Prevention

In order to prevent damages and losses caused by insiders, a comprehensive security concept is required.

This i.a. includes:

- Analysis of risks and weak points
- Continuous sensitisation of all members of the company
- Using your own staff's competence and motivation for the security concept
- Appointment of a security manager
- Security regulations for visitors and external companies
- Modern personnel management (staff selection and attending to staff)
- Monitoring
- Straight company guidelines

Contact us and make an appointment for sensitisation talks.

Your contacts

www.verfassungsschutz.de

www.verfassungsschutz-bw.de

www.verfassungsschutz.bayern.de

www.verfassungsschutz-berlin.de

www.verfassungsschutz-brandenburg.de

www.verfassungsschutz.bremen.de

www.hamburg.de/verfassungsschutz

www.verfassungsschutz.hessen.de

www.verfassungsschutz-mv.de

www.verfassungsschutz.niedersachsen.de

www.mik.nrw.de/verfassungsschutz

www.verfassungsschutz.rlp.de

www.saarland.de/verfassungsschutz.htm

www.verfassungsschutz.sachsen.de

www.mi.sachsen-anhalt.de/verfassungsschutz

www.verfassungsschutz.schleswig-holstein.de

www.thueringen.de/de/verfassungsschutz

Imprint:	Bundesamt für Verfassungsschutz für die Verfassungsschutzbehörden in Bund und Ländern
Pictures:	Fotolia
Print:	INFOX GmbH&Co. Informationslogistik KG, Troisdorf
DOI:	August 2010

Protection of the Constitution

Federal Republic of Germany
Federal States

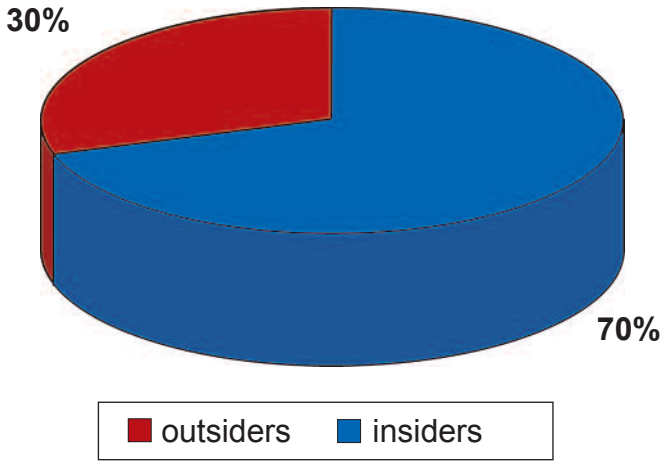
Humans as a security gap – The insider as the companies' most serious

Protection of the Constitution: neutral free of charge confidential

Situation

Company-specific expertise decides on market opportunities and on future chances. Espionage, theft, sabotage, corruption or IT-related crime by a company's own personnel are a threat posed to this competitive advantage.

The risk of falling victim to a loss of expertise due to insiders is significantly underestimated by most companies.



Potential threats

Exhaustive studies prove particularly small and medium-size innovative companies to be at risk. In many cases, there is only little security awareness. Company owners can hardly imagine that there is a possibility to be spied out by their own staff members.

Case studies

1. A fired staff member of an IT company copied the customer database for his new employer.
2. A staff member stole a notebook with sensitive internal data from a mechanical engineering company.
3. A trainee got hold of sensitive data regarding a technical project using a USB stick.
4. A guard took pictures of prototypes in order to sell them to competitors.
5. A staff member sold expertise not yet patented from the field of R&D to other countries.
6. Two senior staff members started their own business with a newly-developed product of their previous employer.

Perpetrators

Given their opportunities of having legal access and their inside knowledge of internal weak points, insiders can do more harm to companies than outsiders ever could. There is no limitation to any hierarchical level any more. Perpetrators can be found everywhere – starting off with the caretaker and ending with the senior manager.

Indicators

- Discontent at the workplace, lacking identification with the company
- Conspicuous curiosity
- Use of espionage means, such as image and sound recording devices or mobile data carriers
- Irregularities in personal environments (lavish lifestyle, signs of alcoholism, drug addiction, compulsive gambling or excessive debts)
- Discrepancies in career histories, e.g. applicants being overqualified or underqualified
- Dubious spontaneous applications
- Suspicious contacts with foreign states' representations or with competitors
- Exceeding access rights