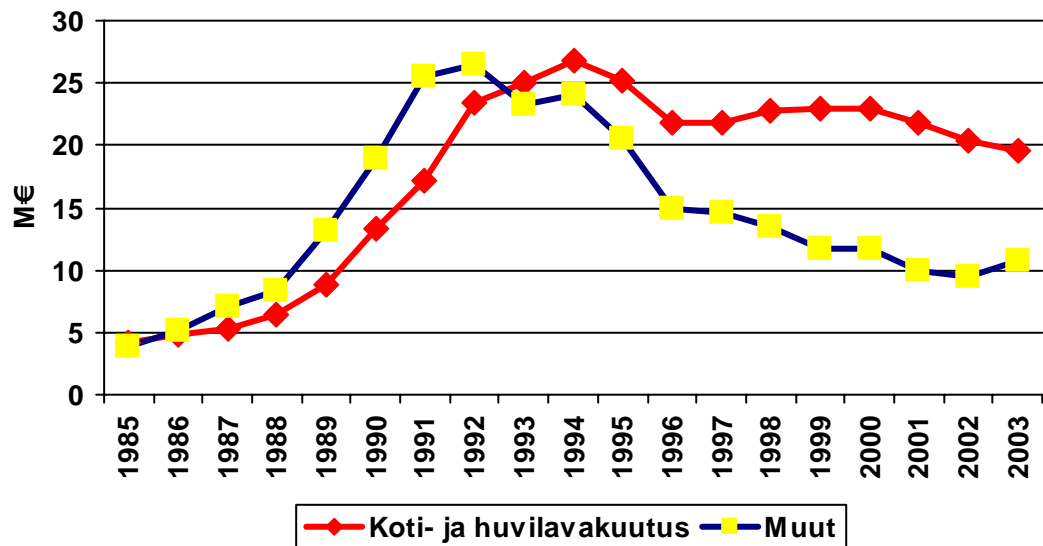
- Selvitä tiedon ja tiedoston alkuperä ennen käyttöä
- Muista, että seinillä on korvat - useammat kuin arvaatkaan
- Lukitse ovesi ja tietokoneesi, kun lähdet muualle
- Käytä salasanoja, joissa on muitakin merkkejä kuin kirjaimia, ja pidä ne salassa
- Ota talteen kaikki tarpeellinen, ennen kuin vahinko sattuu
- Käytä ajantasaisia viruksentorjuntaohjelmia ja muita turvajärjestelyjä
- Selvitä itsellesi oman organisaatiosi tietoturvajärjestelyt

## YRITYSTEN RIKOSTURVALLISUUS 2005

## 5 OMAISUUTEEN KOHDISTUVAT RIKOKSET JA VÄÄRINKÄYTÖKSET

Omaisuusrikokset ovat Vakuutusyhtiöiden keskusliiton mukaan vähentyneet vuosien 2000 ja 2004 välisenä aikana 14,5 prosenttia. Liikemurrot ovat vähentyneet noin puoleen. Vakuutusyhtiöiden maksamat murto- ja varkausvahingot ovat vähentyneet samassa ajassa vain noin viidesosan. Rikoksista aiheutuneet rahalliset vahingot ovat kuitenkin kasvaneet. Poliisi selvitti vuonna 2004 kaikista omaisuusrikoksista ja varkausrikoksista kolmanneksen.

Murto- ja varkausvahingot (Vakes)



Riski joutua omaisuusrikoksen kohteeksi on kaikilla yrityksillä. Yrityksillä on usein oman omaisuutensa lisäksi hallussaan jonkun toisen, esimerkiksi asiakkaan omaisuutta. Omaisuusrikoksen kohdistuessa asiakkaan omaisuuteen, vakuutus ei aina korvaa hallussa pidettyä tai valvonnassa ollutta toisen tahon omaisuutta. Tämä saattaa koskea myös työntekijöiden työpaikalla säilyttämää omaisuutta.

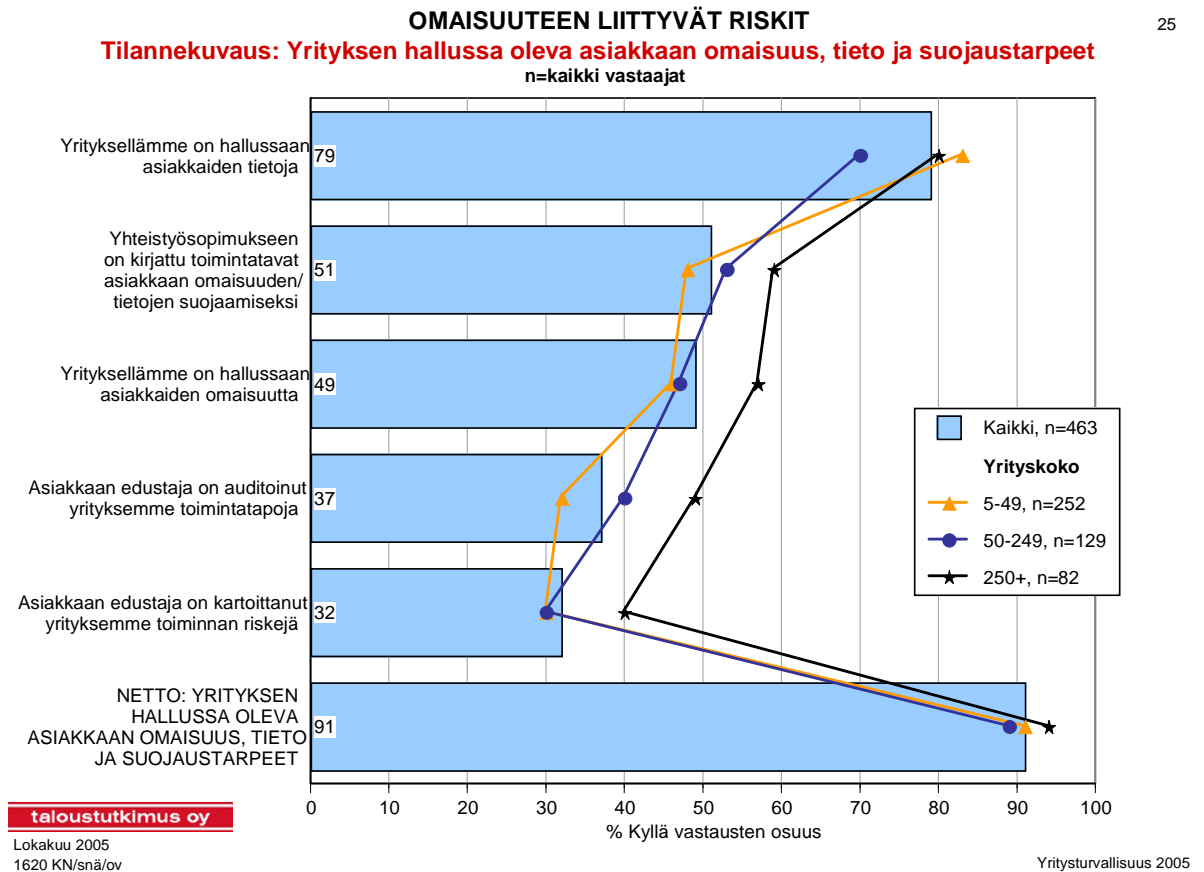
Varautumalla toimitiloihin tai irtaimeen kohdistuvaan rikollisuuteen yritys parantaa myös muiden yritysturvallisuuden osa-alueiden tasoa. Rikosturvallisuuden lisäksi ainakin tietoturvallisuuden, kiinteistö- ja toimitilaturvallisuuden, työturvallisuuden,

henkilöturvallisuuden, tuotannon ja toiminnan turvallisuuden sekä pelastustoiminnan taso usein nousee.

Henkilökunnan on tiedettävä, miten järjestelmiä käytetään. Hyvin suunnitellun ja toteutetun järjestelmän tehokkuus heikkenee, jos henkilökunta ei osaa käyttää järjestelmää, käyttää sitä väärin tai kytkee sen pois, koska kokevat siitä olevan haittaa.

Kuten kaikessa yritysturvallisuustyössä on myös omaisuuden suojaamisessa tärkeää tehdä riskikartoitus ja suunnitella suojaamistoimenpiteet. Näin voidaan voimavarat käyttää tehokkaimmalla tavalla. Hyvin tehty ja ajan tasalla pidetty kartoitus ohjaa riskienhallintatyötä tehokkaasti.

## 5.1 Yrityksen hallussa oleva asiakkaan omaisuus, tieto ja suojaustarpeet



### **Yrityksellä on hallussaan asiakkaiden tietoja**

*”Henkilöllä jää tietokone auki, salasana on näkyvillä, salasanoja ei vaihdeta, annetaan kolmannelle liian helpoisesti. Ei ymmärretä salassapitosopimusten sisältöä. Yleensä puutteet tai tilanteet kohdistuvat tiedon saamiseen/jakamiseen/käyttämiseen/tallentamiseen, ei fyysiseen henkilöriskiin.”*

Neljä yritystä viidestä (79 %) ilmoitti, että niiden hallussa on asiakkaiden tietoja. Eroja ei juuri ollut pienimpien (83 %) ja suurimpien (80 %) vastaajayritysten välillä. Keskisuurten vastaajayritysten keskuudessa osuus oli 70 prosenttia. Tietojen hallussapito on hyvin yleistä ja yritysten tulisi tiedostaa tietojen suojaamisen tärkeys. Riskinä suojaamisen laiminlyönnistä voi seurata asiakasmenetyksiä.

Palvelualalla valtaosalla (91 %) yrityksistä oli hallussaan asiakkaan tietoja. Rakennusalalla asiakkaan tietoja oli hallussa kahdella kolmasosalla (67 %) yrityksistä.

### **Yrityksellä on hallussaan asiakkaiden omaisuutta**

Asiakkaiden omaisuutta hallussaan pitävien osuus kaikista vastaajayrityksistä oli lähes puolet (49 %). Pienten (46 %) ja keskisuurten (47 %) yritysten välillä ei juuri ollut eroja. Suurissa yrityksissä asiakkaan omaisuuden hallussapito oli hieman keskimääräistä yleisempää (57 %).

Teollisuudessa yli puolella (55 %) vastaajista oli asiakkaan omaisuutta hallussaan. Rakennusalalla vastaava luku oli 27 prosenttia.

### **Yhteistyösopimukseen on kirjattu toimintatavat asiakkaan omaisuuden tai tietojen suojaamiseksi**

Sekä luovuttavan että vastaanottavan yrityksen pitäisi kirjata toimintatavat omaisuuden tai tietojen suojaamisesta yhteistyösopimukseen. Menettelytapoja kirjattaessa on turvallisuustasona pidettävä sitä, miten luovuttava yritys itse omaisuutta tai tietoa suojaa. Riskienhallinnan kannalta on tärkeää vaatia vastaanottajalta vähintään saman tason menettelyä. Vastaanottajan kannalta on otettava huomioon se haitta, joka asiakkaiden tietojen tai omaisuuden joutumisesta väärin käsiin voi vastaanottajan liiketoiminnalle seurata.

Kaikista vastaajayrityksistä hieman yli puolella (51 %) oli sopimukseen kirjattu toimintatavat. Tilanne vastaajien kesken jakaantui seuraavasti: pienet (48 %), keskisuuret (53 %) ja suuret (59%). Palvelualan yrityksistä lähes 61 prosenttia oli kirjannut toimintatavat, kun taas harvinaisinta se oli kaupan alalla (28 %).

### **Asiakkaan edustaja on auditoinut yrityksen toimintatapoja**

Auditointi on ainoa tapa varmistaa, säilyttääkö toinen osapuoli tietoja tai muuta omaisuutta niin kuin on sovittu. Päästäessään ulkopuolisen tahon auditoimaan toimintaansa, yrityksen on hyvä pitää mielessä, mitä kaikkea antaa nähtäväksi. Esimerkiksi asiakkaiden tiedot eivät saisi tulla auditoijan tietoon.

Asiakkaat olivat auditoineet neljää yritystä kymmenestä (37%). Suurimmista vastaajayrityksistä joka toinen (49%) ja pienimmistä joka kolmatta (32%) on auditoitu. Keskisuurista yrityksistä 40 prosenttia oli auditoitu.

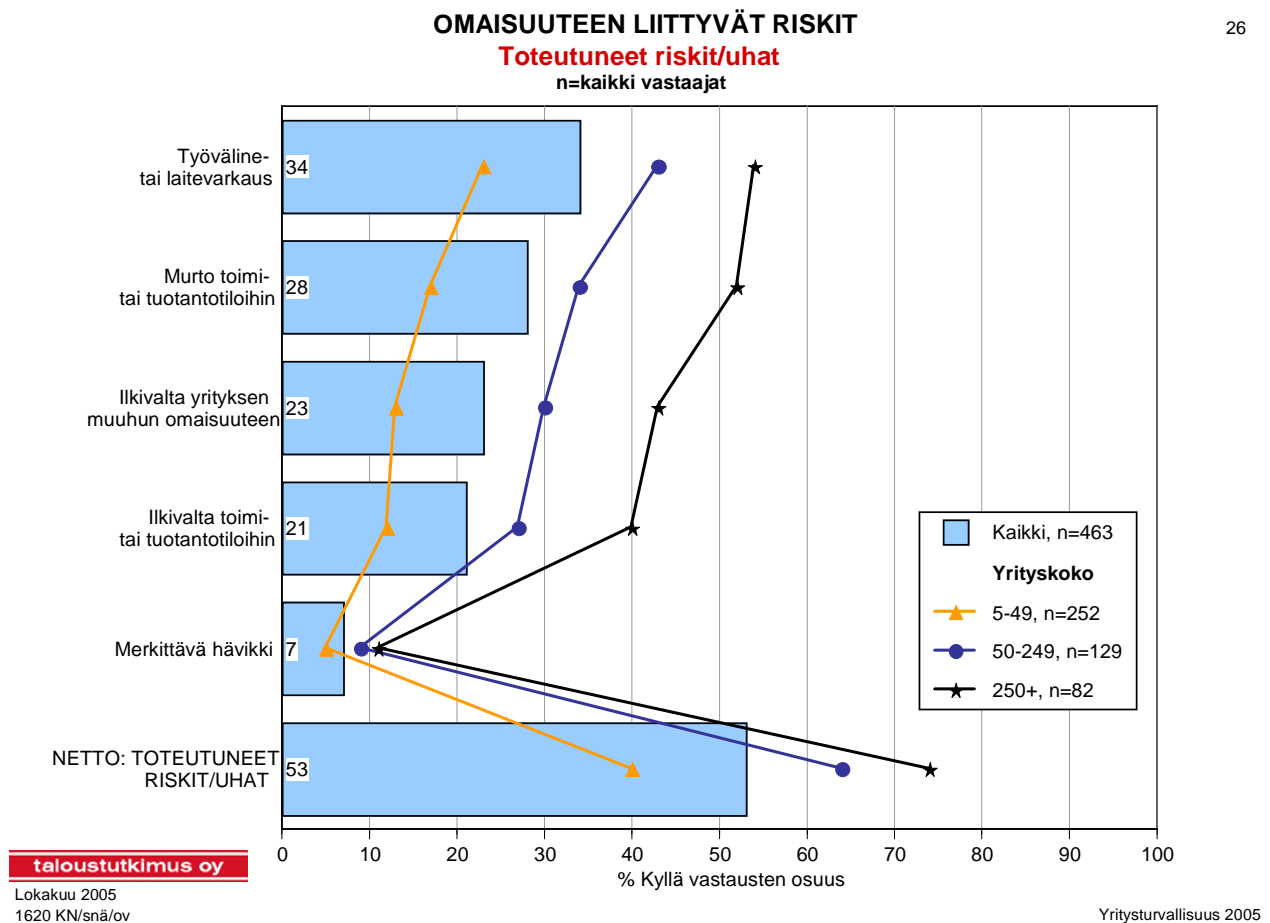
Yleisintä auditointi oli teollisuudessa (55%) ja harvinaisinta kaupanalalla (17%).

### Asiakkaan edustaja on auditoinut yrityksen toiminnan riskejä

Toinen tärkeä auditoitava osa-alue on toisen osapuolen toimintaan liittyvien riskien arviointi. On hyvä selvittää toisen osapuolen toimintaan liittyvät riskit ja arvioida, aiheutuuko niistä omaan toimintaan uusia riskejä tai kasvaako joku oman toiminnan riskeistä niiden takia.

Vastaajayrityksistä noin kolmasosaa (32%) asiakkaat olivat auditoineet toiminnan riskeistä. Suurimmissa yrityksissä (40%) tämä oli yleisintä. Pienten ja keskiuurten vastaajien kesken ei ollut eroa, niistä hieman alle kolmasosaa (30%) oli auditoitu. Teollisuudessa riskien kartoitus oli yleisintä (45%) ja harvinaisinta kaupan alalla (13%).

## 5.2 Toteutuneet riskit ja uhat



### Työväline- tai laitevarkaus

*"Ohjeistuksesta huolimatta henkilö oli jättänyt ruokatunnille lähtiessään huoneensa oven auki, varas käytti tilannetta hyväkseen, lymyi porraskäytävässä ja pujahti sisään henkilöstön lähtiessä syömään. Varas vei kannettavan tietokoneen."*

Kaikista vastaajayrityksistä joka kolmannelta (34 %) on varastettu työvälineitä- tai laitteita. Suurimmista vastaajayrityksistä joka toiselta (54 %), keskiuurista kahdelta viidestä (43 %) ja pienimmistä joka viidenneltä (23 %) on varastettu laitteita. Rakennusalan yrityksistä lähes

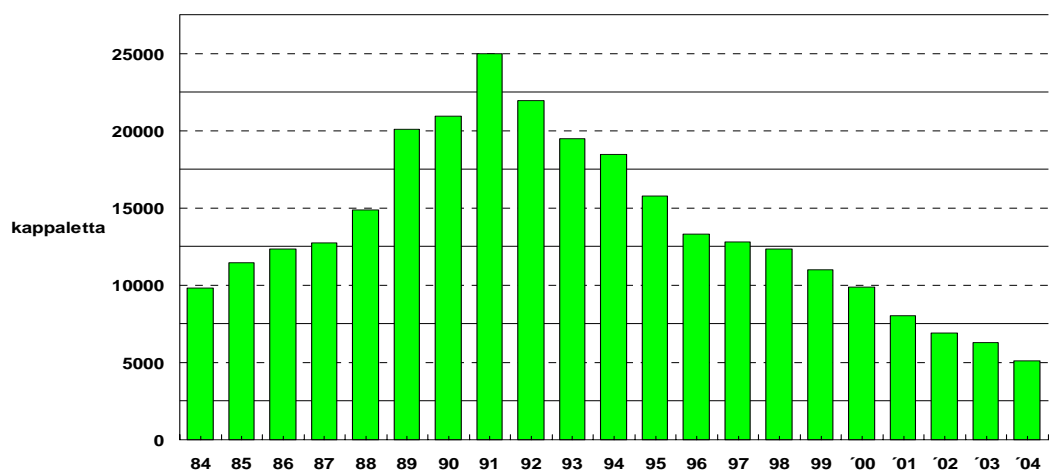
neljä viidestä (79 %) on valikoitunut kohteeksi. Syynä tähän ovat todennäköisesti työmaat, joita on vaikea valvoa.

Työväline- tai laitevarkaudet ovat yleisimpiä rakennusalalla (79 %) ja vähäisimpiä teollisuudessa (25 %).

### Murto toimi- tai tuotantotiloihin

*"Viikonlopun aikana murtauduttiin ajamalla trukilla peltioven lävitse tuotantotiloihin ja sieltä varastoon ja varastettiin kuorma-autollinen nikkeliä."*

### POLIISIN TIETOON TULLEET LIIKEMURROT



Lähde: Tilastokeskus  
02/2004 AP

Keskuskauppakamarin ja Helsingin seudun kauppakamarin kyselyyn vastanneista yrityksistä useampi kuin joka neljäs (28 %) oli joutunut murron kohteeksi. Joka toiseen (52 %) suureen yritykseen oli murtauduttu. Keskisuurista kolmasosaan (34 %) on murtauduttu. Pienissä yrityksissä osuus on 17 prosenttia. Rakennusalan yrityksistä lähes kolme viidestä (58 %) on joutunut murron kohteeksi.

Murrot toimi- tai tuotantotiloihin ovat yleisimpiä rakennusalalla (58 %) ja harvinaisimpia teollisuudessa (21 %).

Vuonna 2004 Uudenmaan läänin alueella alle kolmasosa (32 %) vastaajista oli joutunut murron kohteeksi. Vuoden 2005 saman alueen vastausten mukaan hieman useampi kuin joka kolmas (34 %) oli joutunut murron kohteeksi.

### Toimi- tai tuotantotiloihin kohdistuva ilkivalta

Joka viides (21 %) vastaajayritys on joutunut toimi- tai tuotantotiloihin kohdistuvan ilkivallan kohteeksi. Suurimpien vastaajayritysten ryhmästä kaksi viidestä (40 %) on kohdannut ilkivaltaa. Keskisuurista yrityksistä hieman alle kolmasosa ja pienistä vain noin joka kymmenes on joutunut ilkivallan kohteeksi.

Ilkivalta toimi- tai tuotantotiloihin on yleisintä rakennusalalla (33 %) ja harvinaisinta teollisuudessa (16 %).

Vuonna 2004 Uudenmaan läänin alueella hieman alle viidesosa vastaajayrityksistä oli joutunut ilkivallan kohteeksi. Vuoden 2005 saman alueen vastausten mukaan ilkivallassa oli

tapahtunut huomattavaa kasvua. Useampi kuin joka neljäs yritys (27 %) oli joutunut ilkivallan kohteeksi.

### Yrityksen muuhun omaisuuteen kohdistuva ilkivalta

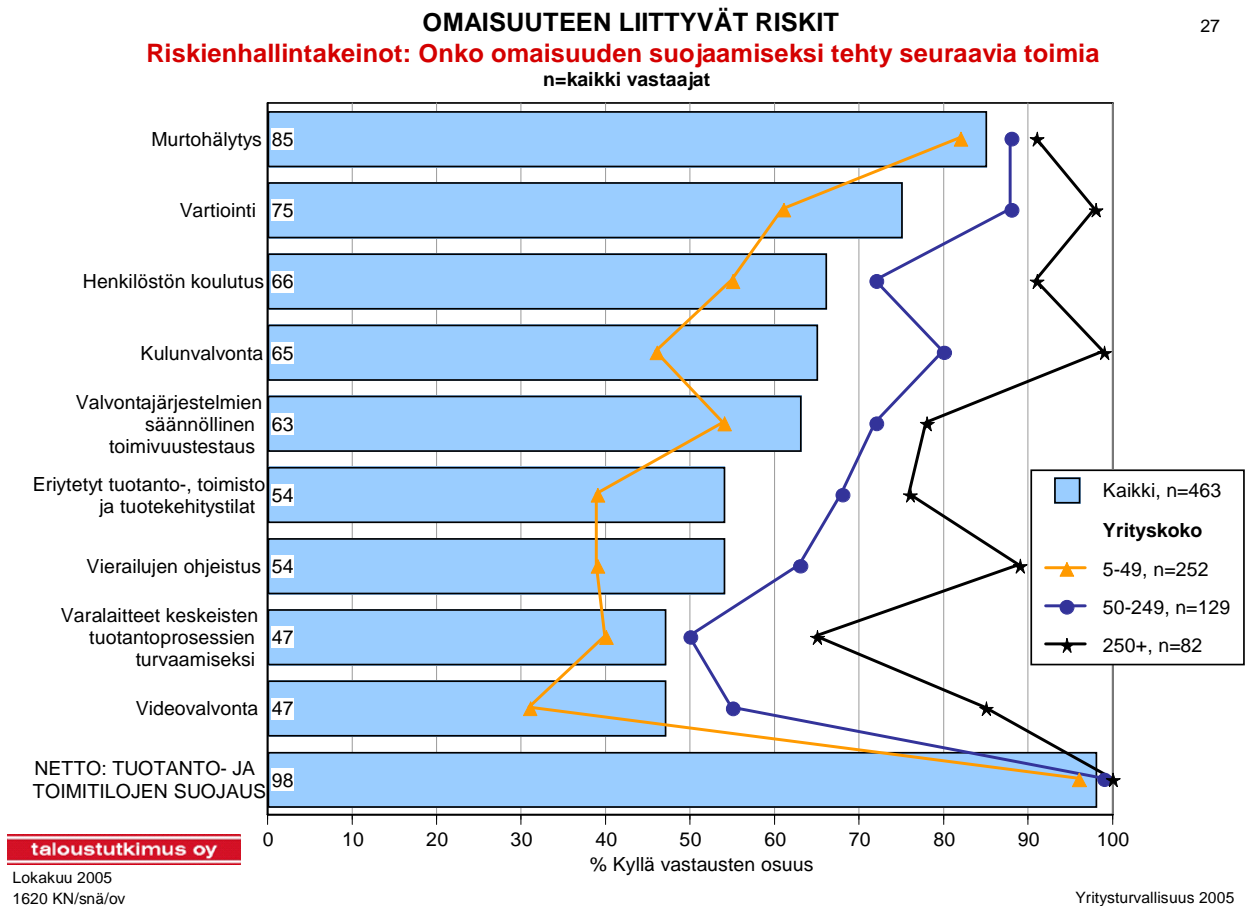
Joka neljännen (23 %) vastaajayrityksen muuhun omaisuuteen on kohdistunut ilkivaltaa. Suurista vastaajayrityksistä kaksi viidestä (43 %), keskisuurista lähes kolmasosa (30 %) ja pienistä joka kahdeksas on kohdannut ilmiön.

Ilkivalta yrityksen muuhun omaisuuteen on yleisintä rakennusalalla (39 %) ja harvinaisinta teollisuudessa (15 %).

### Netto: Toteutuneet uhat

Kaikista vastaajista yli puolet (53 %) on kohdannut jonkun selvityksen tässä luvussa käsitellyn riskin.

## 5.3 Riskienhallintakeinot: Onko omaisuuden suojaamiseksi tehty seuraavia toimia?



## Murtohälytys

*"Murto ikkunasta, tuplalukitus esti oven kautta viemästä laitteita."*

*"Liiketilat tuhoutuivat tulipalossa puutteellisten hälytysjärjestelmien vuoksi - alihankkijan tuotantolaitos tuhoutui tulipalossa."*

Rikosilmoitinjärjestelmän tarkoituksena on antaa ilmoitus, kun joku liikkuu kohteessa järjestelmän ollessa kytkettynä päälle. Sen käyttö ehkäisee rikoksia, mutta järjestelmästä on hyötyä myös vahinkojen rajaamisessa. Tämä on mahdollista erityisesti silloin, kun järjestelmään on kytketty palo- tai kosteusilmaisimia. Paloista ja vesivahingoista aiheutuneet vahingot ovat rahallisesti kaikkein suurimmat vakuutuskorvauksien aiheuttajat, kun otetaan huomioon murroista välillisesti aiheutuneet vahingot. Rikosilmoitinjärjestelmän käytön kannalta on tärkeää testata järjestelmän toiminta säännöllisesti ja varmistaa sen huolto.

Kaikista vastaajayrityksistä enemmistö (85 %) suojaa tilojaan rikosilmoitinjärjestelmällä. Suurimpien vastaajayritysten ryhmässä rikosilmoitinjärjestelmän käyttö on yleisintä (91 %). Keskisuurista yrityksistä 88 prosenttia ja pienistä yrityksistä 82 prosenttia on hankkinut rikosilmoitinjärjestelmän.

Rikosilmoitinjärjestelmien käyttö on yleisintä kaupan alan yrityksissä (94%) ja harvinaisinta se on rakennusalalla (64 %).

Rikosilmoitinjärjestelmä ei yksinään riitä suojaustoimenpiteeksi. Lisäksi pitäisi huomioida rakenteellinen suojaus (ovet, lukitukset, ikkunakaltrit jne.) ja muut sähköiset valvontajärjestelmät (videovalvonta ja kulunohjaus).

## Vartiointi

Kysymyksessä ei ole eritelty minkälaisesta vartioinnista on kysymys. Eri vartiointimuotoja ovat muun muassa paikallis-, piiri-, myymälä- ja aulavartiointi. Yleisin yritysten käyttämä vartiointimuoto on hälytyskeskuspalvelu, jossa rikosilmoitinjärjestelmän hälyttäessä vartija menee kohteeseen selvittämään tilanteen.

Kolme neljästä (75 %) kaikista vastaajayrityksistä käyttää vartiointia keinona torjua omaisuuteen kohdistuvia riskejä. Lähes kaikki suurimmat yritykset (98 %) käyttivät vartiointia. Pienimmistä yrityksistä alle kaksi kolmasosaa (61 %) käytti vartiointia.

## Kulunvalvonta

*"Tiloihin pääsi henkilöstömme "kohteliaisuuden" takia sinne kuulumattomia henkilöitä. Tähän on nyt kiinnitetty huomiota."*

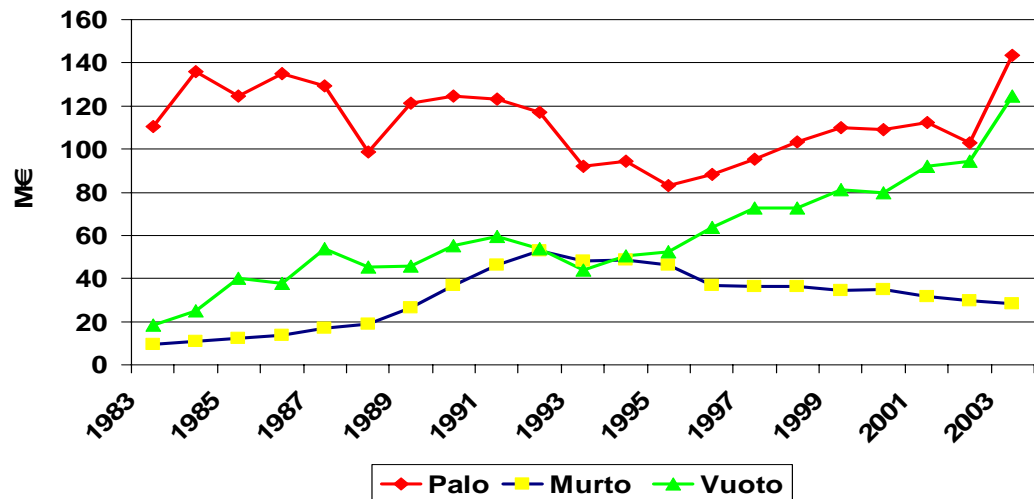
*"Toimitilojen kulunvalvonta ei ole riittävää. Pääovesta sisään tullessa pitää olla koodi, mutta ei autotallin kautta tullessa. Tämä on selvä riski iltaisin ja viikonloppuisi.n"*

Kulunvalvonta estää luvatonta liikkumista silloin, kun rikosilmoitinjärjestelmä on poissa päältä. Kulunvalvonta parantaa turvallisuuden tasoa toimistoaikana, kun tiloissa on eniten kulkijoita.

Kaksi kolmasosaa (65%) yrityksistä käyttää kulunvalvontaa. Suurista yrityksistä lähes kaikki (99%), keskisuurista neljä viidestä (80%) ja pienistä yrityksistä lähes puolet (46%) käyttää kulunvalvontaa.

## Varalaitteet keskeisten tuotantoprosessien turvaamiseksi

**Palo-, murto- ja vuotovahingot 1983-2003**  
Korvausmäärät muutettu 2003 rahan arvoa vastaaviksi



HUOM! 2003 luvuissa mukana myös vakuutusyhdistykset

Riskitilanteissa varalaitteet helpottavat yrityksen mahdollisuuksia jatkaa liiketoimintaansa keskeytyksellä tai mahdollisimman lyhyellä keskeytyksellä. Varalaitteiden olemassaolo ja käytettävyys vaikuttavat yrityksen päivittäiseen toimintaan ja liikevaihtoon.

Lähes puolella kaikista vastaajayrityksistä (47 %) on käytössään varalaitteita. Suurissa yrityksissä lähes kahdella kolmasosalla (65 %) on varalaitteita. Puolet keskisuurista (50 %) ja kaksi viidestä (40 %) pienestä yrityksestä on hankkinut varalaitteita.

Varalaitteet ovat yleisimpiä teollisuudessa (51 %) ja harvinaisimpia kaupan alalla (30 %).

### Videovalvonta

*"Videovalvontakameroita on liian vähän, koska varkaat ovat osanneet valita paikkoja, joihin kamera ei kuvaa."*

*"Tuotantotiloihin tultiin aidan läpi. Valot olivat liian heikkoja valvonnalle pimeään aikaan."*

Videovalvonta ehkäisee omaisuusriskien toteutumista, mutta siitä on myös hyötyä tapahtumien selvittämisessä. Videovalvonnan toimivuuteen vaikuttavat valaistus, kameroiden ominaisuudet, järjestelmän suunnittelu ja toteutus sekä kameroiden säätö.

Lähes puolet (47 %) kaikista vastaajayrityksistä käyttää videovalvontaa. Suurten vastaajayritysten (85 %) keskuudessa sen käyttö on yleisintä. Keskisuurista (55 %) videovalvontaa käyttää hieman yli puolet. Pienimmistä vain joka kolmas (31%) käyttää sitä.

Videovalvonta on yleisintä muiden palveluiden alalla (52 %) ja harvinaisinta rakennusalalla (39 %).

### **Valvontajärjestelmien säännöllinen toimivuustestaus**

*"Puhelinkeskuksen ja numeroiden vaihto. Hälytykset lakkasivat toimimasta."*

*"Hälytysjärjestelmä on ollut välillä epäkunnossa."*

Valvontajärjestelmien toimintakyky voi heikentyä ajan kuluessa. Siksi yritysten tulisi säännöllisesti varmistaa järjestelmien toimivuus.

Kaikista vastaajayrityksistä lähes kaksi kolmasosaa (63%) testaa säännöllisesti valvontajärjestelmien toimivuuden. Enemmistö suurista (78%) ja keskisuurista (72%) vastaajista testaa toimivuutta. Pienistä yrityksistä joka toinen (54%) testaa toimivuuden.

Järjestelmien testaus on yleisintä kaupan alalla (73%) ja vähäisintä rakennusalalla (33%).

### **Eriytetyt tuotanto-, toimisto- ja tuotekehitystilat**

Tuotanto-, toimisto-, ja tuotekehitystilojen eriyttäminen parantaa turvallisuuden tasoa yrityksessä, koska silloin työntekijöillä ja vierailijoilla on pääsy vain tiettyihin tiloihin.

Kaikista vastaajayrityksistä 54 prosenttia on eriyttänyt tiloja. Kun pienistä yrityksistä vain 39 prosenttia eriytti tiloja, suurissa yrityksissä osuus oli 76 prosenttia. Pienissä yrityksissä tarve eriyttää tiloja on kuitenkin usein pienempi.

Tilojen eriyttäminen on yleisintä teollisuudessa (69 %) ja harvinaisinta palvelualalla (40 %).

### **Vierailujen ohjeistus**

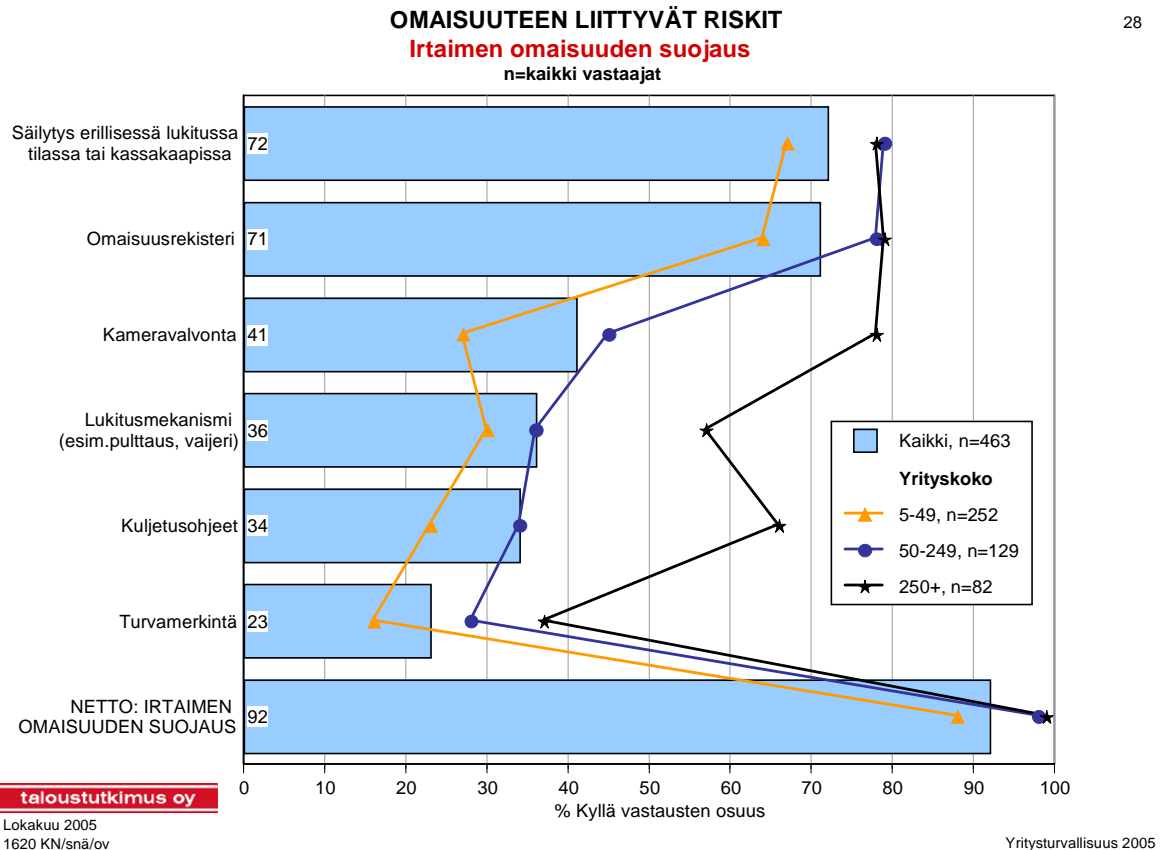
*"Tuntematon henkilö kulki kolmannen kerroksen käytävällä, ohi kaikkien lukittujen ovien..."*

Vierailujen ohjeistuksessa pitäisi määritellä, miten vieraat saapuvat ja poistuvat, mihin tiloihin vieraita saa tuoda ja miten vierailijoita valvotaan isännän toimesta vierailun aikana.

Yli puolet (54%) vastanneista yrityksistä on ohjeistanut vierailukäytännöt. Yleisintä tämä on suurten vastaajayritysten (89%) keskuudessa. Pienistä yrityksistä vain hieman yli kolmasosa (39 %) on ohjeistanut vierailut.

Vierailujen ohjeistus on yleisintä teollisuudessa (61%) ja harvinaisinta rakennusalalla (24%).

## 5.4 Omaisuuteen kohdistuvat riskit: Irtaimen omaisuuden suojaus



### Säilytys erillisessä lukitussa tilassa tai kassakaapissa

Yhteensä 72 prosenttia kaikista vastaajista säilyttää irtainta omaisuutta lukitussa tilassa tai kassakaapissa. Suurimpien (78 %) ja keski suurten (79 %) yritysten osuudet ovat miltei yhtä suuret. Pienimmistäkin vastaajayrityksistä yli kaksi kolmasosaa (67 %) tekee näin.

Säilytys erillisessä lukitussa tilassa on yleisintä kaupan alalla (80 %) ja harvinaisinta teollisuudessa (67 %).

### Omaisuusrekisteri

Rekisteri ja sen lisänä tehdyt turvamerkinnot ovat yksi tapa vähentää sisäisiä epäselvyyksiä irtaimen omaisuuden omistajasta. Lisäksi rekisteri ja merkinnät helpottavat myös rikosten selvittelyn yhteydessä omistussuhteen osoittamista ja oikean omistajan löytymistä.

Kaikista vastaajayrityksistä 71 prosenttia käyttää irtaimen omaisuuden rekisteriä. Rekisteriä käyttää suurista yrityksistä 79 prosenttia ja pienistä 64 prosenttia.

### Turvamerkintä

Merkinnällä helpotetaan omaisuuden tunnistamista ja rikosten selvittelyä. Merkintä saattaa myös ennaltaehkäistä omaisuusrikoksia.

Turvamerkintä on käytössä viidesosalla (23 %) yrityksistä. Yleisintä se on suurissa yrityksissä (37 %). Pienistä yrityksistä vain joka kuudes käyttää turvamerkintää.

Turvamerkinnän käyttö on yleisintä rakennusalalla (45 %) ja harvinaisinta teollisuudessa (20 %) ja kaupassa (20 %).

### **Lukitusmekanismi (esim. pulttaus tai vaijeri)**

Vain noin kolmasosa (36 %) vastaajayrityksistä käyttää lukitusmekanismeja irtaimen omaisuuden suojaamiseen. Suurimpien vastaajayritysten (57 %) keskuudessa se on yleisintä ja pienimpien vastaajayritysten keskuudessa vähäisintä (30 %).

Lukitusmekanismien käyttö on yleisintä kaupan alalla (49 %) ja harvinaisinta teollisuudessa (32 %) ja palvelualalla (34 %).

### **Kameravalvonta**

Kameravalvontaa irtaimen omaisuuden suojaksi käyttää noin kaksi yritystä viidestä (41 %). Yleisintä kameravalvontaa oli suurissa yrityksissä (78 %). Vähäisintä se oli pienimpien vastaajayritysten joukossa, niistä joka neljäs (27 %) käytti sitä.

### **Kuljetusohjeet**

Kuljetusohje ohjaa irtaimen omaisuuden käsittelyä silloin, kun omaisuus on toimitilojen ulkopuolella. Yritysten on aiheellista laatia ohje, jonka edellyttämät menettelytavat ja suojaustoimenpiteet vastaavat mahdollisuuksien mukaan sitä, mitä yritykset omilla toimitiloissa noudatetaan.

Hieman yli kolmasosa (34 %) kaikista vastaajayrityksistä on tehnyt kuljetusohjeet irtaimen omaisuuden suojaksi. Yleisintä se oli suurissa yrityksissä, joista kaksi kolmesta on tehnyt ohjeen. Harvinaisinta ohjeiden laatiminen oli pienissä vastaajayrityksissä, joista hieman alle neljäsosa (23 %) on laatinut ohjeen.

Kuljetusohjeet ovat yleisimpiä kaupan alalla ja teollisuudessa (38 %) ja harvinaisimpia ne ovat rakennusalalla (21 %).

### **Tarkistuslista 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

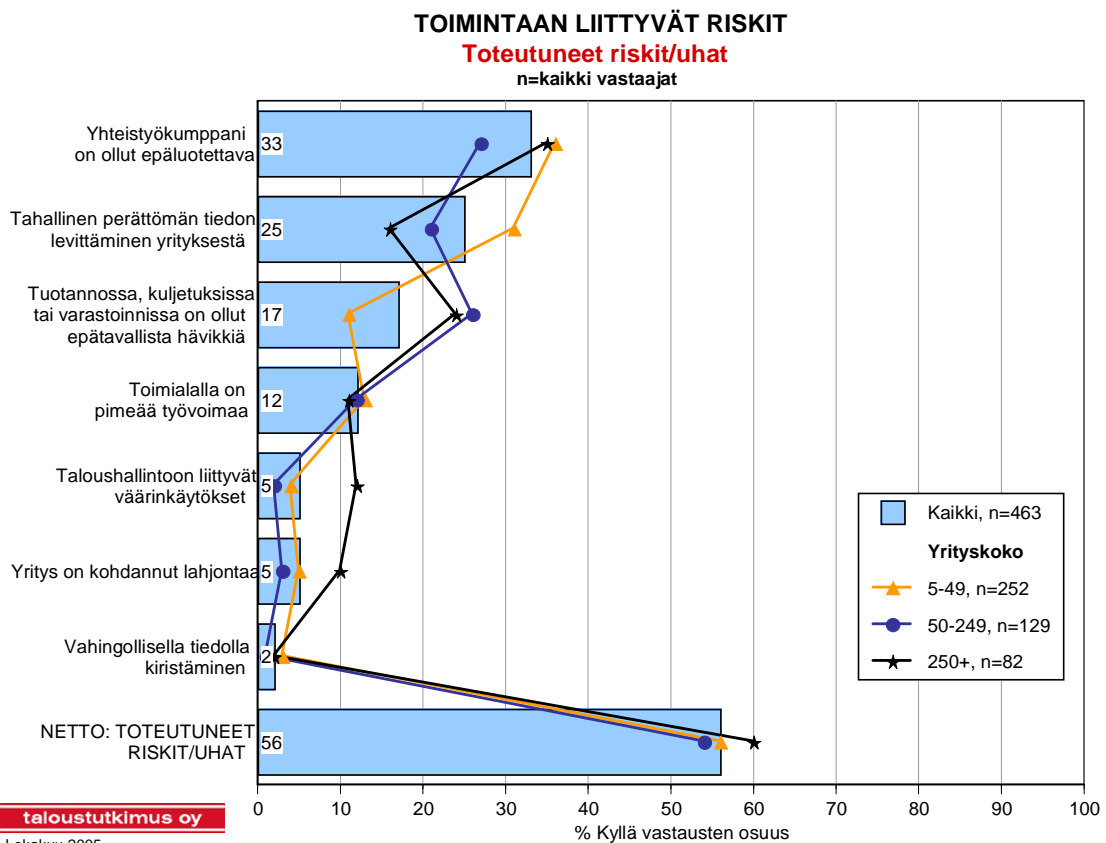
### **Tarkistuslista 4: Irtaimen omaisuuden suojaus**

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

## YRITYSTEN RIKOSTURVALLISUUS 2005

## 6 TOIMINTAAN KOHDISTUVAT RIKOKSET JA VÄÄRINKÄYTÖKSET

### 6.1 Toteutuneet riskit ja uhat



Yrityksen toimintaan kohdistuvista rikoksista ja väärinkäytöksistä ei ole olemassa kattavia tilastotietoja. Keskuskauppakamarin ja Helsingin seudun kauppakamarin selvitykseen vastanneet 463 yritystä tarkastelivat aihetta hävikin, perättömän tiedon levittämisen,

kiristyksen, yhteistyökumppanin epäluotettavuuden, pimeään työvoiman, lahjonnan ja taloushallinnon väärinkäytösten kannalta.

### **Hävikki**

*”Henkilökunnan jäsen varasti valmiita tuotteita myytäväksi suoraan.”*

*”Yrityksen työntekijän sekä ulkopuolisen turvayhtiön vartijan osallistuminen varkauteen.”*

*”Asennettavat tavarat ja työkalut katoavat rakennustyömailta. Työmaiden suojaus on heikkoa. Varkaat tietävät, mitä hakevat – onko heillä yhteyksiä tavarantoimittajiin? Vai ovatko työmaalla työskentelevät yhteydessä ammattirikollisiin?”*

Joka kuudes (17 %) yritys oli havainnut viimeisen kolmen vuoden aikana tuotannossa, kuljetuksissa tai varastoinnissa epätavallista hävikkiä. Hävikki oli selvästi keskimääräistä suurempi ongelma keskisuurissa ja suurissa yrityksissä, joista joka neljäs ilmoitti (24-26 %) hävikistä. Hävikki oli selvästi suurinta rakentamisessa ja kaupassa. Rakennusalalla neljännes (27 %) ja kaupan alalla jopa kolmannes (30 %) yrityksistä oli havainnut hävikkiä tarkasteluajana. Turvallisuusjohtajat ja talousjohtajat ilmoittivat hävikistä huomattavasti useammin kuin toimitusjohtajat.

Kaupan alan yritysten kokemukset hävikin suuruudesta vahvistavat sen, että hävikki on kaupalle iso menoerä. Brittiläisen Retail Research -tutkimuslaitoksen mukaan Suomen kauppojen hävikki suhteessa liikevaihtoon on toiseksi korkein Euroopassa. Suomen vähittäiskaupan hävikistä puolet johtuu myymälävarkauksista. Arviolta kolmannes myymälävarkauksista on kaupan oman henkilökunnan tekemiä. (Helsingin Sanomat 3.7.2005 ja Turun Sanomat 4.3.2005).

### **Perättömän tiedon levittäminen yrityksestä**

*”Globaali amerikkalainen markkinajohtaja tekee kustannuksia kaihtamatta ja pelkästään häirintämielessä tekaistun rikosilmoituksen pienestä suomalaisesta kilpailijasta.”*

Neljännes (25 %) yrityksistä oli kolmen viimeisen vuoden aikana havainnut, että yrityksen toiminnasta oli tahallisesti levitetty perättömää tietoa. Valtaosa (63 %) yrityksistä ei ollut kuitenkaan kohdannut ongelmaa. Ongelma oli keskimääräistä yleisempi pienissä yrityksissä (31 %) ja keskimääräistä harvinaisempi muissa yrityskokoluokissa. Tahallista perättömän tiedon levittämistä oli kohdannut vajaa kolmannes kaupan ja palvelualan yrityksistä, viidennes rakennusalan ja kuudennes teollisuudessa toimivista yrityksistä.

### **Epäluotettava yhteistyökumppani**

Useimmat vastanneista suomalaisista yrityksistä ovat olleet tyytyväisiä yhteistyökumppaniinsa. Kuusi yritystä kymmenestä pitää viimeaikaisia yhteistyökumppaneitaan luotettavina. Kolmanneksella (33 %) yrityksistä oli kuitenkin ollut huonoja kokemuksia yhteistyökumppaneista kolmen viimeisen vuoden aikana. Rakennusalalla toimivista yrityksistä yli puolella (55 %) on ollut epäluotettava yhteistyökumppani tarkasteluajana. Kaikilla muilla toimialoilla osuus jäi kolmannekseen.

### **Pimeä työvoima toimialalla**

Suurin osa vastaajista (79 %) ei ole kohdannut toimialallaan harmaata työvoimaa. Yrityksen koko tai vastaajan asema yrityksessä ei vaikuttanut vastaukseen. Toimialakohtaiset vastaukset erosivat kuitenkin selvästi toisistaan. Teollisuudessa toimivista yrityksistä vain viisi prosenttia oli havainnut, että toimialalla on harmaata työvoimaa. Kaupan ja palveluiden parissa toimivista yrityksistä joka kymmenes oli havainnut toimialalla harmaata työvoimaa. Rakennusalan yrityksistä jopa 58 prosenttia ilmoitti harmaasta työvoimasta toimialallaan. Ero muihin toimialoihin on erittäin merkittävä. Etelä- ja itäsuomalaiset yritykset ilmoittivat muiden vertailualueiden yrityksiä useammin harmaasta työvoimasta.

## Lahjonta

Kaksi kolmesta maailman valtiosta kärsii laajalle levinneestä korruptiosta. Kansainvälisissä korruptiovertailuissa Suomi on ollut toistuvasti yksi vähiten korruptoituneista maista maailmassa.

Kyselyyn vastanneet yritykset olivat kohdanneet lahjontaa vain harvoin. Lahjonta ei kuitenkaan ollut yrityksille täysin tuntematonta. Kaikista yrityksistä viisi prosenttia ja suurista yrityksistä jopa joka kymmenes (10 %) oli kohdannut lahjontaa. Teollisuudessa ja kaupassa toimivat yritykset olivat kohdanneet lahjontaa harvoin (3-4 % yrityksistä) ja palvelualan yritykset hieman useammin (6 %). Rakennusalan yrityksistä joka kymmenes (12 %) oli kohdannut lahjontaa tarkasteluaikana.

## Taloushallintoon liittyvät väärinkäytökset

*”Nuori taloushallinnon kaveri kavalsi rahaa palkkaennakon muodossa. Hän irtisanoutui ja silloin ilmeni kavallus. Rahat ovat yhä edelleen ulosotossa.”*

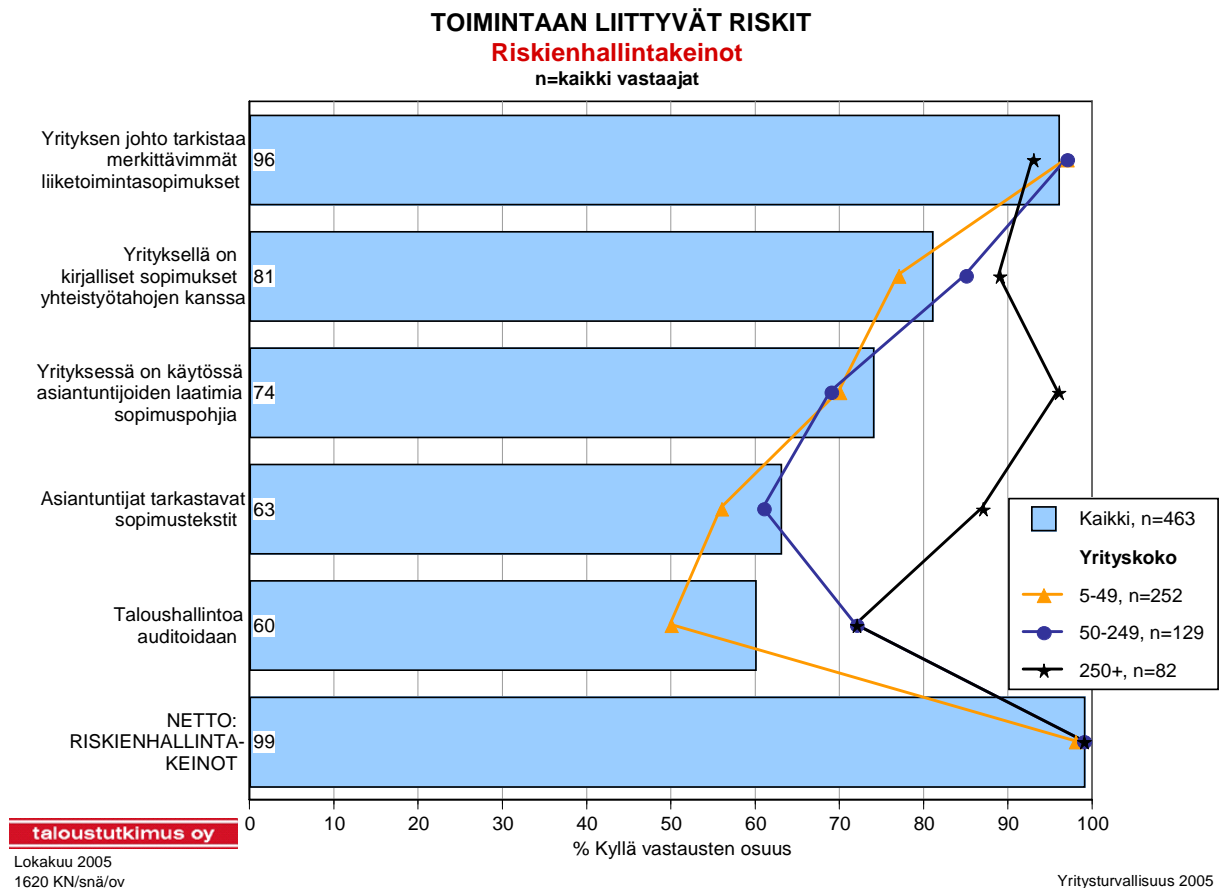
Oikeilla ja riittävillä tilinpäätöstiedoilla sekä asiantuntevalla ja riippumattomalla tilintarkastuksella on merkitystä yritysturvallisuudelle. Tilintarkastuksen tehtävänä ei ole rikosten ja väärinkäytösten estäminen tai paljastaminen. Ammattitaitoinen tilintarkastus ehkäisee kuitenkin myös virheiden ja puutteiden esiintymistä yrityksen toiminnassa. Yrityksen tilinpäätökseen ja toimintakertomukseen liittyvät virheet ja puutteet korjataan normaalisti ennen tilintarkastuskertomuksen julkistamista. Tilintarkastus ehkäisee sekä tahattomia että tahallisia virheitä ja puutteita yrityksen taloushallinnossa.

Valtaosa (91 %) yrityksistä ilmoitti, että niillä ei ole ollut taloushallintoon liittyviä väärinkäytöksiä viimeisen kolmen vuoden aikana. Taloushallintoon liittyviä väärinkäytöksiä oli ollut vain 5 prosentilla kaikista yrityksistä. Tarkasteluaikana keskimääräistä enemmän taloushallinnon väärinkäytöksiä oli suurissa yrityksissä (12 %), kaupan alalla (10 %) ja Etelä-Suomessa (7 %). Itä-Suomen sekä Oulun ja Lapin läänien alueella toimivat vastaajayritykset eivät olleet havainneet tarkasteluaikana taloushallinnon väärinkäytöksiä.

## Vahingollisella tiedolla kiristäminen

Vahingollisella tiedolla kiristäminen oli vastaajayrityksissä erittäin harvinaista. Vastaajista 94 prosenttia ei ollut joutunut tämän rikoksen kohteeksi ja vain 2 prosenttia ilmoitti rikoksesta. Vastauksissa ei ollut merkittäviä eroja yritys- ja vastaajan aseman tai toimialan suhteen.

## 6.2 Riskienhallintakeinot: Miten yritys on varautunut toimintaan kohdistuviin rikoriskeihin?



Lähes kaikilla (99 %) vastanneista 463 yrityksistä on käytössä jokin seuraavista riskienhallintakeinoista: Kirjalliset sopimukset yhteistyötahojen kanssa, asiantuntijat tarkastavat sopimustekstit, asiantuntijoiden laatimat sopimus pohjat, yrityksen johto tarkistaa merkittävimmät liiketoimintasopimukset ja yrityksen taloushallintoa auditoidaan.

### Kirjalliset sopimukset yhteistyötahojen kanssa

Neljällä viidestä (81 %) yrityksestä on kirjalliset sopimukset yhteistyötahojen kanssa. Palvelualalla ja keskisuurissa ja suurissa yrityksissä yhteistyösopimukset tehdään lähes aina kirjallisina. Joka neljäs (23 %) pieni tai rakennusalalla (24 %) toimiva yritys ja joka viides (20-22 %) teollisuuden tai kaupan alan yritys ei tee kirjallisia sopimuksia yhteistyötahojen kanssa.

### Asiantuntijat tarkastavat sopimustekstit

Kuudessa kymmenestä (63 %) yrityksestä asiantuntijat tarkastavat sopimustekstit. Pienissä ja keskisuurissa yrityksissä riskienhallintatoimet ovat tässä keskimääräisellä tasolla, kun taas valtaosa suurista yrityksistä turvautuu asiantuntijan apuun. Etelä-Suomessa toimivat ja palvelualan yritykset turvautuvat keskimääräistä useammin asiantuntijoihin.

**Asiantuntijat laativat sopimusohjat**

Kolmella neljästä (74 %) yrityksestä on käytössä asiantuntijoiden laatimia mallisopimuksia. Pienet ja keskiuuret yritykset ovat sopimusohjien käytön suhteen samalla viivalla 69 - 70 prosentilla, kun taas suuret yritykset erottuvat tässä voimakkaasti edukseen. Suurista yrityksistä vain yksi prosentti ilmoitti, että se ei käytä asiantuntijoiden laatimia sopimusohjia.

**Yrityksen johto tarkistaa merkittävimmät liiketoimintasopimukset**

Vastaajayritysten johto tarkistaa lähes poikkeuksetta (96 %) merkittävimmät liiketoimintasopimukset. Pienissä ja keskiuurissa yrityksissä sekä teollisuudessa, kaupassa ja palvelualalla kontrolli on keskimääräistäkin vahvempi.

**Taloushallinnon auditointi**

Auditoinnilla tarkoitetaan säännöllistä, riippumatonta ja dokumentoitua tarkastusta tai arviointia, jossa toimintaa verrataan annettuihin vaatimuksiin tai ohjeisiin. Tekijä voi olla ulkopuolinen tai omaan henkilöstöön kuuluva.

Yli puolet (60 %) yrityksistä on auditoinut taloushallintoaan. Auditointi on yleisintä keskiuurissa ja suurissa yrityksissä sekä teollisuudessa ja palvelualalla.

## YRITYSTEN RIKOSTURVALLISUUS 2005

### 7 TURVALLISUUSJOHTAMINEN

Yrityksen turvallisuuskulttuurilla tarkoitetaan yrityksessä toimivien ihmisten käyttäytymistä ja suhtautumista turvallisuuteen. Hyvä turvallisuuskulttuuri tukee yrityksen kilpailukykyä vähentämällä turvallisuusriskejä. Turvallisuusjohtaminen on yritysturvallisuuden päivittäistä toteuttamista ja hallintaa. Turvallisuusjohtamiseen kuuluvat ensisijaisesti yrityksen johdon ja henkilöstön sitouttaminen turvallisuustyöhön, sisäinen yhteistyö turvallisuusasioissa sekä riskikartoituksen tekeminen.

#### Yrityksen johdon osallistuminen turvallisuuden kehittämiseen

*”Ongelmana on henkilökunnan ja johdon välinpitämättömyys: Eihän meille ennenkään ole mitään sattunut-asetne”*

*”Tosiasiallista johdon sitoutumista ei ole, henkilöstön säännöllisen koulutuksen puute, avoimuuden puute turvallisuusasioista tiedottamisessa, turvallisuusasioiden vieminen jokaisen henkilön työtehtäviin kuuluvaksi.”*

*”Tarvittavan tiedon puute. Aiheeseen tarvittava aika on yrityksen varsinaisesta toiminnasta pois. Jonkinlainen valmis malli kokonaisvaltaisen turvallisuussuunnitelman ja ohjeistuksen luomiseen olisi paikallaan.”*

Neljä viidestä (80 %) yrityksestä ilmoitti, että yrityksen johto osallistuu henkilökohtaisesti turvallisuuden kehittämiseen. Joka kuudennessa (16 %) yrityksessä johto ei ollut mukana turvallisuussuunnittelussa. Yrityskoko, toimiala tai vastaajan asema ei vaikuttanut merkittävästi vastauksiin.

Etelä- ja Länsi-Suomessa toimivista yrityksistä valtaosa (80 - 88 %) ilmoitti, että yrityksen johto osallistuu henkilökohtaisesti turvallisuuden kehittämiseen. Itä-Suomessa toimivien yritysten kohdalla osallistumisaste oli alhaisempi (60 %).

#### Turvallisuusasioiden käsittely henkilökunnan kanssa

*”Suurin haaste turvallisuudelle on, että henkilökunta saadaan huomaamaan asian tärkeys”*

Rikosten ja väärinkäytösten ehkäiseminen ja paljastaminen on jokaisen yrityksessä työskentelevän vastuulla. Henkilökunnan turvallisuustietoisuuden lisääminen ja sitouttaminen turvallisuustyöhön ovat keskeisiä turvallisuusjohtamisessa. Valtaosa (82 %) yrityksistä käsittelee turvallisuusasioita yhdessä henkilökunnan kanssa. Teollisuudessa ja palvelualalla toimivat yritykset käsittelevät turvallisuusasioita hieman keskimääräistä

useammin henkilökunnan kanssa. Erot muilla toimialoilla toimivien yritysten vastauksiin ovat kuitenkin suhteellisen pieniä. Henkilöstö ei ole mukana turvallisuusasioiden käsittelyssä joka kuudennessa (16 %) yrityksessä. Pienistä, alle 50 henkilön yrityksistä viidennes (19 %) ei käsittele turvallisuusasioita henkilöstön kanssa.

### **Työntekijöiden vaikutusmahdollisuudet**

Työntekijöiden mahdollisuudet vaikuttaa turvallisuutta koskevaan päätöksentekoon sitouttavat henkilöstöä turvallisuustyöhön, tuovat uusia näkökohtia turvallisuussuunnitteluun sekä vähentävät muutosvastarintaa.

Useimmissa vastaajayrityksissä yrityksen työntekijät voivat vaikuttaa turvallisuutta koskevaan päätöksentekoon. Joka kymmenessä (11 %) vaikutusmahdollisuuksia ei kuitenkaan ole.

### **Yhteistyö turvallisuusasioissa**

Yrityksen rikos- ja väärinkäytösriskejä voidaan pienentää yrityksen sisäisellä yhteistyöllä. Sisäisen yhteistyön ja koordinoinnin puute voi muodostua merkittäväksi esteeksi yritysturvallisuudelle, koska riskejä pitäisi tarkastella jokaisella toiminta-alueella eri näkökulmista. Turvallisuuteen liittyvät toiminnot on yrityksissä perinteisesti hajautettu. Kokonaisvaltainen turvallisuuden hallinta vaatii kuitenkin yrityksen sisäisten ja ulkoisten toimijoiden keskinäistä yhteistyötä, tiedonkulkua ja oppimista.

Yrityksen eri osastojen välistä yhteistyötä turvallisuusasioissa oli 67 prosentilla yrityksistä. Sisäinen yhteistyö turvallisuusasioissa oli yleisintä keskisuurissa ja suurissa yrityksissä sekä teollisuudessa ja palvelualalla. Tähän tutkimukseen vastanneilta yrityksiltä ei kysytty ulkoisten toimijoiden, esimerkiksi alihankkijoiden kanssa tehtävästä yhteistyöstä turvallisuusasioissa.

### **Kirjallinen riskikartoitus**

Turvallisuusjohtamisen ja riskienhallinnan perustana on kirjallinen riskikartoitus. Riskikartoituksen tuloksien tulisi olla sellaisessa muodossa, että niitä voidaan käyttää päätöksenteon apuna.

Yritysturvallisuuteen liittyvä kirjallinen riskikartoitus oli tehty 38 prosentilla vastaajayrityksistä viimeisen kolmen vuoden aikana. Yrityksen koko ja toimiala vaikuttivat vastauksiin. Pienistä yrityksistä vain joka neljäs (24 %), keskisuurista joka toinen (49 %) ja suurista yrityksistä kuusi kymmenestä (62 %) oli tehnyt kirjallisen yritysturvallisuusriskikartoituksen. Riskikartoitusta ei ollut tehnyt kolme neljästä pienestä tai rakennusalalla toimivasta yrityksestä.

### **Toimintaohje poikkeustilanteita varten**

Neljässä kymmenestä (44 %) vastaajayrityksestä on laadittu ohje poikkeustilanteita varten. Poikkeustilanteisiin varautuminen yleistyy selvästi yrityksen koon kasvaessa: poikkeustilanneohje on neljänneksellä (25 %) pienistä, yli puolella (58 %) keskisuurista ja neljällä viidestä (79 %) suuresta yrityksestä. Joka toisella teollisuudessa toimivalla yrityksellä on poikkeustilanneohje. Muilla toimialueilla laaditaan ohjeita selvästi vähemmän.

### **Yritysturvallisuus on osa yrityksen vuotuista strategiasuunnittelua sekä budjetti- ja toimintasuunnittelua**

Vain kolmannes (33 %) yrityksistä oli liittänyt yritysturvallisuuden osaksi vuotuista strategiasuunnittelua ja budjetti- ja toimintasuunnittelua. Rakentamisessa osuus oli keskimääräistä vähäisempi (24 %). Pienten ja suurten yritysten antamien vastausten välinen ero oli merkittävä. Pienistä yrityksistä 21 prosenttia vastasi, että yritysturvallisuus on osa

vuotuista strategiasuunnittelua ja budjetti- ja toimintasuunnittelua. Suurissa yrityksissä osuus oli 60 prosenttia.

### **Turvallisuus on osa yrityksen laatujärjestelmää**

Turvallisuus on osa yrityksen toiminta- tai laatujärjestelmää joka toisessa (57 %) vastaajayrityksessä. Keskisuurissa ja suurissa yrityksissä sekä teollisuudessa toimivissa yrityksissä turvallisuus nähtiin useimmin osana toiminta- tai laatujärjestelmää.

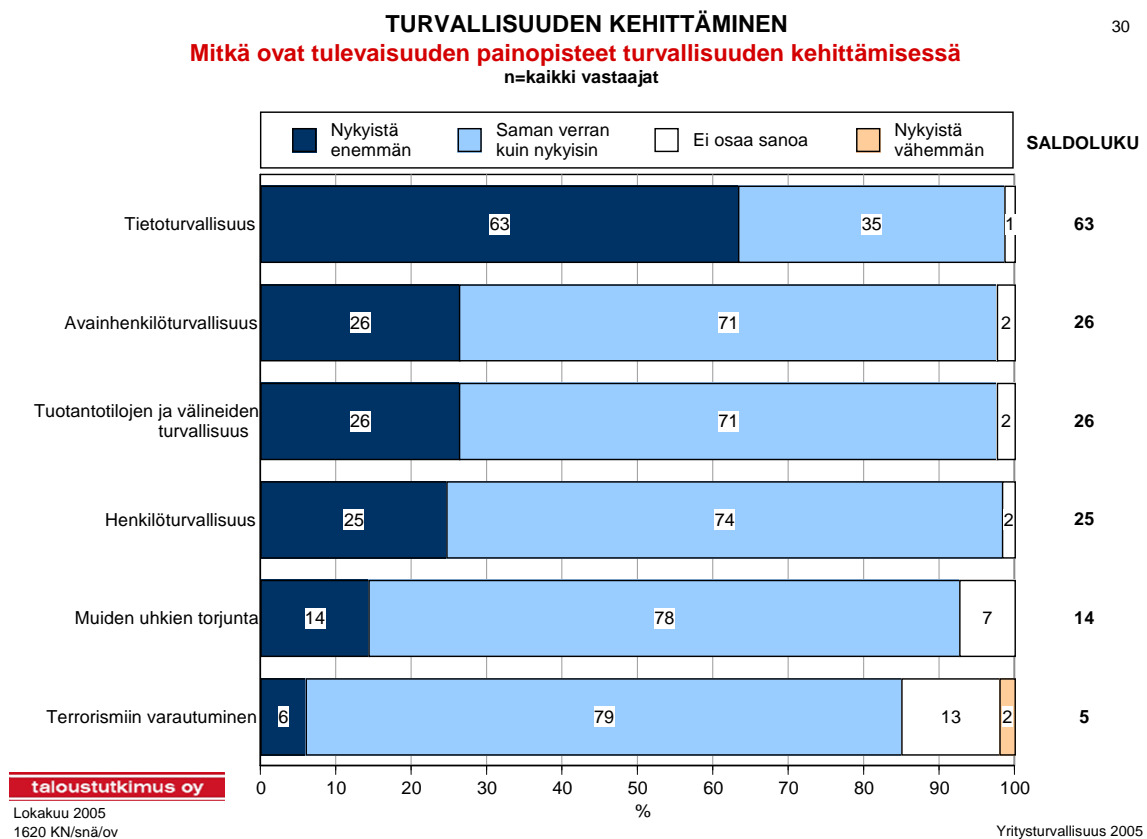
### **Tarkistuslista 5: Yrityksen turvallisuusjohtaminen**

- Yrityksen johto osallistuu henkilökohtaisesti turvallisuuden kehittämiseen
- Turvallisuusasioita käsitellään henkilöstön kanssa
- Työntekijät voivat vaikuttaa turvallisuutta koskevaan päätöksentekoon
- Yrityksen eri osastot/toimialat tekevät yhteistyötä turvallisuusasioissa
- Yritysturvallisuuteen liittyvä kirjallinen riskikartoitus on tehty viimeisen kolmen vuoden aikana
- Yrityksellä on toimintaohje poikkeustilanteita varten
- Yritysturvallisuus on osa yrityksen a) vuotuista strategiasuunnittelua b) vuotuista budjetti- ja toimintasuunnittelua
- Turvallisuus on osa yrityksen toiminta- tai laatujärjestelmää

## YRITYSTEN RIKOSTURVALLISUUS 2005

## 8 TURVALLISUUDEN PARANTAMINEN

## 8.1 Painopisteet turvallisuuden kehittämisessä



Kyselyyn vastanneet yritykset arvioivat myös tulevaisuuden painopisteitä turvallisuuden kehittämisessä.

Turvallisuuden kehittäminen painottuu tietoturvallisuuteen. Lähes kaksi kolmesta (63 %) yrityksistä vastasi, että tietoturvallisuuteen panostetaan yrityksessä jatkossa nykyistä enemmän. Tietoturvallisuus oli kaikissa yrityskokoluokissa tärkein kehittämisen kohde.

Taluspäälliköt ja turvallisuusjohtajat vastasivat toimitusjohtajia merkittävästi useammin, että tietoturvallisuuteen pitää panostaa nykyistä enemmän.

Lähes kaikki (99 %) yritykset korostavat henkilöturvallisuuden merkitystä turvallisuuden kehittämisessä. Kolme neljästä (74) yrityksestä aikoo panostaa henkilöturvallisuuteen saman verran kuin nykyisin ja neljäs nykyistä enemmän (25 %).

Kaikissa yrityksissä avainhenkilöturvallisuus on turvallisuuden kehittämisen kohde. Keskisuurista ja suurista yrityksistä vajaa kolmannes ja pienistä yrityksistä neljäs aikoo panostaa siihen nykyistä enemmän. Muiden vastaajien osalta avainhenkilöturvallisuuteen liittyvät panostukset pysyvät ennallaan. Erityisesti turvallisuusjohtajat lisäisivät avainhenkilöturvallisuuden painoarvoa turvallisuuden kehittämisessä.

Tuotantotilojen turvallisuus pysyy keskeisellä sijalla turvallisuuden kehittämisessä. Neljäs vastaajista aikoo lisätä siihen resursseja ja kolme neljästä pitää ne ennallaan.

Terrorismiin varautuminen oli vain harvalle yritykselle turvallisuuden kehittämisen kohde. Vaikka Suomen riski joutua terrorismin kohteeksi on suhteellisen pieni, kansainvälisessä liiketoiminnassa yritykset voivat joutua varautumaan terrorismiin uhkaan. Kaikista yrityksistä 6 prosenttia vastasi, että yritys aikoo varautua nykyistä enemmän terrorismiin tulevaisuudessa. Pienistä yrityksistä osuus oli vain 2 prosenttia, kun taas suurista yrityksistä joka kuudes (16 %) aikoi lisätä voimavaroja terrorismiin varautumiseen.

Kaikista vastaajista joka seitsemäs (13 %) ei osannut arvioida terrorismiin liittyvä uhkan laajuutta tai merkitystä yrityksen liiketoiminnalle.

## 8.2 Rikoriskeihin liittyvä tiedonsaanti

### Viranomaistiedon saatavuus ja tarve vastaajayrityksissä

Yritysten rikosturvallisuuskyselyyn vastanneista yrityksistä neljäs (24 %) sai tietoa rikoksista ja rikosilmiöistä viranomaisilta. Kaksi kolmesta (61 %) vastaajasta ilmoitti, että yritys ei ole saanut tietoa viranomaisilta yrityksiin kohdistuvista rikoksista ja rikosilmiöistä. Osuus oli merkittävästi suurempi pienissä yrityksissä, joissa jopa kolme neljästä (73 %) ei saanut tietoa. Keskisuurissa yrityksissä osuus oli keskimääräisellä tasolla (69 %), kun taas suurista yrityksistä vain neljäs (27 %) ei saanut tietoa viranomaisilta. Teollisuudessa, kaupassa ja palvelualalla toimivista yrityksistä kaksi kolmesta ja rakennusalalla jopa neljä viidestä ei ollut saanut tietoa rikosilmiöistä viranomaisilta.

Kaikista kyselyyn vastanneista yrityksistä 36 prosenttia oli saanut tietoa rikosilmiöistä muuta kautta, esimerkiksi lehdistöstä ja muista yrityksistä. Puolet (49 %) vastaajista ei ollut kuitenkaan saanut tietoa muistakaan lähteistä. Vastaukset vaihtelivat merkittävästi yrityskoon mukaan. Kun suurista yrityksistä vain 18 prosenttia ei ollut saanut tietoa muualta, niin keskisuurissa yrityksissä osuus oli 49 prosenttia ja pienissä yrityksissä jopa 60 prosenttia. Ero suurimman ja pienimmän yrityskokoluokan antamissa vastauksissa oli yli 40 prosenttiyksikköä.

Kyselyyn vastanneilta yrityksiltä tiedusteltiin tiedonsaannin lisäksi sitä, onko yrityksellä tarvetta saada viranomaisilta tietoa rikoksista ja rikosilmiöistä. Joka toinen (47 %) vastaaja ilmoitti tarvitsevansa tietoa viranomaisilta. Vaikka tiedon saanti rikoksista oli vähäisintä pienimmässä yrityskokoluokassa, niin pienimmät yritykset ilmoittivat keskimääräistä harvemmin (38 %) tarvitsevansa tietoa. Keskisuurista yrityksistä joka toinen (51 %) ja suurista yrityksistä kaksi kolmasosaa (66 %) ilmoitti tiedontarpeesta. Toimialakohtaisissa vastauksissa ei ollut merkittäviä eroja. Teollisuudessa ja rakennusalalla toimivista yrityksistä neljä kymmenestä ja kaupassa ja palvelualalla joka toinen ilmoitti tarvitsevansa tietoa viranomaisilta.

### **Tiedonsaanti kauppakamareilta**

Kauppakamari on alueensa yritysten edunvalvonta-, yhteistyö- ja palveluorganisaatio. Kauppakamarijärjestössä on 16 400 jäsenyritystä. Kauppakamarien toiminta perustuu kauppakamarilakiin.

Selvitykseen vastanneet yritykset toivoivat vastauksissa, että kauppakamari tukisi yrityksiä turvallisuusjohtamisessa.

Henkilömäärältään pienet (alle 50 henkilöä) ja keskisuuret yritykset (50-249 henkilöä) toivoivat kauppakamarilta erityisesti yritysturvallisuuteen liittyvää koulutusta, tiedotusta ja neuvontaa, turvallisuuskartoituksia, muistilistoja huomioitavista asioista sekä turvallisuus- ja riskikartoitusmateriaalia. Suuret yritykset (yli 250 henkilöä) korostivat myös turvallisuuskoulutuksen ja uhkista tiedottamisen merkitystä. Suuret yritykset toivoivat myös, että kauppakamarit kehittäisivät viranomaisyhteistyötä ja tarjoaisivat turvallisuusauditointipalvelua.

## YRITYSTEN RIKOSTURVALLISUUS 2005

### 9 JOHTOPÄÄTÖKSET

#### **Turvallisuustietoisuutta lisättävä**

Yrityksen toiminnan turvaaminen sekä yrityksen henkilöstön, yhteistyökumppanien ja asiakkaiden turvallisuus ovat keskeinen osa yrityksen riskienhallintaa. Teknisiin yrityksen turvallisuutta edistäviin ratkaisuihin turvaudutaan useimmissa yrityksissä. Liian moni yritys unohtaa kuitenkin sen, että turvallisuus lähtee ihmisistä. Turvallisuuskoulutusta ei ole järjestänyt puolet pienistä, kolmannes keskisuurista ja viidennes suurista yrityksistä. Huolellisella rekrytoinnilla ja henkilöiden taustaselvityksillä yritys pystyy vähentämään merkittävästi henkilökuntaan liittyviä turvallisuusriskejä ja varmistamaan, että palkattava henkilö soveltuu työtehtävään. Vain kolmannes yrityksistä selvittää palkattavan työntekijän taustan. Taustaselvitysten tekeminen ei ole yleistä missään kokoluokassa. Yritykset selvittävät avainhenkilöidensä taustat huolellisemmin kuin muun henkilökunnan taustat.

#### **Yritykset panostavat tietoturvaan**

Toteutuneista tietoriskeistä yleisimpiä yrityksissä olivat tietoverkkoon murtautumisen tai hakkeroinnin yritys ja tietojen kopiointi omaan käyttöön ennen siirtymistä pois yrityksen palveluksesta.

Yritykset ymmärtävät hyvin tiedon merkityksen kilpailukyvyille. Ne käyttävät salassapitosopimuksia, kilpailukieltosopimuksia ja koulutusta yritykselle tärkeän tiedon suojaamisessa. Parannettavaa on erityisesti tiedon luokituksen ja käsittelyohjeiden laatimisessa. Luokittelu- ja käsittelyohjeet ovat tiedon suojaamisen perusta, sillä ilman niitä yrityksen on hyvin vaikeaa yksilöidä ja suojata liike- ja ammattisalaisuuksiaan. Turvallisuuden kehittämisessä yritykset panostavat tietoturvaan.

#### **Yritykset ovat varautuneet omaisuusrikoksiin**

Omaisuusriskeistä useimmin toteutuivat työväline- tai laitevarkaudet ja murrot toimi- tai tuotantotiloihin.

Omaisuuksien suojaamisessa yritykset hyödyntävät laajasti teknisiä suojajärjestelmiä ja vartiointia. Irtainta omaisuutta merkitään ja suojataan monin tavoin. Riskien vähentämiseksi yritysten on erityisesti panostettava koulutukseen ja inhimillisten tekijöiden huomioimiseen. Esimerkiksi valvontajärjestelmien käyttö edellyttää henkilöiden perehdyttämistä järjestelmien vaatimiin toimintatapoihin.

### **Lahjonta ja pimeä työvoima eivät täysin tuntemattomia**

Kyselyyn vastanneet yritykset olivat kohdanneet lahjontaa vain harvoin, mutta lahjonta ei myöskään ollut täysin tuntematonta. Kaikista yrityksistä viisi prosenttia ja suurista yrityksistä jopa joka kymmenes oli kohdannut lahjontaa. Rakennusalan yrityksistä joka kymmenes oli kohdannut lahjontaa viimeisen kolmen vuoden aikana.

Kymmenesosa vastaajista oli kohdannut toimialallaan pimeää työvoimaa. Teollisuudessa osuus oli vain viisi prosenttia. Kaupan ja muiden palveluiden parissa toimivista yrityksistä joka kymmenes oli havainnut toimialalla pimeää työvoimaa. Rakennusalan yrityksistä lähes kaksi kolmasosaa ilmoitti pimeästä työvoimasta toimialallaan. Ero muihin toimialoihin oli merkittävä.

### **Yritykset eivät saa riittävästi tietoa rikoksista ja väärinkäytöksistä**

Yrityksiin kohdistuvat rikokset ja väärinkäytökset eivät ole ainakaan vähentyneet viime vuosina. Kolmannes vastaajista ilmoitti, että yritykseen kohdistuvat rikosriskit ja väärinkäytökset ovat lisääntyneet ja kaksi kolmasosaa, että ne ovat pysyneet ennallaan. Eniten rikokset ovat lisääntyneet suurimmissa yrityksissä.

Suurin osa vastaajista ei saa kuitenkaan riittävästi tietoa viranomaisilta yrityksiin kohdistuvista rikoksista ja rikollisuudesta. Pienimmissä yrityksissä koetaan suuria enemmän, ettei tietoa saada. Yritykset toivoivat, että elinkeinoelämän ja viranomaisten välistä tiedotusta sekä yrityksille suunnattua yritysturvallisuuskoulutusta lisättäisiin.

### **Turvallisuusjohtaminen johdon vastuulla**

Turvallisuusjohtamiseen kuuluvat ensisijaisesti yrityksen johdon ja henkilökunnan sitouttaminen turvallisuustyöhön, sisäinen yhteistyö turvallisuusasioissa sekä pitkäjänteinen riskienhallintatyö.

Neljässä viidestä yrityksestä johto osallistuu henkilökohtaisesti turvallisuuden kehittämiseen. Neljäsosassa vastanneista yrityksistä yrityksen eri osastot eivät tee yhteistyötä turvallisuusasioissa. Yritysturvallisuuteen kuuluva kirjallinen riskikartoitus oli tehty neljällä kymmenestä vastaajayrityksestä viimeisen kolmen vuoden aikana. Vain kolmannes yrityksistä oli liittännyt yritysturvallisuuden osaksi vuotuista strategiasuunnittelua ja budjetti- ja toimintasuunnittelua.

## YRITYSTEN RIKOSTURVALLISUUS 2005

**LÄHTEITÄ JA LISÄTIETOA**

Helsingin kauppakamari (2004) Selvitys yritysten liiketoiminnan riskeistä ja toiminnalle olennaisten turvallisuuden osa-alueiden hallinnasta Uudenmaan alueella. Yritysturvallisuusprojekti 2004.

Kauppakamarijärjestön kotisivuilla on tilintarkastukseen liittyviä ohjeita, selvityksiä ja ratkaisuja sekä KHT- ja HTM-tilintarkastajien yhteystietohaku. <http://www.kauppakamari.fi> ja [http://www.kauppakamari.fi/kkk/toimialat/Tilintarkastus/fi\\_FI/Tilintarkastus/](http://www.kauppakamari.fi/kkk/toimialat/Tilintarkastus/fi_FI/Tilintarkastus/) (21.10.2005)

Lehtonen, Jaakko (1999) Kriisiviestintä.

Suomen Hotelli- ja Ravintolaliitto, Palvelualojen ammattiliitto ja Työturvallisuuskeskus (2002) Toimi ennalta – ehkäise väkivaltaa-opas sekä Kaupan Keskusliitto, Poliisi, Suomen Vakuutusyhtiöiden Keskusliitto ja Työturvallisuuskeskus 2000, Avaimet turvatoimiin.

Suomen Kauppakeskusyhdistys ry (2005) Kauppakeskusten turvallisuusjohtaminen. Selvitys tukee myös yrityksen turvallisuusjohtamista ja riskien tunnistamista.

Suomen toimitila- ja rakennuttajaliitto RAKLI:n sivuilla on Toimitilaturvallisuus ja sähköiset turvallisuusjärjestelmät - opas. [Http://www.rakli.fi/tiedotteet/julkaisut/julkaisutaraportit/](http://www.rakli.fi/tiedotteet/julkaisut/julkaisutaraportit/) (1.11.2005)

Tampereen teknillinen yliopisto, Turvallisuustekniikan laitos (2004) Yhteistyö yritysturvallisuuden hallinnassa. Pikaopas yhteistyön ja kokonaisvaltaisen turvallisuuden kehittämiseen. Oppaaseen on koottu vinkkejä yhteistyön kehittämiseen ja arviointiin. Opas on suunnattu yritysten ja organisaatioiden turvallisuustoiminnassa mukana oleville. Ks. myös Turvallisuustekniikan laitoksen kotisivu <http://turva.me.tut.fi> (27.10.2005).

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

Teknologian tutkimuskeskuksen Tekesin kotisivuilla on yrityksille sopimuksiin liittyviä muistilistoja ja mallisopimuksia sekä sopimusopas pk-yritysten yhteishankkeisiin. [Http://www.tekes.fi/rahoitus/yritys/](http://www.tekes.fi/rahoitus/yritys/) (20.10.2005).

Teollisuus ja Työnantajat (2001) Ovatko yrityksesi tietoriskit hallinnassa? Käytännön tietoturvallisuusopas PK-yrityksille. Oppaassa on tietoturvallisuuteen liittyviä tarkistuslistoja, esimerkkejä ja sopimusmalleja. [Http://www.ek.fi/ytnk/pdf/tietoturva.pdf](http://www.ek.fi/ytnk/pdf/tietoturva.pdf) .

Tietoyhteiskunnan kehittämiskeskus TIEKE on tehnyt yrityksille muistilistoja tietoturvan tason tarkistamiseksi. Verkkokaveri-tietopalvelussa on tietoa tietoturva-asioissa yrityksille, [www.tieke.fi/verkkokaveri](http://www.tieke.fi/verkkokaveri) (20.10.2005)

Ulkoasiainministeriön matkustusturvallisuuden neuvottelukunta on laatinut Turvallista matkaa oppaan. Opasta voi käyttää tausta-aineistona laadittaessa yrityskohtaista matkustusturvallisuusopasta. Opas on löydettävissä ministeriön kotisivuilta [http://www.formin.fi/doc/fin/palvelut/matkustaminen/MNK\\_esite.pdf](http://www.formin.fi/doc/fin/palvelut/matkustaminen/MNK_esite.pdf) (20.10.2005).

Vakuutusyhtiöiden keskusliiton kotisivuilla on ohjeita omaisuuden suojaamisesta. Sieltä löytyvät seuraavat ohjeet: Rakenteellinen murtosuojausohje, Vältä omaisuusrikos toimistossa, Avainturvallisuusohje, Kassakaappiohje ja Tietotekniikkalaitteiden katoamisien ja varkauksien torjuntaohje. Vakuutusyhtiöiden keskusliiton kotisivu <http://www.vakes.fi/> (1.11.2005)

VTT Automaatio ja Turun kauppakorkeakoulu (2000) Kokeiletko aina onneasi? Riskienhallinnan perusteet PK-yrityksille ja työtekijöille.

Tilastokeskuksen sivuilta löytyy tilastotietoa esimerkiksi rikollisuudesta ja rikostenselvittämisprosenteista. [Http://www.stat.fi/](http://www.stat.fi/) .

Yrittäjänäisten keskusliitto (2005) Yrittäjänäisten turvaopas. Oppaassa on riskinäkökulmien mukaan ohjeita yrittäjiä uhkaavien turvallisuusriskien ennaltaehkäisystä. [Http://www.yrittajanaiset.fi](http://www.yrittajanaiset.fi) (20.10.2005)

Yritysturvallisuuden neuvottelukunnan sivuilla on monipuolista tietoa siitä, miten yritysturvallisuutta voidaan edistää yrityksessä. [Http://www.ytnk.fi](http://www.ytnk.fi)

**Liite****YRITYSTURVALLISUUSKYSELY****1. YRITYSRIKOSTEN MÄÄRÄN KEHITYS**

*Ovatko yritykseen kohdistuvat rikosriskit ja väärinkäytökset viimeisen kolmen vuoden aikana*

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

**2. IHMISIIN LIITTYVÄT RISKIT****a) Toteutuneet riskit /uhat**

*Onko yrityksessänne viimeisen kolmen vuoden aikana*

Kyllä / Ei/ EOS

- 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?

**b) Riskienhallintakeinot:**

*Onko yrityksenne käyttänyt seuraavia riskienhallintakeinoja?*

Kyllä / Ei/EOS

- Taustaselvitykset työntekijöistä
- Taustaselvitykset avainhenkilöistä
- Yhteistyökumppanien luotettavuusselvitykset
- Asiakkaiden luottokelpoisuusselvitykset
- Alihankkijoiden referenssien tarkastaminen
- Kaikki sopimukset tehdään kirjallisina
- Salassapitosopimus on käytössä
- Kilpailukieltosopimus on käytössä

*Miten yrityksenne on varautunut ihmisiin kohdistuviin rikosriskeihin työtehtävissä?*

Kyllä / Ei/EOS

- Työympäristön teknisillä ratkaisuilla
- Avainhenkilöille on varamiesjärjestelmä
- Poikkeustilanteisiin on tehty kriisiviestintäsuunnitelma
- Henkilötietojen suojaus on määritelty
- Matkustamisesta on annettu turvallisuusohjeet
- Työntekijöille annetaan turvallisuuskoulutusta

Työntekijöitä kannustetaan kertomaan havaitsemistaan turvallisuuspuutteista  
Turvallisuusasiat ovat osa perehdyttämiskoulutusta

### 3. TIETOON LIITTYVÄT RISKIT

#### a) Toteutuneet riskit /uhat

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

Kyllä / Ei/ EOS

Kriittisistä yritysasioista kertominen luvatta kolmannelle osapuolelle  
Luottamuksellista yritysasiaa sisältävän asiakirjan luovuttaminen luvatta kolmannelle osapuolelle  
Yritystiedon (sisällön) luvaton urkkiminen / vakoilu  
Yritystiedon (sisällön) luvaton muuttaminen / väärentäminen  
Tietojen kopiointi omaan käyttöön ennen siirtymistä pois yrityksen palveluksesta  
Tietoverkkoon murtautuminen tai hakkerointi  
Tietoverkkoon murtautumisen tai hakkeroinnin yritys  
Tiedostojen tahallinen tuhoaminen

Arvioi tapahtuneen vahingon suuruus asteikolla *pieni, keskisuuri, suuri*. Merkitse myös tekijä: *ulkopuolinen taho tai lähipiiriin kuuluva*.

Pieni, keskisuuri, suuri, EOS U/L

Kriittisistä yritysasioista kertominen luvatta kolmannelle osapuolelle  
Yritysasiaa sisältävän asiakirjan luovuttaminen luvatta kolmannelle osapuolelle  
Yritystiedon (sisällön) luvaton urkkiminen / vakoilu  
Yritystiedon (sisällön) luvaton muuttaminen / väärentäminen  
Tietojen kopiointi omaan käyttöön ennen siirtymistä pois yrityksen palveluksesta  
Tietoverkkoon murtautuminen tai hakkerointi  
Tiedostojen tahallinen tuhoaminen

#### b) Riskienhallintakeinot:

Miten yrityksenne on varautunut tiedon väärinkäytöksiin?

*Tiedon suojaus*

Kyllä / Ei/EOS

Onko yrityksellänne tärkeitä tietoja( liike- ja ammattisalaisuudet) koskeva luokittelu- ja käsittelyohje?  
Onko yrityksellänne muita tietoja koskeva luokittelu- ja käsittelyohje?  
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 yritysvalvontaan kohteena?

#### 4. TOIMINTAAN LIITTYVÄT RISKIT

##### a) Toteutuneet riskit /uhat

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

Kyllä / Ei/ EOS

- 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
- Taloushallintoon liittyvät väärinkäytökset
- Vahingollisella tiedolla kiristäminen

##### b) Riskienhallintakeinot:

*Miten yrityksenne on varautunut yrityksen toimintaan kohdistuviin rikosriskeihin työtehtävissä?*

Kyllä / Ei/EOS

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

*Kuuluvatko yrityksen turvallisuusjohtamiseen seuraavat osat?*

Kyllä / Ei/EOS

- Yrityksen johto osallistuu henkilökohtaisesti turvallisuuden kehittämiseen
- Turvallisuusasioita käsitellään henkilöstön kanssa
- Työntekijät voivat vaikuttaa turvallisuutta koskevaan päätöksentekoon
- Yrityksen eri osastot/toimialat tekevät yhteistyötä turvallisuusasioissa
- Yritysturvallisuuteen liittyvä kirjallinen riskikartoitus on tehty viimeisen kolmen vuoden aikana
- Yrityksellä on toimintaohje poikkeustilanteita varten
- Yritysturvallisuus on osa yrityksen a) vuotuista strategiasuunnittelua b) vuotuista budjetti- ja toimintasuunnittelua
- Turvallisuus on osa yrityksen toiminta- tai laatu järjestelmää

#### 5. OMAISUUTEEN LIITTYVÄT RISKIT

**Tilannekuvaus: Yrityksen hallussa oleva asiakkaan omaisuus, tieto ja suojaustarpeet**

Kyllä / Ei/ EOS

- Yrityksellämme on hallussaan asiakkaiden omaisuutta
- Yrityksellämme on hallussaan asiakkaiden tietoja
- Asiakkaan edustaja on kartoittanut yrityksemme toiminnan riskejä
- Asiakkaan edustaja on auditoinut yrityksemme toimintatapoja

Yhteistyösopimukseen on kirjattu toimintatavat asiakkaan omaisuuden / tietojen suojaamiseksi

**a) Toteutuneet riskit /uhat**

*Onko yrityksenne omaisuuteen kohdistunut seuraavia rikoksia tai väärinkäytöksiä viimeisen kolmen vuoden aikana? Merkitse myös tekijä: ulkopuolinen taho(U) tai lähipiiriin kuuluva (L)*

Kyllä / Ei/ EOS U/L

Murto toimi- tai tuotantotiloihin  
 Ilkivalta toimi- tai tuotantotiloihin  
 Ilkivalta yrityksen muuhun omaisuuteen  
 Työväline- tai laitevarkaus  
 Merkittävä hävikki

*Arvioi tapahtuneen vahingon suuruus asteikolla pieni, keskisuuri, suuri.*

Pieni, keskisuuri, suuri, EOS

Murto toimi- tai tuotantotiloihin  
 Ilkivalta toimi- tai tuotantotiloihin  
 Ilkivalta yrityksen omaisuuteen  
 Työväline- tai laitevarkaus  
 Tietokone- tai muu laitevarkaus

**b) Riskienhallintakeinot:**

*Onko omaisuuden suojaamiseksi tehty seuraavia toimia?*

*Tuotanto- ja toimitilojen suojaus*

Kyllä / Ei/EOS

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

*2. Irtaimen omaisuuden suojaus*

Kyllä / Ei/EOS

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

## 6. TURVALLISUUDEN KEHITTÄMINEN

*Mitkä ovat tulevaisuuden painopisteet turvallisuuden kehittämisessä?/ Panostaako seuraaviin yritysturvallisuuden osa-alueisiin nykyistä enemmän/ saman verran kuin nykyisin/ Nykyistä vähemmän*

Tietoturvallisuus  
Henkilöturvallisuus  
Avainhenkilöturvallisuus  
Tuotantotilojen ja välineiden turvallisuus  
Terrorismiin varautuminen  
Muiden uhkien torjunta

*Rikosriskeihin liittyvä tiedonsaanti viranomaisilta*

Kyllä / Ei/EOS

Saako yrityksenne tietoa viranomaisilta yrityksiin kohdistuvista rikoksista ja rikosilmiöistä

Saako yrityksenne tietoa jostain muualta?

Tarvitseeko yrityksenne tietoa viranomaisilta?

### **Avoimet kysymykset:**

Mitä asioita pidätte suurimpina esteinä yritysturvallisuudelle?

\_\_\_\_\_

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

\_\_\_\_\_

Kohdistuuko yrityksenne erityisiä turvallisuusuhkia esimerkiksi toimialanne tai kansainvälisen kehityksen vuoksi. Mitä ne ovat?

\_\_\_\_\_

Miten kauppakamari parhaiten tukisi yritystänne turvallisuuden parantamisessa

\_\_\_\_\_



**Keskuskauppamari**

Aleksanterinkatu 17, PL 1000

00101 Helsinki

puh. (09) 696 969

faksi (09) 650 303

[keskuskauppamari@chamber.fi](mailto:keskuskauppamari@chamber.fi)

