

Background

If a business or country possesses advanced know-how or technology, someone else will try to steal or copy it. During the first industrial revolution, the Americans were desperate to obtain cutting edge British technology to mass-produce textiles. They had cotton but no machines of their own. It was illegal for textile workers to travel to America but in 1789 English factory supervisor Samuel Slater did just that. Almost single-handedly he created the American textile industry by building machines from memory.

So industrial espionage has always been with us, but who are today's spies? You can forget ninjas breaking into heavily guarded factories in the dead of night. The reality is quite different and frequently the crime is digital and knowledge-based rather than the theft of a physical object. More often the 'spy' is an employee, past or present, or a seemingly innocent visitor. They may also be students on *internships or sponsored by rival companies or foreign governments. In one case Li Li Wuang a Chinese student was arrested for stealing commercial secrets from the French company where she was an *intern. Confidential files had been wiped off the firm's computers only to be discovered on her PC. Luckily for her there was no proof that the information had been sent so she was released and allowed to continue with her studies. A 26-year-old Hungarian was not so lucky. He was sentenced to three years in prison for breaking into the Swedish company Ericsson's intranet system. This type of crime even reaches the world of Formula 1 racing. Former Ferrari employees were found guilty of industrial espionage by gaining unauthorized access to Ferrari's computer system.

So what can firms do to protect themselves from breaches of security?

Glossary

**intern* = a student on work experience

**internship* = a period of work experience for a student

These are some pieces of advice that security experts often give:

- First of all, they should take care over who they employ and run thorough background checks.
- They should protect sensitive data behind closely guarded passwords that are changed on a regular basis.
- R&D areas should be behind closed doors and away from curious eyes.
- If you do have guests, politely ask them to leave their mobiles outside to prevent anyone taking photographs of machinery, processes or prototypes. A state-of-the-art design can be taken in a split second.
- Anti-spyware should be installed and monitored on your computer system.
- Most firms would draw the line at banning mobile phones, but staff should be forbidden from bringing in memory sticks or any kind of external drive into the office.
- People should only have access to data on a need-to-know basis.
- One consultant controversially suggests keeping any foreign trainees well away from sensitive material however sweet or innocent they appear.

On a personal level we can all do things like keeping office drawers locked and password-protect access to our computers. Incidentally, never use the name of a pet, loved one, or favourite team as passwords: they are child's play for any competent hacker to break. The spy can also be the 'colleague' you chat to and share your ideas with on a professional bulletin-board. Never ever download a file from a seemingly well-meaning contact – it could contain a Trojan Horse that gives access to all your data. Before you know it he has stolen your personal details and accessed sensitive information. You have been warned!

Exercises

1 Work with a partner. Discuss these questions.

- 1 How strict is security where you work?
- 2 Are there areas that are forbidden to most members of staff?
- 3 Have there ever been problems with security?

2 Read the first two paragraphs of the text and answer these questions.

- 1 What important knowledge was transferred to America?
- 2 Who usually carries out industrial espionage?
- 3 Who is often behind the crime?
- 4 What was a Chinese student accused of doing by a French firm?
- 5 Why was a Hungarian man less lucky?
- 6 What happened at Ferrari and who was responsible?

3 Imagine you are telling someone about the first part of the article. Summarize the type of crime and the type of criminal.

4 Work in pairs or groups and brainstorm the different ways that companies can protect themselves from industrial espionage. Make a list.

5 Read the rest of the text. How many ways of preventing espionage did you predict? Did you come up with other ways that are not dealt with in the article?

6 Match 1–6 to a–f to make collocations from the text.

- | | |
|----------------|---------------|
| 1 industrial | a file |
| 2 unauthorized | b of security |
| 3 breach | c access |
| 4 rival | d espionage |
| 5 sensitive | e company |
| 6 confidential | f data |

7 Match the phrases in *italics* to their definitions.

- 1 If someone does something *single-handedly*, they do it ...
a with one arm. b on their own.
- 2 If something is at the *cutting edge*, it is ...
a at the front of research and development. b is dangerous to touch.
- 3 If something is *state of the art*, it ...
a belongs in a museum. b presents the highest level of development for its time.
- 4 If you *draw the line at* something, ...
a you refuse to do it. b you agree to do it.

8 Look back at the text and choose three words that you could use in your day-to-day work.

9 Imagine you are in charge of security at a high tech firm. What do you tell colleagues who say the following?

“ I belong to this really useful bulletin board – it’s great to swap ideas with other colleagues in a friendly and open atmosphere. After all, we’re all scientists, aren’t we? ”

“ I’ve got this really sweet trainee who is here for the summer. I don’t know what I would do without him. He has even offered to work late when everyone else has left the office. ”

“ There is a group of possible investors coming to have a look around this afternoon. Do you think it will be all right if I let them have a look at the prototype – I’d be interested in hearing their views. ”