OneSecurity

E-espionage

What risks does your organisation face from cyber-attacks?

Contents

E-espionage: a real threat to all businesses

What is E-espionage?

Put simply, e-Espionage is unauthorised and usually criminal access to confidential systems and information for the purposes of gaining a commercial or political advantage.

The UK Centre for the Protection of National Infrastructure (CPNI), summarises the risk as follows:

"The espionage, or spying, threat did not end with the collapse of Soviet communism in the early 1990s. Espionage against UK interests continues from many quarters"

In the past, espionage activity was typically directed towards obtaining political and military intelligence. This remains the case, but in today's high-tech world, the intelligence requirements of a number of countries also include new communications technologies, IT, genetics, aviation, lasers, optics, electronics and many other fields.

The threat against UK interests is not confined to the UK itself. A foreign intelligence service operates best in its own country and some may therefore find it easier to target UK interests at home, where they can control the environment and where the UK traveller may let their guard drop."

Source: http://www.cpni.gov.uk/Threat/summary-221.aspx

When you hear the term 'espionage', what springs to mind? If it's James Bond, then you need to think again. Today, the risk of espionage is current and concrete for all organisations worldwide, across both the private and public sectors. A major driver behind this threat is the growing reliance on internet-enabled computer systems for storing, processing and communicating business-critical digital information across organisational boundaries, and the increase of telecommunications across the Internet.

These trends have given rise to a new and specific term for the risk that confidential information may be compromised or stolen by external criminals: 'E-espionage'. A definition of this risk is contained in the accompanying information panel.

Every minute of every day, a growing number of well-resourced and highly sophisticated cyber-criminals from across the world are seeking to gain unauthorised access to valuable data held by companies and governments. And the increasingly interconnected and open nature of today's internet-enabled corporate systems is helping to boost their opportunities.

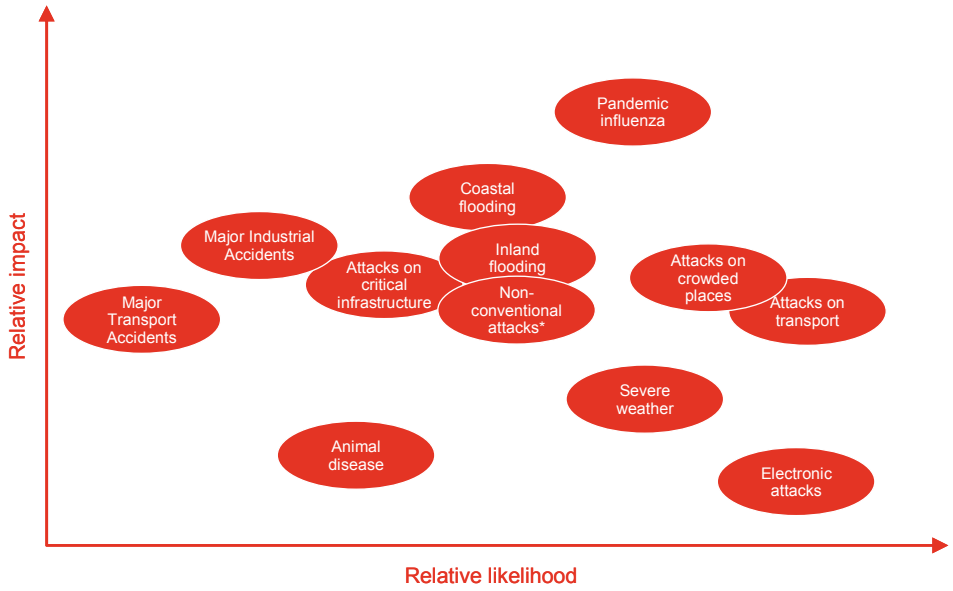
Sounding the warning

The authorities are very aware of the risks, and are urging businesses to take action. In late 2007, Jonathan Evans - the Director-General of MI5, and to whom Centre for the Protection of National Infrastructure (CPNI) is accountable - sent a confidential letter to 300 UK business leaders at banks, accountants and legal firms, warning them of a co-ordinated, web-based E-espionage campaign against the UK economy. And, as MI5 points out on its website: "Intelligence services…are targeting commercial enterprises far more than in the past."

As a result, the threat of electronic attacks is very real, both for individual companies and for critical national infrastructure such as power, water and financial institutions. This trend was further underlined by the UK Cabinet Office when it published the first National Risk Register in November 2008, as part of the National Security Strategy. The register sets out the Government's assessment of the likelihood and potential impact of a range of different risks that may directly affect the UK.

As Figure 1 shows, the register ranks electronic attacks as the second most pressing risk for the UK, narrowly behind attacks on transport infrastructure. And while the risk of electronic attacks was accorded a relatively low 'impact' rating, this will inevitably rise over time as the reliance on internet-enabled systems and networks increases in all areas of the economy. Also, as we will discuss in this paper, one of the key problems with E-espionage is the difficulty of establishing when and where it has happened, and what its effects actually are.

Figure 1: An illustration of the high consequence risks facing the United Kingdom



Source: National Risk Register, UK Cabinet Office

"Social malware is unlikely to remain a tool of governments. Certainly organisations of interest to governments should take proper precautions now, but other firms had better start to think about what it will mean for them when social malware attacks become widespread. What Chinese spooks did in 2008, Russian crooks will do in 2010, and even low-budget criminals from less developed countries will follow in due course."

The snooping dragon: social-malware surveillance of the Tibetan movement, University of Cambridge, March 2009

A strategic business issue

Traditionally, Boards have tended to regard the security and integrity of their corporate data as a matter for the IT function. However, the increasing threat and the rising impact of possible breaches mean the prevention and detection of E-espionage should now be on every Board's agenda. Those that fail to focus on it are putting the very future of their organisations at risk.

To gauge your business's readiness and ability to manage the risk of E-espionage, try asking yourself a few questions – such as:

1. Is the threat of E-espionage on your corporate risk register, and/or discussed in your Annual Report?
2. Do you know how many security incidents you have suffered in the past year, and the nature of those incidents?
3. Are you monitoring your information systems and their exposure on a 24/7 basis?
4. Do you have a security strategy and governance approach that is aligned with your business strategy?

If your answer to any of these is questions is 'no', then you need to read this paper.

How big is the threat?

Malware: a powerful opponent

Malware – or 'malicious software' – of the type exposed in the Ghostnet investigation is a powerful tool for cyber-criminals looking to engage in E-espionage. For example, it can invade a computer undetected and take control, targeting and extracting sensitive documents. It can even turn on the camera and audio-recording functions of an infected computer, enabling the criminals to monitor what is going on in the room. The investigators were unable to establish whether these capabilities had been used in this case.

As the recent official warnings indicate, the threat of E-espionage is real – and is rising all the time under the impact of several factors. One of these is the current economic downturn and people's resulting uncertainty over their jobs and financial security. So the recession is increasing the motivation and incentives for people to commit cybercrime, including fraud and E-espionage.

At the same time, corporations' increasing reliance on global enterprise-wide systems can heighten the danger still further. This is because these centralised core systems effectively widen the range and sensitivity of the data that may be accessible to anyone breaking in – thereby boosting companies' risk exposure.

In early 2009, Canada-based Information Warfare Monitor (IWM) published a report called *Tracking GhostNet: Investigating a Cyber Espionage Network,* detailing the findings of a 10-month investigation into a global electronic spy network that has infiltrated computers in various government offices around the world. The report said the network had used malware (see information panel) to infiltrate 1,295 computers in 103 countries, including systems belonging to foreign ministries and embassies and those linked with the Dalai Lama.

And in March 2009, a study from University of Cambridge entitled *The snooping dragon: social-malware surveillance of the Tibetan movement,* documented 'malware-based electronic surveillance of a political organisation by the agents of a nation state'. The authors highlighted that the implications go far beyond government bodies, commenting: "This report is of importance not just to companies who may attract the attention of government agencies, but to all organisations. As social-malware attacks spread, they are bound to target people such as accounts-payable and payroll staff who use computers to make payments. Prevention will be hard."

This message was underlined in April 2009, when the Wall Street Journal reported that 'cyber spies' had penetrated the US electricity transmission grid and implanted software that could be activated to disrupt the system. The report quoted Dennis Blair, Director of US National Intelligence, as telling lawmakers: "Over the past several years, we have seen cyber attacks against critical infrastructures abroad, and many of our own infrastructures are as vulnerable as their foreign counterparts…A number of nations, including Russia and China, can disrupt elements of the US information infrastructure."

What is at risk?

So the threat of E-espionage is growing. But what is at risk for companies that fail to manage it effectively?

The first step towards establishing this is to take stock of your current management processes and attitudes towards E-espionage risks. Traditionally, Boards have not even had this issue on their radar screens, and have tended to pigeonhole it as a matter only for IT. The results of this mindset are that security against E-espionage attacks is often 'bolted on' as an after-thought rather than being built into the initial business decision, and that security teams are commonly not involved up front

Experience shows that this approach is not just misguided, but positively dangerous for the organisation concerned. As the studies and media reports described above demonstrate, it is potentially easier today for criminals to steal information from a business – or even compromise a country's national infrastructure – through hacking rather than mounting a physical attack. So E-espionage should be on the strategic Board agenda, and embedded into decision-making and systems projects from the ground up.

Confidentiality, integrity and accessibility: the key elements of information security

'Information security' involves protecting information and information systems from unauthorised access, use, disclosure or disruption. The three pillars of effective security are confidentiality, integrity and accessibility – often summarised as 'CIA'. Each of these three elements needs to be kept constantly in view for systems to do their job. However, there has historically been a tendency for businesses to place too little emphasis on the 'I' (integrity), with the focus mainly falling on the need for data to be accessible and secure from theft. However, the implications of data being altered without authorisation means integrity should always be taken fully into account alongside the two other elements.

An expanding array of business-critical assets and operations

This need is becoming all the greater because E-espionage now poses a threat not just to a business's reputation, but to its very existence. And the onset of the global economic downturn is now magnifying this threat still further.

In today's knowledge-driven marketplace, a company's core intellectual property (IP) is often pivotal to the value of its business. And increasingly this business-critical IP is stored and shared in digital form on enterprise-wide systems, meaning that E-espionage raises the risk of a company's core assets and marketplace being literally stolen overnight. Preventing this from happening by ensuring IP is well-protected is clearly a Board-level duty.

If cybercriminals do gain access, the impact can be disastrous. For example, a company in a sector such as defence, electronics or pharmaceuticals might find its products have been reverse-engineered without its knowledge, and are now being counterfeited and sold at a fraction of the price. What is more, the damage from an incursion can extend beyond the potential loss of data, to encompass threats to data integrity (see information panel on 'CIA'). Consider the impact of financial, regulatory or safety-critical data being modified by a criminal seeking to undermine an organisation.

A further consideration that can increase the risk and exposure to E-espionage is the growing use of outsourcing and offshoring of operations. While these activities may appear non-core or commoditised, they often have access to and use core business data, including personal information on customers. To manage E-espionage risk effectively, an organisation must be sure that its outsourced and offshore operations meet the standards of its internal enterprise processes across all three aspects of 'CIA'. If not, the criminals seeking out the weakest link in the business's value network may well target those operations.

"Considering that modern life is reliant upon technology, from key infrastructure like water systems and transportation to banking services and power grids, the scope of cyberspace is vast, extending beyond any physical or geographic barriers. Thus, warfare in cyberspace has unprecedented potential to damage nation-states and poses a real threat to modern life."

Bank of America/Merrill Lynch report, February 2009

Vulnerability varies by industry

Boards should also bear in mind that the exposure and risk varies between different industries. In the National Risk Register, the UK Cabinet Office comments: "The risk and impact of electronic attacks on IT and communication systems varies greatly, according to the particular sectors affected and the source of the threat. Electronic attacks have the potential to export, modify or delete information or cause systems to fail."

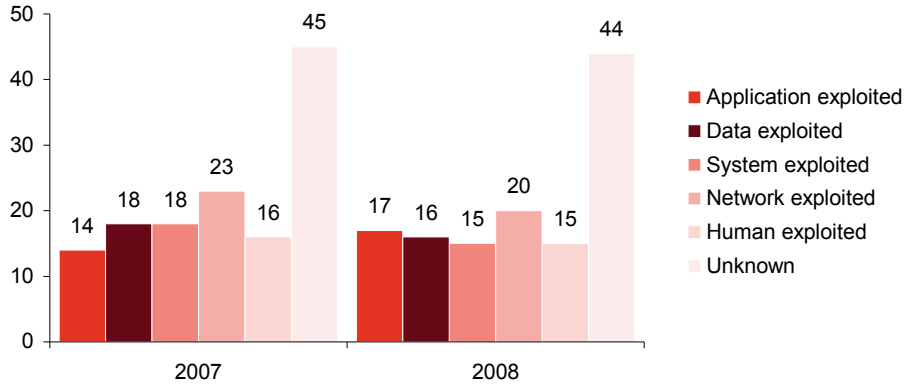
Clearly, an organisation could find itself effectively shut down overnight if its business-critical transmission networks are disrupted. But many other businesses are also highly vulnerable over a longer timeframe, given the dependence of their bottom line on their IP. So investors and other stakeholders across all industries are becoming more aware of this growing risk, and are increasingly demanding evidence in investor presentations and Annual Reports that managements are addressing and managing it.

Are companies aware and ready to act?

As businesses worldwide face up to the challenges posed by the rise of E-espionage, questions are being raised about their understanding of the risks and readiness to act. Our research and wider experience suggest that many organisations have yet to grasp the enormity of the threat – and need to take significant steps before they can start to tackle it effectively.

PwC recently conducted research into IT security among more than 7,000 CEOs, CFOs, CIOs, CSOs, vice presidents and directors of IT and information security from 119 countries. The study found that more than three out of 10 respondents worldwide cannot answer basic questions about the risks to their company's most sensitive information – with fully 35% admitting they do not know how many security incidents have occurred.

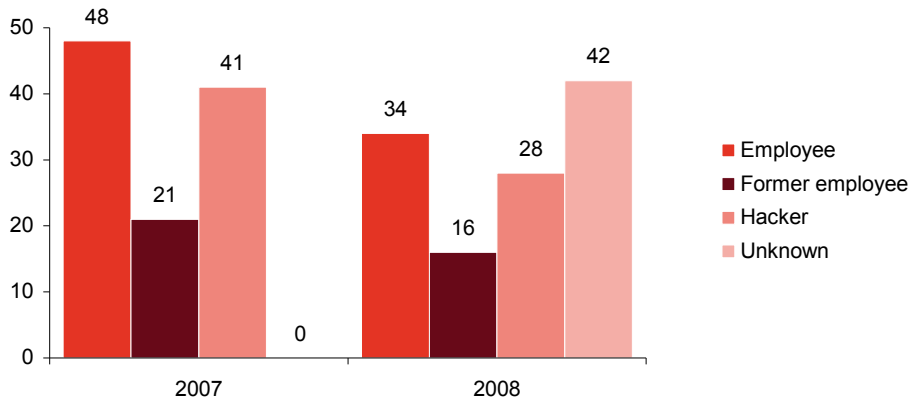
Figure 2: Types of security incidents



Source: PwC Research

Even where respondents are aware that they have had security incidents, many do not know what type of incidents they have suffered, with 44% admitting they lack this information (see Figure 2). This finding is disturbing, since such information is fundamental to any effective strategy for managing security risks.

Figure 3: Source of security incidents



Source: PwC Research

There is a similar lack of awareness about the sources of security incidents that have taken place. In our 2008 research, as in 2007, the most common sources remain current employees, former employees and hackers. As Figure 3 shows, all three categories appear to have declined this year.

Does this means the risks from these sources have really receded? Unfortunately not. This is the first year in which we have offered “don’t know” as a potential response to this question – and over two-fifths (42%) of all respondents selected this as one of their answers. This finding is backed up by other research studies and media stories. For example, it has been reported that most users of the computers compromised by Ghostnet were unaware of the breach.

“There is a known risk to commercially valuable and confidential information in some government and private sector systems from a range of well resourced and sophisticated attacks. Electronic attack may be used more widely by different groups or individuals with various motives… IT systems in government departments and various organisations, including elements of the national infrastructure have been and continue to be attacked to obtain the sensitive information they hold. Some of these attacks are well planned and well executed.”

UK Cabinet Office – National Risk Register

Knowing your enemy

This lack of specific management information about the number, nature and source of breaches is a worrying finding. If your business does not know about your attacks or level of exposure, it is impossible to create an effective strategy to address them, or to build a business case for investments in security.

This difficulty is compounded by the covert nature of E-espionage activities, and the fact that it is often very hard to establish where attacks have come from. The whole area of E-espionage detection and prevention is an arms race where the cyber-criminals have access to much of the best brainpower and technology, and are always pushing ahead. These criminals are smart, well-funded and adept at covering their tracks. Attempts to track down and tackle them can also come up against legislative and political hurdles, because E-espionage transcends national borders and national governments are often believed to be behind it.

However, these practical considerations are not valid reasons for failing to protect your business against E-espionage. This is a real and expanding area of risk that Boards have a duty to tackle. We will now look at how they can do this.

Fighting the threat: next steps for companies

In PwC's view, the threat of E-espionage should be one of the top issues addressed by today's Boards. However, there are many steps companies can take today to meet this challenge and mitigate the risks.

The first step is to conduct a **risk assessment** to establish the size, number, nature and source of the attacks to date, gauge the current vulnerabilities, and assess the resulting impact on your business. This will include asking key questions, such as what are the most critical digital assets, and which ones would or could people steal or compromise, and how.

The information from this risk assessment provides the basis for **formulating a security strategy and appropriate budgeting** to execute it. Without a carefully-considered security strategy in place, your business risks spending its time and resources on fire-fighting as problems emerge. A strategy enables the organisation to stay on the front foot, anticipating and closing off areas of vulnerability before the cyber-criminals attack. It also supports regular ongoing assessments of incidents, threats, risks and vulnerabilities

Crucially, your security strategy needs to be **aligned with your business strategy**. For example, if your organisation is planning to boost its proportion of sales through online channels, then preventing and detecting E-espionage must be an integral element built in to the system specifications from day one – not added later as a bolt-on. When formulated and implemented properly, the security strategy can become a business enabler by building trust among stakeholders, and supporting sustainable growth at lower risk

Once the strategy is in place, companies can use a **broad range of tools** to mitigate risk, refine the strategy and stay ahead of the cyber-criminals. Anti-espionage technology is advancing apace, and should be evaluated. Training and awareness-raising among staff are further worthwhile investments, ensuing that staff know the warning-signs of a breach, and the processes that should be followed to prevent one. It is also important to ensure the current security processes are still appropriate and being followed rigorously.

A checklist of key questions

To help you assessing and tackle your E-espionage risks, here is a checklist of ten key questions to ask:

1. Do you know the scale, number, nature and source of the incidents you have suffered to date?
2. Have you clearly identified what are your business's most valuable assets and which ones are most at risk from attack?
3. What would be the business impact of information/assets being stolen or compromised?
4. What is your strategy to manage, mitigate and minimise this risk?
5. Do you discuss this risk with investors and in the Annual Report?
6. What processes and technologies have you put in place to execute your security strategy?
7. What investment are you making to put these in place and ensure they remain effective?
8. How often do you reassess the risk and the strategy to manage it?
9. What new threats to your business are emerging in the E-espionage arena?
10. Have you educated and trained your staff to recognise and respond to the issue?

A call to action

Having answered these questions, you will find that the challenges and requirements for your strategy will be much clearer. And the key to success is maintaining a clear and rigorous focus on this risk at Board level, rather than pigeonholing it as an issue purely for IT. Today, global E-espionage is a major business risk, not just a technological curiosity – and every Board needs to treat it as such.

For more information about how PwC can help you manage the risks of E-espionage, please contact:

William Beer, Director
PricewaterhouseCoopers LLP
email: william.m.beer@uk.pwc.com
mobile: +44(0) 7841 563890

Neal Ysart, Senior Manager
PricewaterhouseCoopers LLP
email: neal.ysart @uk.pwc.com
mobile: +44(0) 7740 92312

About the authors

William Beer

William is a Director in the Risk Assurance Services group and has over 20 years of broad international experience at multinational IT companies. He has worked extensively in IT services, security environments and with security technologies.

Additionally William has focused on information security including security intelligence services, managed security services, data compromise and computer crime. Other areas that he specialises in include information security incident management, security architecture, security governance and risk management. William provides specialised quality assurance work and is the chair of the OneSecurity leadership team.

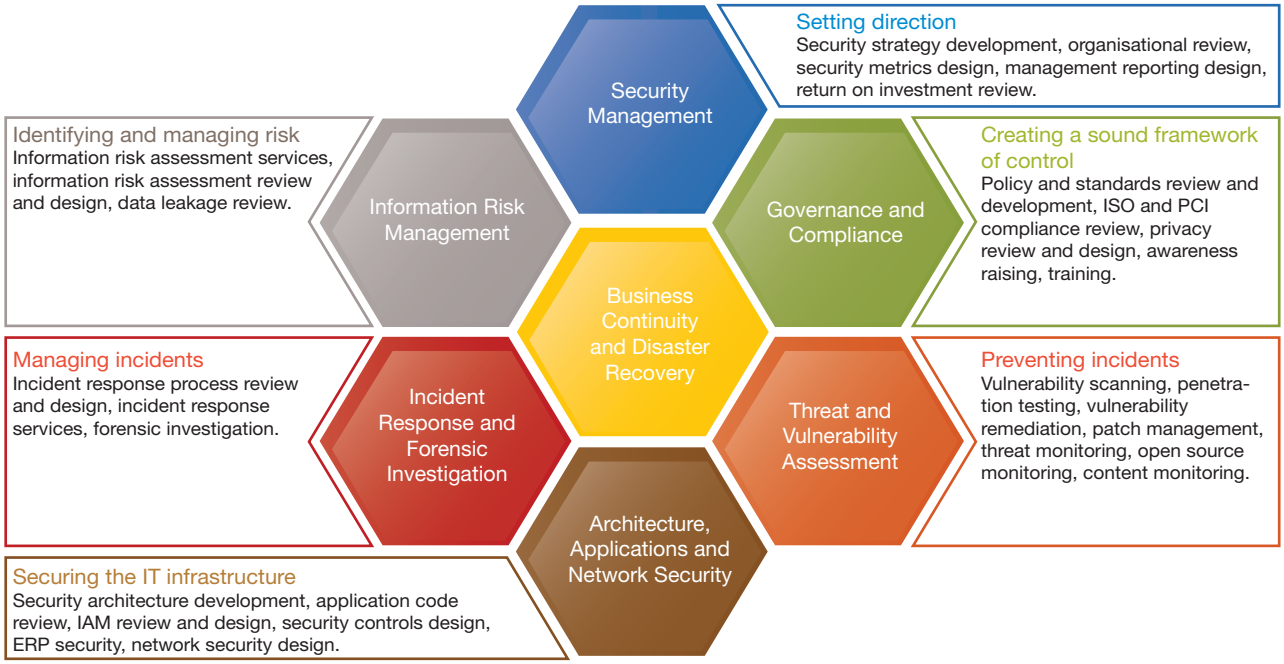
Neal Ysart

Neal is a Senior Manager in the Forensic Technology Solutions group and since joining PwC in 2000, has been involved in the development and delivery of a range of technology risk-based services for a number of organisations. Prior to joining the firm he had 17 years public sector experience serving with the Metropolitan Police Service.

Neal has detailed investigative and review skills and substantial experience of working in high risk and demanding environments with a track record of managing both teams and projects effectively. Neal has significant experience of working at board level to help organisations assess, review and redesign their risk management frameworks and regularly communicates business risk management best practices at senior levels within organisations and at industry events.

About PwC OneSecurity

The PricewaterhouseCoopers OneSecurity team has over 30 years' experience in all aspects of security, from espionage to governance risks. Our globally based team understands and speaks business language, we know when and how best to involve experts in legal, IT, business continuity, disaster recovery, crisis management, fraud, forensic and human resources expertise. This wide range of know-how means we can help your organisation to devise a dynamic and forward-thinking security strategy that identifies all the security risks you face, and offers practical and effective ways of addressing them that won't just save you money, but could even end up making you money.



www.pwc.com/uk

hb04728