



1


Threats and compliance

We live in an analogue world and, increasingly, work, play and do business in a digital one. Our assets, the things we own in either world and that are valuable to us, are also attractive to others. As we've extended our field of activity into the digital **world wide web** (or **internet**), as we've developed new technologies and acquired new skills, so we've been followed by all those antisocial elements who plagued us in the analogue one.

Over the centuries, we've become accustomed (particularly in the First World) to taking appropriate precautions around our analogue assets, health and security. We know how to secure homes, offices and cars. We know what precautions to take while walking, shopping or doing business. We know which neighbourhoods to stay out of. We teach our children what to do, and we have well-developed police and justice systems that deal (to one extent or another) with miscreants.

Although the police and justice systems are still coming to grips with the digital world, the miscreants – criminals (of all sorts: organized, white collar and occasional), malefactors, spies and other undesirables – have already successfully adapted their modus operandi to **cyberspace**. Of course, that doesn't mean that they've deserted the analogue world, they've just extended their sphere of operations to the digital one. We've therefore got to get as good at dealing with the cyber **threats** and **risks** as we already are at dealing with the analogue ones.

In the same way that the CEO of a business can understand the Profit and Loss statement without needing to be an accountant, or the average individual can understand the rules for maintaining and driving a motor car without having to be an auto-mechanic, so any business person or computer user can understand how to be safe online, without needing to be a computer expert. Just as you would be hard-pushed to help a medical specialist diagnose and cure an illness, without first having a good idea



of what it takes to stay healthy, or what disease feels like, so it would be difficult to ensure that your business IT infrastructure, home network or personal computer was adequately secured – or even to call in appropriate outside help – without some grasp of the ABCs of information security.

THREATS

This book's purpose is to arm non-technical business executives and computer users everywhere with the basic information they need if they are to ensure that they and their businesses stay safe online. Staying safe online requires a combination of behaviour and tools that are appropriate and proportionate to the cyber-threats and computer-related risks that we face. Our starting point, therefore, must be to understand the threats and risks. A threat is 'potential cause of an unwanted **incident**, which may result in harm to a system or organization' and a risk is the 'combination of the probability of an event and its consequence' (both definitions from **ISO 17799:2005**). A threat and a risk are not, in other words, the same thing. There are many threats that pose no risk to individual organizations (for instance, the **hacker** threat poses no risk to someone who doesn't use a computer, and the grave **cyber-terrorism** threat poses a limited risk to a small organization whose only use of the internet is for e-mail). We will deal, here, with threats and, in the next chapter, with risks and **risk assessment**.

Threats in the digital world, as in the analogue one, originate with people. These people fall into five groups:

- criminals (thieves, fraudsters, organized crime);
- malefactors (hackers, vandals, terrorists, cyber-warriors, some ex-employees and other disgruntled or vengeful individuals);
- spies (commercial and governmental);
- undesirables (scam artists, spammers (see **spam**), 'ethical' hackers and nerds); and
- the incompetent, or the simply unaware (staff, contractors, customers and other third parties).

From an organizational perspective, these people are found both inside and outside the organization (the balance overall is probably 50:50), but from a standalone computer perspective, there's only you.

Incompetence, lack of awareness and lack of skill are similar problems in either space. The digital threats, and the type of attacks that express them, have the same sort of objectives as they do in the analogue world, but because of the nature of computers, digital data and the internet, their

characteristics are different. These characteristics, as identified by Bruce Schneier (2000), are:

- **Automation:** computers automate mundane tasks; illegal or destructive activity, with which someone would struggle to cost-effectively achieve critical mass in the analogue world, can be automated. Computers make **denial of service attacks** and large-scale junk mail possible, just as they enable 100 per cent surveillance of the internet communications traffic of any individual or organization.
- **Data collection:** digital data requires less storage space than the equivalent analogue information and can be more quickly harvested, stored and mined. What can be done will (often) be done and, as a result, massive databases of personal and commercial data now exist all over the world. They make spamming (see **spam**), surveillance and **identity theft** that much easier.
- **Action at a distance:** in cyberspace, the bad guys are just a mouse click away; the criminal who is trying to steal your money may be based in Chechnya, Moldavia or on a Pacific island. He or she will be just as effective, quick and silent as a criminal next door, far harder to trace and arrest than his or her analogue equivalent, and financially more successful.
- **Propagation:** the web enables ideas, skills and digital tools to be shared around the world within hours. It also enables techniques to be widely replicated and a vast array of computers to be linked into any one attack.

The types of attacks, therefore, that we have to be ready to deal with in cyberspace, are:

- criminal attacks (fraud, theft and grand larceny, identity theft, hacking, extortion, **phishing**, **intellectual property (IPR)** and copyright theft, piracy, brand theft, **'spoofing'**);
- destructive attacks (cyber-terrorism, hackers, ex-employees, vengeful individuals, **cyber war**, cyber-vandals, anarchists, **viruses**);
- nerd attacks (denial of service attacks, publicity hounds, **adware**)
- espionage attacks (data and IPR theft, **spyware**).

These attacks affect individuals and businesses indiscriminately. Individuals and small businesses are rarely directly or individually targeted in an attack (unless they have very substantial assets or some other significant value to the attacker), but they are nevertheless at risk in an environment where automation, action at a distance and propagation enable an attacker to successfully target a very big number of smaller fish. Malefactors know that the majority of individuals and smaller businesses have

inadequate cyber-protection and they exploit this, for instance, deploying large numbers of unprotected computers in huge **zombie** networks, to mount large-scale denial of service attacks and to distribute floods of **spam**. Defences need to be proportionate.

Large businesses and public sector organizations, who have significant assets to protect or who make attractive, high-profile targets, are directly threatened. Their networks are more extensive and more complex, and the quantity and diversity of people and organizations involved with them so great, that they have to be very systematic in identifying and responding to the possible threats.

Impacts of information security breaches

A 2001 global study by the UK DTI found that lapses in security **policy** had cost businesses between 5.7 per cent and 7 per cent of annual revenues in 2000. European businesses alone, it claimed, lost more than £4.3 billion in that year due to internet-related crime. Its seventh annual Information Security Breaches Survey (**ISBS 2004**), managed by Pricewaterhouse-Coopers (www.security-survey.gov.uk) identified the following symptoms:

One-third of large businesses and two-thirds of all companies still have no **information security policy**.

Processes for keeping **anti-virus software** up to date are often weak.

Only half of all wireless **networks** have security controls in place.

Spam is a growing issue (probably now 80 per cent of all e-mail).

Two-thirds of UK businesses had at least one malicious security breach in the last year, an increase from just under half two years earlier.

Over a quarter of businesses suffered a significant incident arising from accidental systems failure or data corruption.

The average UK business now has one security incident a month; large businesses have one per week.

Security breaches continue to cost UK industry several billions of pounds every year.

Organizations were significantly more pessimistic about the future outlook for information security breaches, believing that incidents will happen more often in future and be harder to detect.

The majority of businesses are still spending less than 1 per cent of their IT budget on security; the benchmark against which their expenditure should be compared is in the range of 5 to 10 per cent. Part of the problem may be that less than half of all businesses ever estimate the return on their information security investment.

The UK National High Tech Crime Unit's (www.nhtcu.org) 2004 survey produced the following key findings:

- Of all respondents, 167 out of 201 had experienced high tech crime in 2003.
- The total estimated impact of these crimes was over £195 million.
- Three out of 44 financial service companies experienced financial fraud of over £60 million between them.
- Almost three-quarters of respondents agreed that the single most important impact of a computer-enabled crime was whether the company could continue to operate, function and do business with its customers.

Ernst & Young (www.ey.com/global/content.nsf/International/Home) has been publishing an annual Information Security Survey since 1993. Its 2004 survey interviewed nearly 1,300 executives across 51 countries. Only 20 per cent of organizations strongly agreed that information security was a CEO-level priority, and only 24 per cent gave their information security departments the highest rating in meeting the needs of the organization. This suggests that there is a direct correlation between the effectiveness of the information security department and the informed, focused interest of the CEO. This handbook will help every CEO get better performance from that department. The executive summary of the EY survey made two observations:

Since the release of our first survey in 1993, Ernst and Young has examined the various dimensions of information security as practiced by global organizations. Ironically, this year's survey seems to echo the sentiments of previous years, as organizations apparently continue to rely on luck rather than proven information security controls. Perhaps the remarkable thing is how little attitudes, practices and actions have changed since 1993 – during a period when threats have increased significantly. Two factors lead us to believe matters have deteriorated.

First the threats are more lethal than they were in 1993. What many organizations are slow to recognize is that what they don't know is hurting them and hurting them badly. While scaremongers focus the public's attention upon the external threats with questionable damage guess-estimates, organizations face greater damage from insiders' misconduct, omissions, oversights, or an organizational culture that violates pre-existing policies and procedures.

Second, there is little visible change in how security is practised by organizations. In 1994, a respondent told us: 'It is apparently going to take a major breach of security before this organization gets its act together.' Some ten years later, that sentiment is still quite evident and typifies organizations' reluctance to deal with the significant threats and to invoke well-accepted controls.

The top five incidents identified in the Ernst & Young survey affected more than 50 per cent of organizations. Hardware failure that brought down critical business systems, the top incident, affected 72 per cent of the respondents. Does this mean that they now have tried and tested **business continuity plans** in place? Revealingly, less than 50 per cent of the respondents thought that they would be able to continue business operations in the event of a serious disruption.

Cybercrime

Europol, the European Police agency, observed in its 2003 report on EU organized crime: 'The establishment of worldwide financial markets, economic globalization, and the creation of the EU common market have provided good opportunities for organized crime groups.' In section 4.4, the report observes that 'organized crime groups are clearly among the major beneficiaries of technological progress. . . crucially, the development of cyberspace [has] provided great opportunities and a vast arena in which organized crime groups can operate. . . High technology crime will continue to represent one of the major areas of crime in the future, paralleling the development of e-commerce and internet banking.'

The US Computer Security Institute (CSI) has, with the participation of the San Francisco Federal Bureau of Investigation's Computer Intrusion Squad, conducted nine annual surveys into information security at CSI member firms. The results of the 2004 survey showed that 2004 total financial losses to criminal abuse, across the 269 respondents, were \$141 million. While the biggest loss arose from viruses (\$55 million) and denial of service attacks (\$26 million), \$11 million of these losses was from theft of proprietary information against \$8 million for financial fraud and \$7 million in laptop thefts. It was clear that the other half of those who took part in the overall survey were unable (because they had no method of tracking) or unwilling (because of the possible reputational damage) to provide estimates of the financial losses from the successful attacks they suffered. It is also clear that incidents of **cybercrime** originate equally from outside and inside the attacked computer systems.

Finally, the magazine *Information Security* carried out an online survey of 2,545 information security practitioners in a broad spectrum of public

and private organizations in North America, Europe and the Far East. Although this was carried out in July and August 2001, its findings are still very relevant:

A virus, **worm**, **Trojan** or some other form of **malware** had affected 90 per cent of the organizations – even though 80 per cent of them had antivirus software in place.

The number of organizations hit by web server attacks doubled in number between 2000 and 2001.

Insider security incidents occurred more often than outsider ones, but security professionals were more concerned about securing the external **perimeter** of the organization than dealing with the internal issues.

These internal security incidents included installation of unauthorized software at 78 per cent of the participant organizations, use of company computing resources for illegal or illicit communications or activities (such as porn site surfing or e-mail harassment), and the use of company computing resources for personal profit (gambling, unsolicited e-mail or spam, personal e-commerce businesses, etc).

Many of these so-called information security incidents are actually crimes. The UK's **Computer Misuse Act 1990** made it an offence for anyone to **access** a computer without authorization, to modify the contents of a computer without authorization, or to facilitate (allow) such activity to take place. It identified sanctions for such activity, including fines and imprisonment. Other countries have taken similar action to identify and create offences that should enable law enforcement bodies to deal with computer misuse.

Cyber war

On 12 September 2001, the US General Accounting Office (GAO) reported that 24 US federal bodies, from the Treasury to the Pentagon, had computer systems 'riddled with weaknesses'. It recognized the ease with which hackers could read or tamper with critical information. On 18 September 2001, the Nimda worm infected and shut down 100,000 computers worldwide within 24 hours. It is believed that every significant terrorist or criminal organization has cyber-capabilities and has become very sophisticated in its ability to plan and execute attacks using the most recent technology.

Eliza Manningham-Butler, Director General of the UK's Security Service, said this at the 2004 CBI annual conference:

8 ■ A business guide to information security

A narrow definition of corporate security including the threats of crime and fraud should be widened to include terrorism and the threat of electronic attack. In the same way that health and safety and compliance have become part of the business agenda, so should a broad understanding of security, and considering it should be an integral and permanent part of your planning and Statements of Internal Control; do not allow it to be left to specialists. Ask them to report to you what they are doing to identify and protect your key assets, including your people.

Certainly, businesses have got this message, with 97 per cent of them concerned at board level about cyber-terrorism. They should be. More than 400 million computers are linked to the internet; many of them are vulnerable to indiscriminate cyber-attack. The critical infrastructure of the First World is subject to the threat of cyber assaults, ranging from defacing websites to undermining critical national computer systems. In February 2003, the White House published the National Strategy to Secure Cyberspace, in which the President recognized that securing cyberspace 'would be an extraordinarily difficult task, requiring the combined and coordinated effort of the whole of society and that, without such an effort, an infrastructure that is essential to our economy, security and way of life could be disrupted to the extent that society would be debilitated'.

Future risks

There are a number of trends that lie behind these increases in threats to information security, which, when taken together, suggest that things will continue to get worse, not better:

- The use of distributed computing is increasing. Computing power has migrated from centralized mainframe computers and data processing centres to a distributed network of desktop, laptop and micro-computers, and this makes information security much more difficult.
- There is a strong trend towards mobile computing. The use of laptop computers, **Personal Digital Assistants (PDAs)**, mobile phones, digital cameras, portable projectors and MP3 players has made working from home or on the road relatively straightforward, with the result that **network perimeters** have become increasingly porous. There are many more **remote access** points to networks, and the number of easily accessible **endpoint devices** has increased dramatically, increasing the opportunities to break into networks and steal or corrupt information.
- There has been a dramatic growth in the use of the internet for business communication, and the development of wireless, **VoIP** and **broadband** technologies will drive this even further. The internet provides

an effective, immediate and powerful method for organizations to communicate on all sorts of issues. This exposes all these organizations to the security risks that go with connection to the internet:

- Better hacker tools are available every day, on hacker websites that, themselves, proliferate. These tools are improved regularly and, increasingly technologically proficient criminals – and computer literate terrorists – are thus enabled to cause more and more damage to target networks and systems.
- Increasingly, hackers, **virus writers** and spam operators are co-operating to find ways of spreading more spam: not just because it's fun, but because direct e-mail marketing of dodgy products is lucrative. Phishing and other internet fraud activity will continue evolving and will become an ever bigger problem. This will lead, inevitably, to an increase in **blended threats** that can only be countered with a combination of technologies and processes.
- Increasingly sophisticated technology defences, particularly around user authorization and **authentication**, will drive an increase in **social engineering**-derived hacker attacks.
- Widespread computer literacy. While most people today have computer skills, the next generation is growing up with a level of familiarity with computers that will enable them to develop and deploy an entirely new range of threats. **Instant messaging** is an example of a new technology that is better than e-mail, because it is faster and more immediate, but which has many more security **vulnerabilities** than e-mail. We will see many more such technologies emerging.
- Wireless technology – whether **WiFi** or **Bluetooth** – makes information and the internet available cheaply and easily from virtually anywhere, thereby potentially reducing the perceived value and importance of information and, certainly, exposing confidential and sensitive information more and more to casual access.
- The falling price of computers has brought computing within most people's reach. The result is that most people now have enough computer experience to pose a threat to an organization, if they are prepared to apply themselves just a little to take advantage of the opportunities identified above.

What does this all mean, in real terms, to individuals and to individual organizations?

- No organization is immune.
- Every organization, at some time, will suffer one or more of the abuses or attacks identified in these pages.

- Individual and business activity will be disrupted. Downtime in business critical systems (such as ERP [enterprise resource planning] systems) can be catastrophic for an organization. However quickly service is restored, there will be an unwanted and unnecessary cost in doing so. At other times, lost data may have to be painstakingly reconstructed and, sometimes, it will be lost forever.
- **Privacy** will be violated. Organizations have to protect the personal information of employees and customers. If this privacy is violated, there may – under **data protection** and **privacy legislation** – be legal action and penalties, including against directors individually.
- Organizations and individuals will suffer direct financial loss. Protection in particular of commercial information and customers' **credit card** details is essential. Loss or theft of commercial information, ranging from business plans and customer contracts, to intellectual property and product designs, and industrial know-how, can all cause long-term financial damage to the victim organization. Computer fraud, conducted by staff with or without third-party involvement, has an immediate direct financial impact.
- Reputations will be damaged. Organizations that are unable to protect the privacy of information about staff and customers, and which consequently attract penalties and fines, will find their corporate credibility and business relationships severely damaged and their expensively developed brand and brand image dented.

The statistics are compelling. The threats are evident. No one can afford to ignore the need for information security. The fact that the threats are so widespread and the sources of danger so diverse means that it is insufficient simply to implement an anti-virus policy, or a business continuity policy, or any other standalone solution. A conclusion of the CBI Cybercrime Survey 2001 was that 'deployment of technologies such as firewalls may provide false levels of comfort unless organizations have performed a formal risk analysis and configured firewalls and security mechanisms to reflect their overall risk strategy'. Nothing has changed.

COMPLIANCE, REGULATORY AND LEGAL ISSUES

Certainly, organizations can legally no longer ignore the issue. There are a number of pieces of UK legislation that are relevant to information security: the **Copyright Designs and Patents Act 1988**; the **Computer Misuse Act 1990**; the **Data Protection Act 1998**; the **Human Rights Act 1998**; the **Electronic Communications Act 2000**; the **Freedom of Information Act 2000**; **Regulation of Investigatory Powers Act 2000**; the **Privacy**

and Electronic Communications Regulations 2003 and the Software Licensing Regulations.

Apart from the Freedom of Information Act (which came fully into force in January 2005), the Data Protection Act (**DPA**) 1998 is perhaps the most high profile of these recently passed laws; it requires organizations to implement data security measures to prevent unauthorized or unlawful processing (which includes storing) and accidental loss or damage to data pertaining to living individuals. Non-computerized or manual records, videotape and microfilm, are all also covered by this legislation. According to BSI, the UK Information Commissioner has stated that organizations that can demonstrate compliance to BS 7799 will be able to satisfy his office that appropriate measures are in place to meet the security requirements of the DPA.

While these Acts apply to all UK-based organizations, stock exchange listed companies are also expected to comply with the recommendations of the Combined Code on Corporate Governance and the Turnbull Guidance. Crucially, these require directors to take a risk assessment-based approach to their management of the business and to consider all aspects of the business in doing so.

The implications of this are that directors of listed businesses and of public sector organizations must be able to identify the steps they have taken to protect the **availability, confidentiality and integrity** of the organization's information assets. In all of these instances, the existence of a risk-based information security management policy, implemented through an Information Security Management System (ISMS), is clear evidence that the organization has taken the necessary and appropriate steps.

INFORMATION SECURITY

So, what is 'information security'? 'Information security' is, according to the internationally recognized code of information security best practice, ISO 17799:2005, the 'preservation of the confidentiality, integrity and availability of **information**; in addition, other properties, such as authenticity, **accountability, non-repudiation** and **reliability** can also be involved'.

Information is the life blood of the modern business. All organizations possess **critical** or sensitive information. According to a 2000 UK Department of Trade and Industry survey, 49 per cent of organizations believe that information is critical or sensitive because it will be of benefit to competitors, while 49 per cent believe that it is critical to maintaining customer confidence. The 2004 survey identified the fact that, while 58 per cent of all businesses had highly confidential information stored on their computer systems, 77 per cent of large businesses were in this category.

Roughly nine-tenths of UK businesses now send e-mail across the internet, browse the web and have a website; and 87 per cent of them now identify themselves as 'highly dependent' on electronic information and the systems that process it, compared with 76 per cent in 2002. Information and information systems are, in other words, at the heart of any organization trying to operate in the high-speed wired world of the 21st century.

The proliferation of increasingly complex, sophisticated and global threats to this information and its systems, in combination with the compliance requirements of a flood of computer- and privacy-related regulation around the world, is forcing organizations to take a more joined-up view of information security. Hardware-, software- and vendor-driven solutions to individual information security challenges no longer cut the mustard. On their own, in fact, they are dangerously inadequate.

News headlines about hackers, viruses and online fraud are just the public tip of the data insecurity iceberg. Business losses through computer failure, or major interruption to their data and operating systems, or the theft or loss of intellectual property or key business data, are more significant and more expensive.

This handbook provides business owners, executives, general managers and individual users in organizations of all sizes and types with an overview of the information security needs of their organization. It enables them to understand what their IT management is telling them, to sort the wheat from the chaff, the jargon and the hype from the real issues and to make pragmatic information security decisions that are right for their business, rather than just right for the IT people. This handbook provides sufficient information and insight to help the reader navigate the dangerous sea of technology-specific solutions pitched by vendors and/or the IT department. It does this by looking at the actual threats facing organizations of different sizes and types, recognizing that there are no 'one size fits all' solutions, but that there are some basic principles (the **Infosec Basics for Business**) that should underpin all responses.

Organizations that want to take a more structured approach to information security (developing, for instance, an Information Security Management System) and to their overall strategy for managing information and their information assets should be looking to develop an IT governance framework. They are referred to two books, both complementary to this one, that will help them achieve this: *IT Governance: Guidelines for Directors* and *IT Governance: A Manager's Guide to Data Security and BS 7799/ISO 17799*.

BENEFITS OF TAKING ACTION

- Individuals will decrease the likelihood of suffering disruption, inconvenience and from the effects of cybercrime.
- Directors of listed companies will be able to demonstrate that they are complying with the requirements of the Turnbull Guidance and/or complying with current international best practice in **risk management** with regards to information assets and security.
- Organizations will be able to demonstrate, in the context of the array of relevant legislation, that they have taken appropriate action to comply with the laws, particularly (in the United Kingdom) the Data Protection Act 1998.
- Organizations and individuals will have systematically protected themselves from the dangers and potential costs of external or internal attack, cybercrime and the impacts of cyber war.
- Each organization will improve its credibility with staff, customers and partner organizations and this can have direct financial benefits through, for instance, improved sales.
- Better, informed, practical decisions about what security technologies and solutions to deploy will reduce the overall costs of information security while improving the effectiveness of those investments.
- Directors will be able to ensure that the information security solutions that are deployed help the business progress, rather than hinder it – that the technology becomes a ‘business enabler’, leading to improved performance.

The major benefit, overall, is that the **logical** world will become more like the analogue one to which we have become used over the last few centuries: safe, predictable and prosperous.

