

**S**pying is one of the oldest tricks in the book – if you want valuable information, pinch it off someone else. And the revolution in global communications and technology has put today's espionage firmly in the realm of cyberspace.

The UK's National Security Review recently claimed the threat of "attacks on UK cyberspace by hostile states, or large-scale cyber crime" was one of the top two risks to the country, international terrorism being the other. It says: "Government, the private sector and citizens are under sustained cyber attack today, from both hostile states and criminals. They are stealing our intellectual property, sensitive commercial and government information, and even our identities, in order to defraud individuals, organisations and the government." Unless action is taken, this threat could become even worse, the report says.

However, computer forensics firm Stroz Friedberg's managing director, Seth Berman – a former assistant US attorney in the computer crime unit of Massachusetts – thinks few companies outside the defence and financial services sectors take the risk seriously. "They don't realise until after they've become a target how serious and damaging it can be," he says.

Companies generally see cyber attacks as a remote risk that is expensive to defend against. Yet the risk managers *StrategicRISK* spoke to – all of whom wished to remain anonymous – said the threat of cyber attack or cyber espionage was something their company took very seriously. "For many, cyber risks will be a number one priority," confirms KPMG head of audit risk and compliance David Defroand.

The reason for this divergence in opinion is that organisations, individuals and governments are exposed to different levels of risk, depending on the value and attractiveness of the information or assets they hold. Companies operating in strategically important industries or hi-tech areas, such as nuclear, defence and energy, are the most vulnerable, according to Massimo Cotrozzi, an IT risk expert with security consultancy KCS.

### Cyber risk hotspot

One of the most high-profile cyber risk hotspots is China. Companies with operations, subsidiaries or valuable secrets in China are firmly in the firing line. Several recent attacks have originated from the country and the Chinese government is widely regarded, although not officially condemned, as a sponsor of cyber crime. It is rumoured that China stole Japan's high-speed rail technology to use in its own rail expansion plans, for example.

# Know your enemy

Computer crime is becoming ever more sophisticated and widespread. **Nathan Skinner** traces the scale of the problem and asks whether businesses are switched on to solutions

The global cost of cyber crime is put at \$1 trillion (€757bn) a year. There are two types of cyber attack. The first involves generalised viruses that exploit so-called 'zero-day' weaknesses in applications – vulnerabilities unknown to even the software developer. Good-quality virus software and up-to-date security patches are required to protect against this.

The second type, which has developed over the past few years, involves targeted hacking aimed at stealing information such as credit card details or intellectual property. Hackers today are highly professional and operate almost with impunity online. Some even work for the military or government – conspiracy theorists believe the MI6 officer found dead in a London apartment recently may have been a hacker.

Companies should be wary of being spied upon by competitors looking to steal trade secrets or get the upper hand in a contract bidding war. One corporation could be spying on another to gain access to a secret product design, for example. Berman thinks this is the risk companies are least prepared for. In Europe, such activity is rare because the consequences of being caught are serious, he says. But in China there is almost no legal recourse and the line between government and business interests is blurred. Some even say this kind of spying on western competitors is encouraged.

A recent investigation by the Canadian-run organisation Information Warfare Monitor and

US-based watchdog Shadowserver suggests that Chinese cyber spies are systematically targeting and compromising computer systems, particularly in India and several other countries as well as the offices of the Dalai Lama and the United Nations.

Investigators uncovered large quantities of stolen material belonging to governments and businesses, including encrypted diplomatic letters and secret documents. The attackers made use of social media systems such as Twitter, blogs and Yahoo Mail to steal the information. Although the identity and motivation of the attackers remains unknown, the report provides evidence they operated or staged their operations from China's Chengdu Province.

"Clearly, this investigation and our analysis tracks back directly to China, and to known entities within the criminal underground of China. There is also an obvious correlation between the victims, the nature of the documents stolen and the strategic interests of the Chinese state," said the Shadowserver report.

### European trail

China is not the only culprit. In October, a cross-border investigation involving officers from the USA, UK, Ukraine and the Netherlands led to several arrests in one of the largest cyber criminal cases ever launched.

Using a Trojan horse virus known as Zeus, hackers in eastern Europe infected computers around the

## Phone hacking

Criminals are using technology to spy on companies by hacking into mobile phones and listening in on calls. The issue caused a stir in the UK when national newspaper the *News of the World* allegedly hired private investigators to illegally gain access to mobile phone messages, generating big stories,



including some about the Royal family. By March 2010, the paper had spent more than £2m (€2.38m) on settlements with victims of phone hacking.

A report by information management specialist Ponemon Institute revealed that businesses are putting themselves at risk of mobile phone interception. According to the survey, 67% of IT professionals are not confident that confidential information conveyed during cellphone conversations is secure in their organisation.

In response to this threat, some companies have begun using technology to secure their voice calls. Manchester-based Henderson Risk, for example, which has a subsidiary Kosovo and provides risk management services to international banks, uses Cellcrypt Mobile to enable staff to discuss commercially sensitive issues securely. Other solutions include PhoneCrypt from SecurStar, Cryptophone from Berlin-based GSMK and Gold Lock, which is licensed by the Israeli military.

world. The virus was spread via an e-mail and, when opened, installed itself on the victim's computer, capturing passwords, account numbers, and other data used to log onto online bank accounts. The hackers used this information to make unauthorised transfers of large sums of money, often routing the funds via a network of 'money mules'. See our infographic opposite for how the cyber crime worked.

Weysan Dun, FBI special agent in charge of the investigation, said: "International tolerance for this kind of criminal activity is decreasing. Our partners overseas are dealing more aggressively and effectively with cyber crime than ever before."

## Homegrown hackers

But KCS warns that China is protecting an ever-increasing web of homegrown hackers, capable of cyber warfare and industrial espionage. "Chinese hackers – many of them young – are being offered large financial awards to infiltrate western computer systems, with military targets in particular being attacked," said the consultancy in a statement. "Some of the hackers are backed directly by government organisations, while others are tolerated by the Chinese authorities, which turn a blind eye."

KCS claimed to have contact with "those most active in targeting critical European and US infrastructures" through its Asian offices, as well as being aware of attack methods.

"Our intelligence sources have disclosed that some of the hackers are being requested to specifically attack military targets in the west, which is a cause for alarm," says KCS chief executive Stuart Poole-Robb. Within the next 18 months, he says, Chinese hackers will easily be able to exploit weaknesses in western computer systems – mainly military command centres and commercial targets such as phone producers, aerospace, health and nuclear organisations.

"Recent intrusions, we have learned, have been performed through 'botnets' – a collection of software agents or robots – which run autonomously and automatically," he adds.

Even though many companies are aware of these risks, they are not employing the right techniques and managing the risk appropriately, says Cotrozzi. "Know your enemy and know the value of the assets you are defending," he says. "Then invest in the appropriate level of mitigation activities."

It is often the case that the IT manager responsible for security cannot secure the board's backing for the right level of investment, he adds.

The bigger a company, the more likely it is to have measures in place to combat cyber espionage. Rolls Royce recently won a lucrative \$1bn contract to supply jet engines to China Eastern Airlines so, given the value of its technology, it is no doubt well aware it is a target for espionage, both old and new.

Those not taking the risk seriously do not consider themselves a target. And as hackers become more sophisticated and able to cover their tracks, the problem is growing. A company may be the victim of an attack without even knowing it. ■

Nathan Skinner is editor of StrategicRISK

