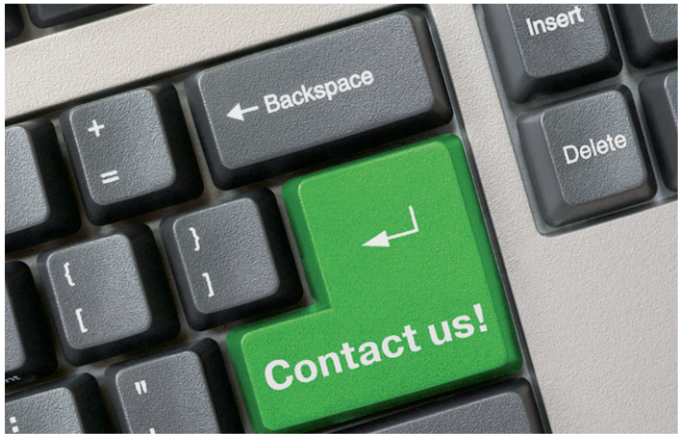
Recommended action

- Determine essential values/information
- Analyse risks and weak points while involving all staff members
- Create a comprehensive security concept including rights management
- Appoint a security manager
- Continuously raise all staff members' awareness and train them
- Establish safety rules for visitors and other companies
- Consistently apply and develop your security concept
- Promote the staff members' identification with your company

Do not hesitate to contact us and make an appointment for confidential awareness talks.



Your points of contact in economic security

initiative wirtschaftsschutz

Protecting values in a concerted effort

For additional information and your local contacts' communication data, please visit the website

www.wirtschaftsschutz.info

Imprint

Publisher: BfV (German federal domestic intelligence service) for the community of the domestic intelligence services of the Federation and the federal states

Pictures: © Nikolai Sorokin - Fotolia.com

DOI: March 2016

Domestic intelligence service

Federal Republic of Germany
Federal States

Economic Security

Dangerous insiders

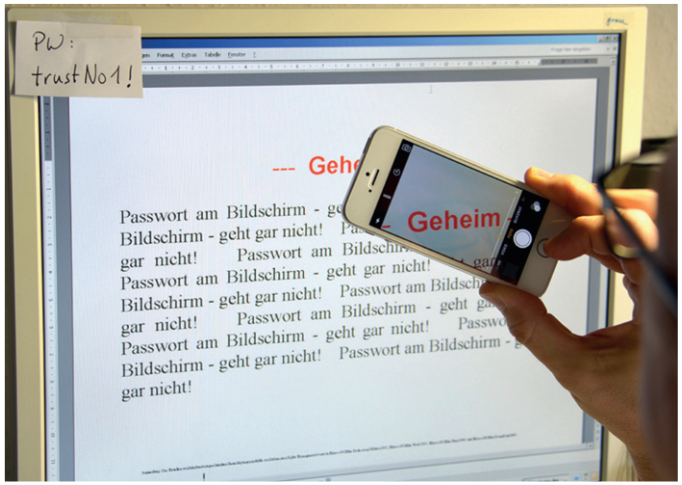
Humans as a security gap

Prevention through Dialogue and Information

Risk potential

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

Offences such as espionage, theft, sabotage, or corruption by a company's own personnel pose a threat to your know-how and to your competitive advantage.



Many company owners can hardly imagine having a perpetrator within their own ranks. Exhaustive studies prove particularly small and medium-sized innovative companies to be at risk. This is aggravated by an insufficient security awareness.

Case studies

- A dissatisfied staff member deliberately destroys storage media containing important know-how
- A fired staff member copies the customer database for his new employer
- A staff member steals a laptop with sensitive company data
- A trainee gets hold of sensitive data from a technical project using a USB flash drive
- A guard takes pictures of prototypes in order to sell them to competitors
- A staff member sells know-how not yet patented from the field of R&D to other countries
- Two senior staff members start their own business with a newly-developed product of their previous employer.

Perpetrators

Given their opportunities of legal access and their inside knowledge of internal workflows, insiders can do enormous harm to companies.

Regardless of their status within the company, anyone can become a perpetrator – starting off with the caretaker and ending with the senior manager.

Indicators

- Discontent at the workplace, lacking identification with the company
- Conspicuous curiosity
- Irregularly introducing and using mobile devices or storage media
- Irregularities in personal environments
- Suspicious contacts with foreign states' representations or with competitors
- Attempts to extend rights of access granted
- Exceptional working hours