



**PREVENTING CRIME AND  
MISCONDUCT IN BUSINESS**

# Preventing crime and misconduct in business



## Companies must invest in crime risk prevention

Over a third of Finnish companies consider that the risk of crime and misconduct has increased during the period 2003-2005. The risk of becoming a target for criminal activities has grown particularly in large companies with more than 250 employees.

Investing in crime and misconduct prevention tends to be more financially advantageous rather than settling losses after they have occurred. Corporate security protects the company's business activities, interest groups, data and property from human error, misconduct and criminal intent. To support their efforts to establish a secure environment, companies need information about criminal practices and methods of safeguarding themselves. Small businesses are most in need of this type of information.

Small and medium-sized companies invest all too little in risk-reducing measures. The reasons for this can often be found in limited available resources and a

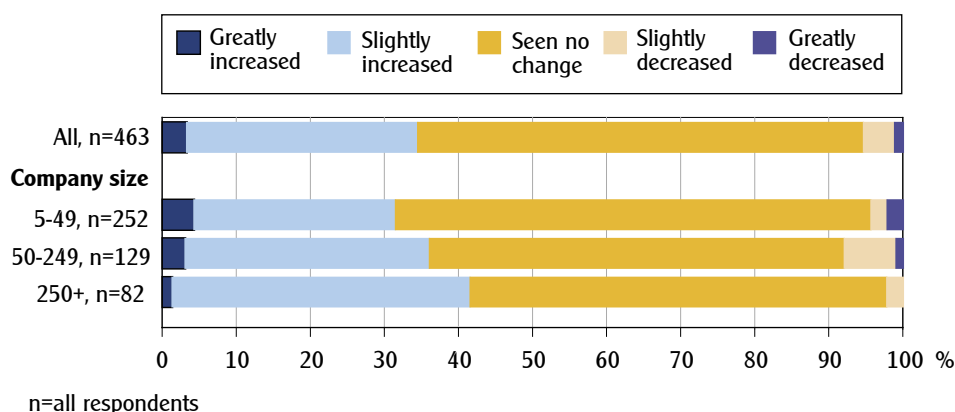
lack of awareness about the types of crime and other threats they may be facing. In Finland, 73 % of small businesses (less than 50 employees) and 59 % of medium-sized businesses (50-250 employees) do not receive information from the authorities concerning crimes and other threats.

The largest companies (more than 250 employees) clearly invest the most in measures to reduce potential security risks. However, a notably higher number of crimes and acts of misconduct are directed at large companies. A quarter of large companies in the survey do not receive information from the authorities about criminal practices and methods.

The Central Chamber of Commerce of Finland and the Helsinki Region Chamber of Commerce conducted a comprehensive survey concerning the nature and severity of the risks of crime and misconduct directed at Finnish companies, the utilised prevention methods, and the companies' preparedness. This report is based on the responses of 463 company executives.

## Corporate crime in Finland

During the past three years, criminal risks and misconduct in business have



## Security training carried out in only every second company

*“An outsider passed through all of the locked doors simply because of the courtesy of personnel.”*

*“An employee gave out the password to the company’s data network on the basis of a fabricated story.”*

The majority of companies rely on technical security measures. However companies should invest in security training in addition to technical solutions, because security can fail as a result of unintentional or deliberate actions made by personnel. Security training is not offered in half of small companies, one third of medium-sized companies and one fifth of large companies in the survey.

Information leaks can also be reduced through training. If the company has not provided any guidance on information management, then the easiest way to gain access to confidential company information may simply be by contacting one of its employees. Half of

the companies have not trained their personnel in how to handle confidential information.

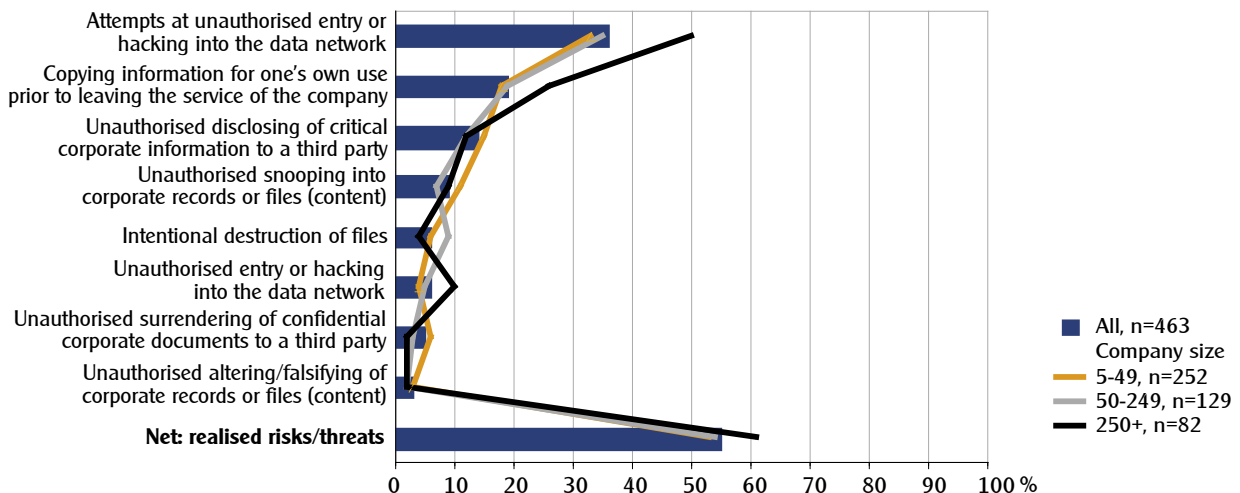
A thorough employee recruiting process, including background checks, assists in developing corporate security. These processes help the company to reduce the security risks related to its personnel and ensure that a person is suitable for the task he/she is being hired to perform. Only a third of the companies perform background checks when hiring new employees. Every second company checks, however, the background of their key personnel.

## Data security violations are common

Attempted crimes and acts of misconduct are often directed at company records and files. More than half of the responding companies stated that their company’s data security was violated during the period 2003-2005. The most common breaches involved attempts at unauthorised entry into the company’s data network (36 % of the companies). In large companies the number of attempts at unauthorised entry was higher than the average. One in five companies did not know whether or not there had ever been an attempt at unauthorised entry into their own data network. A majority of companies (63 %) considered that further improvements to their data security are needed.

### Risks related to data security

Realised risks/threats



### Data security in companies

- ▶ 33 % of companies use background checks on employees and
- ▶ 49 % on key personnel
- ▶ 57 % have security training for personnel
- ▶ 54 % check the reliability of partners
- ▶ 37 % have guidelines for classifying and handling business and professional secrets
- ▶ 33 % have guidelines for the classification and handling of other information
- ▶ 44 % arrange training in handling confidential information

Precautions for the event that an employee should be hired by or become a competitor

- ▶ 73 % of the companies use non-disclosure agreements and
- ▶ 54 % non-competition agreements

a company can be leaked to an external party with deliberate intent. In every fifth company, an employee had copied internal company data prior to moving to another company within the same field of business or starting up his / her own company.

The chance that confidential business information may end up in the hands of competitors may significantly harm a company's business activities. In order to define a crime as it relates to business secrets and to acquire the appropriate legal safeguards, the company must determine which information might be considered as secret, establish instructions for handling confidential

### Data security improves a company's legal standing

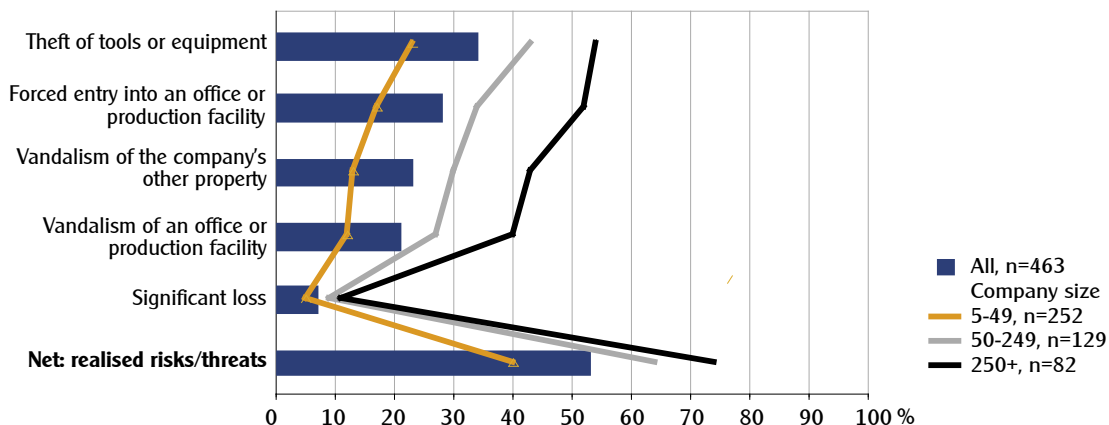
Every company has information that needs to be protected. However, confidential information about

*"The greatest risks to corporate security are people who are about to leave the company."*

*"We don't have a non-competition agreement, and the departure of two agents brought a surprising loss for our company's representation. Bids that had been made by our company were then reissued in another company's name."*

### Risks related to property

Realised risks/threats



# Preventing crime and misconduct in business

material and train its personnel on how to handle such information. 73 % of the companies have a non-disclosure agreement in use, but only one third of the companies have drawn up guidelines concerning the processing or handling of business or professional secrets. Every second company has a non-competition agreement in use.

## Property is well protected

Most of the risks related to a company's property concern the theft of tools and equipment (34%); this type of theft is experienced in as much as 79 % of companies in the construction field. 28 % of the companies had experienced unauthorised entries into their offices and production facilities. The greatest loss of material is experienced in construction and trade fields.

Companies utilise a wide variety of technical security systems and security guard services in order to protect their property. Moveable property is well marked and protected. In order to reduce the risks, companies should invest in training and determining the human risk factors. For example, the use of a monitoring system requires that personnel acquaint themselves with the procedures required by the systems.

## Service sector employees are being threatened

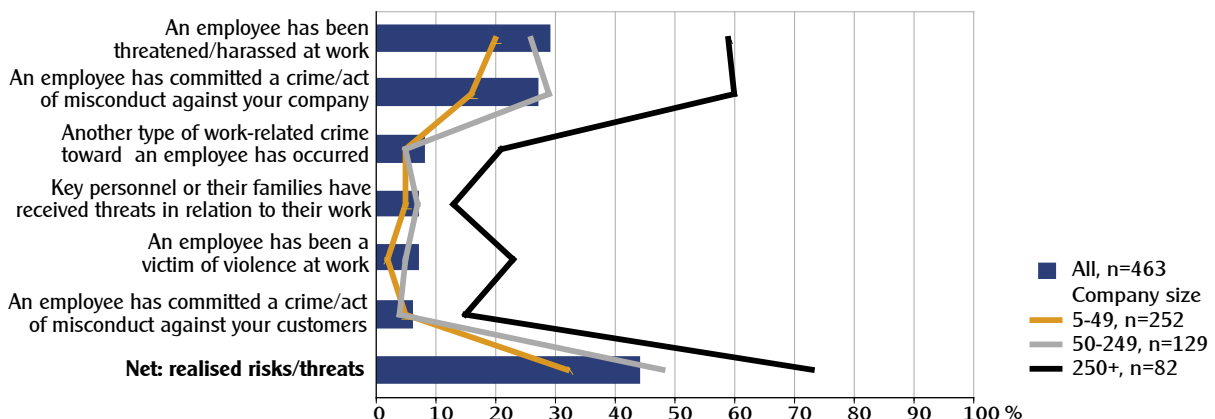
Seven per cent of all the companies in the survey stated that an employee of their company had been a victim of a violent act. However, threats of violence were clearly more common than actual acts of violence, since every third company stated that their employees had experienced threats at work. Violent or threatening situations arose in connection with, among others, meetings with drunk or intoxicated customers or in different burglary, seizure or petty larceny situations. The risk of violence is increased when an employee works alone or late at night. To some extent, violence can be reduced through training and technical safety measures. Monitoring equipment also assists in resolving violent crimes.

Key personnel often face security threats because of their position, wealth, visibility or the company's activities or field of business. Among the large companies, every eighth stated that key personnel or

*"In a small company, the significance of key personnel is great. It is not easy to create a deputy system."*

## Risks related to personnel

Realised risks/threats



their families had been threatened. The percentage was lower in small companies (5 %) and in medium-sized companies (7 %). Only half of the small companies (56 %) had a deputy system in place for key personnel. Of the large companies, four out of five (80 %) had preparations in place in case of the need to replace key personnel.

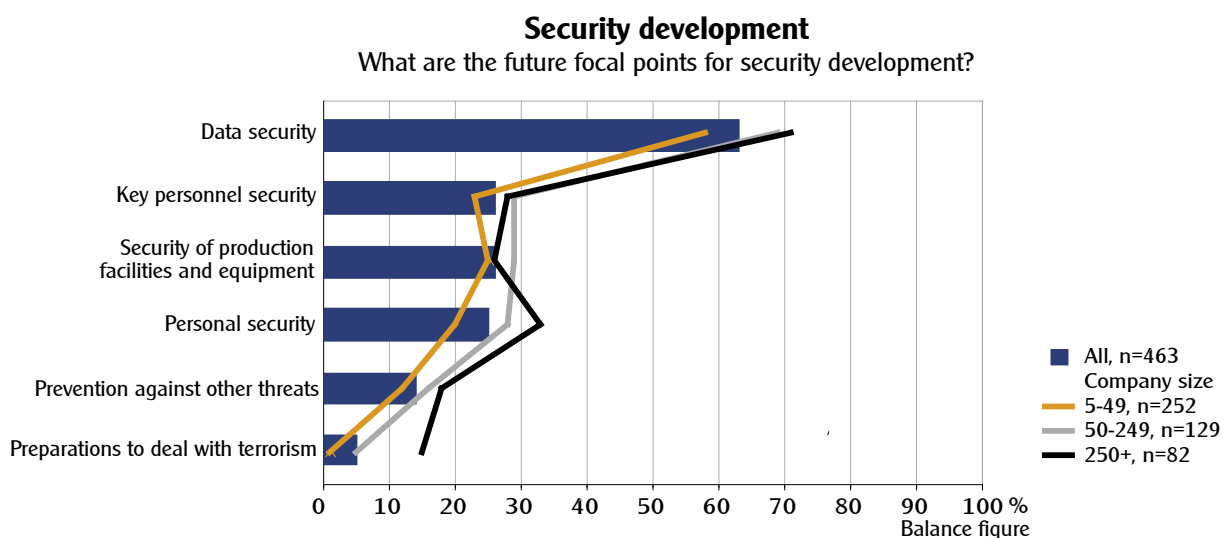
## Management shows the direction

The security culture of a company refers to the behaviour and attitude of the company's personnel towards security. A good security culture reduces security risks and supports a company's competitiveness. Risk prevention is most successful in a company where the management is committed to risk management. In four out of five companies surveyed, the management personally participates in security development. A lack of internal co-operation and co-ordination may also form a significant obstacle to corporate security,

because potential risks should be examined from the different viewpoints of all areas of operation. A quarter of the responding companies reported that the different departments within their company do not co-operate with each other when dealing with security issues. Only one third of the companies had incorporated corporate security as a part of their annual strategic plan, budget proposal and plan of action.

### **The amount of companies that do not receive information from the authorities on crimes and other threats**

- ▶ 73 % of small businesses
- ▶ 59 % of medium-sized businesses
- ▶ 27 % of large businesses



# Preventing crime and misconduct in business

## Unknown risks cannot be controlled

*"Nothing has ever happened to us."*

Before it can prepare for risks, the company must understand the risks that are related to their activities and operating environment. Risk assessment helps a company to evaluate the internal and external threats it may be facing. A thorough assessment that is regularly updated helps to guide risk management work. Only 38 % of the companies have carried out a documented risk assessment.

## Research method

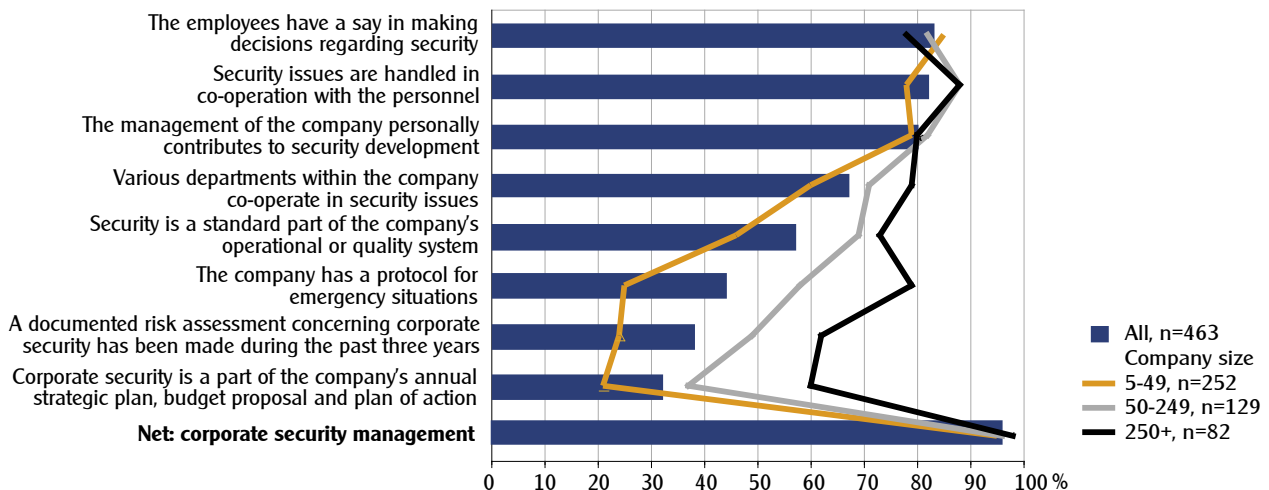
A total of 463 representatives of Finnish companies responded to the 'Corporate security – Criminal

risks and their management' survey conducted in September 2005. The nationwide survey enquired about crimes and acts of misconduct which have taken place in the companies, as well as what risk management measures the company had employed. The Central Chamber of Commerce of Finland and the Helsinki Region Chamber of Commerce drew up the report on the basis of the e-mail survey conducted by the Finnish market researcher Taloustutkimus Oy – TOY Research.

The responding companies represented the fields of services (43 %), industry (35 %), trade (15 %) and construction (7 %). Half of the companies were small in size, employing less than 50 persons. A quarter of the respondents (28 %) represented medium-sized companies with 50-250 employees. Large companies of more than 250 employees represented a fifth (18 %) of the respondents.

## Risks to business activities

Are the following statements true as they relate to the security management of your company?





**The Central Chamber of Commerce of Finland** is the central organization of 20 Chambers of Commerce, which have over 16,000 members. Membership is voluntary. The Chambers of Commerce promote free competition, market economy and free world trade. For more information, visit [www.chamber.fi](http://www.chamber.fi) and enter the homepage of the Central Chamber of Commerce of Finland.

Aleksanterinkatu 17, P.O. Box 1000  
00101 Helsinki, Finland  
Tel. +358 9 696 969, fax +358 9 650 303  
[www.chamber.fi](http://www.chamber.fi)

Dr **Kari Jalas**, Managing Director  
Tel. +358 9 6969 6618, fax +358 9 6969 6652  
[kari.jalas@chamber.fi](mailto:kari.jalas@chamber.fi)

Ms **Kaisa Saario**, Adviser  
Tel. +358 9 6969 6626, fax +358 9 650 303  
[kaisa.saario@chamber.fi](mailto:kaisa.saario@chamber.fi)



**The Helsinki Region Chamber of Commerce** operates in the capital region. The Helsinki Region Chamber of Commerce is the biggest Chamber of Commerce in the Nordic countries with over 6 000 member companies.

Kalevankatu 12  
00100 Helsinki, Finland  
Tel. +358 9 228 601, fax +358 9 2286 0228  
[www.helsinki.chamber.fi](http://www.helsinki.chamber.fi)

Mr **Heikki Perälä**, Managing Director  
Tel. +358 9 228 601, fax +358 9 2286 0228  
[heikki.perala@helsinki.chamber.fi](mailto:heikki.perala@helsinki.chamber.fi)

Mr **Panu Vesterinen**, Project Manager  
Tel. +358 9 228 601, fax +358 9 2286 0228  
[panu.vesterinen@helsinki.chamber.fi](mailto:panu.vesterinen@helsinki.chamber.fi)