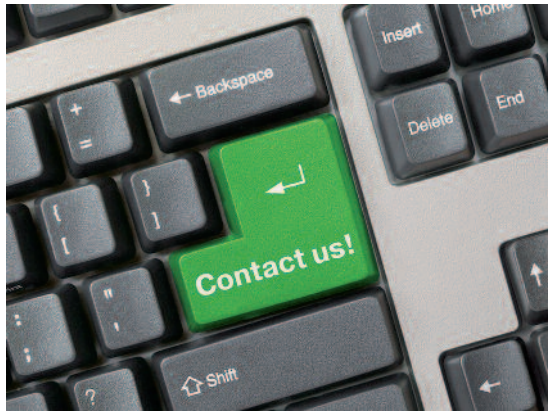
In the event of damage, ask yourself i.a. the following questions:

- Has sensitive corporate know-how been stolen?
- May further possibilities of entry or access arise for the perpetrators?
- Are there any indications of insider knowledge or a staff member being the perpetrator?
- Are there any indications of a manipulation regarding technical equipment of your company?
- Is there any conspicuous relation between the time of the theft and a company-related event?

Contact us and make an appointment for confidential 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:	December 2011

Protection of the Constitution

Federal Republic of Germany
Federal States

Industrial espionage through theft and burglary

Burglary/theft and industrial espionage?

Your company got broken into? Have staff members been robbed in the context of their profession? Have you ever asked yourself if the aim was not to get the stolen items, but to obtain your know-how?

The Offices for the Protection of the Constitution hold information about methods of foreign intelligence services or competitors aimed at getting the know-how of German companies. Burglary and theft range among them.

Our sensitisation talks with companies have confirmed that these offences are often not perceived as being relevant in the context of espionage.

Case studies

- In a multi-storey company building, the perpetrators purposefully broke into the eighth storey and stole the hard drives of several notebooks. However, they ignored other profitable pieces of booty such as the notebooks themselves, flat screens, and cash.

- In another case, the perpetrators broke into a company building and directly went to the IT area – as could be proved by their traces – where they tried to download company data from the server.

- There are more and more cases of notebooks, smart phones, and company documents being stolen during trade fairs, at airports and railway stations, or from company cars. It is not seldom that valuable know-how of companies gets lost during such incidents.

- Most insidious are those cases where nothing seems to have been stolen at all. If traces of a burglary are all you notice, it is possible that either listening devices like bugs, cameras, or Trojans have been placed somewhere, or that data or copies have been walked off with unnoticed.

Experiences

As a rule, investigations have been focused on theft or burglary in the described cases. Only after a sensitisation by the Offices for the Protection of the Constitution was the actual purpose revealed: an assault on the company's know how.

It is often difficult to reveal an involvement of foreign intelligence services in such cases, especially when the attack dates back a while. This is why it is vital to contact the Offices for the Protection of the Constitution as soon as possible.

Also with regard to potential in-house perpetrators it is important to react quickly in order to prevent a further loss of sensitive company know-how.