PART TWO

ESSENTIALS OF INFORMATION SYSTEMS

Part Two concentrates on the essential components of information systems. Most people view IT strictly from a technological paradigm, but in fact, IT's power and influence is not so much a factor of its technical nature, but rather of what that technical infrastructure carries, houses, and supports: information. And information is power to an organisation. Part Two highlights this point and raises awareness of the significance of information to organisational success. Understanding how enterprise architectures support information, how employees access and analyse information to make business decisions, and how wireless and mobile technologies can enable information access 24/7 are the primary learning goals of Part Two. Properly managing information is a key organisational resource and can give a company a definite competitive advantage. The bottom line is that managers who treat information as a corporate asset yield success in the marketplace.

The section begins by covering information ethics and information security. With the many new governance and compliance regulations, all managers must understand the ethical issues surrounding information. As a key organisational resource, information must be protected from misuse and harm. This involves addressing ethical concerns around the collection, storage, and usage of information; protecting information privacy; and ensuring that information is secure against unauthorised access and attack.

Graduate Spotlight

Name: Michael Josem, Australia

Course studied: Bachelor of Information Systems/Bachelor of Arts at Monash University

Employer: PokerStars

Current position: Game security specialist—I work to protect the security of online poker games. We're constantly looking at new ways of analysing information that we have access to, and using this information to detect unusual results.

What led you to be interested in business information systems?

My father was in the business of assisting retail businesses with business information systems. From a young age, and growing up around computers, they were always of interest to me.

What are your thoughts on the future of the industry?

The twentieth century was defined by the wall—the Berlin Wall, the Iron Curtain, and so on—barriers to people communicating. I believe that the twenty-first century will be defined by the web—the global interconnectedness of networks—and that organisations that succeed will be those that harness the huge intelligence of these huge crowds of people. Google is succeeding essentially because it has developed an algorithm to rank the relative value of web pages. I became prominent in my industry as a result of an entirely voluntary, 'wiki-style' investigation into unusual results, and in that sense, my career success is really a product of open cloud-computing and open online communities.

How have your studies helped you in your career?

My studies gave me a solid fundamental understanding of the principles involved. No employer expects a new graduate to be an expert on everything, but every employer expects a graduate to have a solid understanding of the fundamentals.

CHAPTER 4
ETHICS AND INFORMATION SECURITY

SECTION 4.1 Ethics
- Ethics
- Information ethics
- Developing information management policies
- Ethics in the workplace

SECTION 4.2 Information security
- Protecting intellectual assets
- The first line of defence—people
- The second line of defence—technology

Employability Skills

ACS:	Group 1: Ethics/social implications/ professional practice Group 2: Security	IS2002:	Business fundamentals; Analytical and critical thinking skills; Interpersonal, communication and team skills
AACSB:	Analytical skills; Reflective thinking; Ethical understanding and reasoning abilities	DEST:	Communication

What's in IT for me?

This chapter concerns itself with protecting information from potential misuse. Organisations must ensure they collect, capture, store and use information in an ethical manner. This could be any type of information they collect and utilise, including information about customers, partners and employees. Companies must ensure that personal information collected about someone remains private. This is not just a nice thing to do. The law requires it. Privacy laws differ in every jurisdiction and only Australia's unique regulations are discussed in the following chapter. Students who are interested in the particular regulations as they exist in other countries should consult alternative resources. Perhaps most importantly, information must be physically kept secure to prevent access and possible dissemination and use by unauthorised sources.

You, the business student, must understand ethics and security because they are the top concerns voiced by customers today. These concerns directly influence a customer's likelihood to embrace electronic technologies and conduct business over the Internet. In this sense, these concerns affect a company's bottom line. You can find evidence in recent news reports about how the stock price of organisations dramatically falls when information privacy and security breaches are made known. Further, organisations face potential litigation if they fail to meet the ethical, privacy and security obligations concerning the handling of information in their companies.

The authors would like to acknowledge redchip lawyers (Brisbane, Australia) for their expertise and cooperation in the adaptation of this chapter for the Australian and New Zealand contexts. In particular, we would like to thank Gavin Barnes, Megan Alley and Christopher Perkins for their valuable and professional contribution.

Case Study

Keeping a record: your record retention obligations

redchip lawyers

Producing and storing large amounts of information is an unavoidable by-product of operating a business in the information age. The sheer volume of the information that businesses collect has meant organisations often need to implement and manage an effective record retention system.

In the wake of the Worldcom and Enron scandals that rocked the American financial system, the US Congress introduced the *Sarbanes-Oxley Act* in 2002. The Act imposes criminal penalties for destroying, altering, concealing or falsifying records.

While US regulations often influence regulations in Australia and around the world, the Australian government has not to date introduced anything as severe as the *Sarbanes-Oxley Act*. There is no set of uniform requirements upon Australian companies to maintain their records, leading to a situation where various regulations apply to different types of records. Three such regulations are:

Tax regulations	Companies must keep their records relating to the income tax collected from their employees. They must keep these records for 5 years. Companies must also keep records that relate to their payment of Goods and Services Tax (GST). They must keep these records for 5 years.
Corporate regulations	Companies must keep the records which explain their financial statements (such as profit and loss statements and balance sheets). This includes invoices, receipts, cheques and orders which may be stored electronically, but must be guarded against damage, destruction and falsification. The records must be available for inspection. These records must be kept for 7 years.
Privacy regulations	Companies must inform individuals how their personal information will be used and how it will be protected. All personal information must be accurate and up to date. Irrelevant or useless information cannot be kept indefinitely. Individuals have the right to access their personal information on request.

Benefits of a record retention system

A record retention system includes a schedule for processes such as the length of time each document or record will be retained as an active record, reason for retention, and a final disposition of the record (archive or destruction).

'Discovery' is the process that follows an initiation of legal action. Before a matter goes to court, all parties must deliver relevant documents to the other side. There are enormous costs associated with the process of discovery, and the fear of a legal discovery order will see companies scramble to settle out of court rather than pay the millions of dollars associated with the order. However, if a company chooses to disclose its records, a record retention system certainly expedites the process.

There are other benefits to having a record retention system. As well as providing guidelines for which records can and should be kept, a record retention system should also provide guidelines for the destruction of records. It is equally important that companies destroy certain records before they breach Australian privacy regulations.

Insider trading, sexual harassment and other workplace relations issues can also be prevented using proactive monitoring. An effective record retention system should include email surveillance. Retention of email records can in turn provide employers protection from potential legal liability, and in cases where workplace harassment is alleged to be occurring, can provide employees protection in the form of proof.

Implementing a record retention system

Implementing a record retention system may require a great deal of work across all departments, although it is the IT department which must get the process up and running. The following are a few practical considerations for companies planning to implement a record retention system.

- The company must define what records are to be kept and clearly state how long those records should be maintained. These definitions must be reviewed by the legal department who should liaise with the IT team to ensure they are being properly interpreted.
- The company must invest in the appropriate technology and infrastructure to retain their records. Experts believe that 80 per cent of corporate communication is electronic via email and instant messaging,[1] so any technology must be capable of capturing and storing that voluminous data in a searchable format. The technology must also be able to meet regulatory demands. Companies which archive hard copies of their records must ensure their documents are suitably protected from damage, destruction or falsification.
- The company must regularly test and review their record retention system to ensure that data can be accessed and retrieved quickly, the system continues to meet regulatory requirements and employees are implementing the system appropriately.

Case Study

QUESTIONS TO FOLLOW

Introduction

Ethics and security are two fundamental building blocks for all organisations. In recent years, corporate scandals such as those affecting HIH and OneTel along with terrorist events such as the September 11 attack on New York and the Bali bombings have shed new light on the meaning of ethics and security. When the behaviour of a few individuals can destroy billion-dollar organisations, the value of ethics and security should be evident.

4.1 ETHICS

LEARNING OUTCOMES

- Explain the ethical issues surrounding information technology.
- Identify the differences between an 'ethical computer use policy' and an 'acceptable use policy'.
- Describe the relationship between an 'email privacy policy' and an 'Internet use policy'.
- Explain the effects of spam on an organisation.
- Summarise the different monitoring technologies and explain the importance of an employee monitoring policy.

ETHICS

Ian Clarke, the inventor of a file-swapping service called Freenet, decided to leave the United States for the United Kingdom, where copyright laws are more lenient. Wayne Rosso, the inventor of a file-sharing service called Grokster, left the United States for Spain, again saying goodbye to tough US copyright protections. Sharman Networks is the owner of popular file-sharing application KaZaA. Interestingly, although it has its headquarters in Australia, the company is incorporated in Vanuatu, and abides by US copyright laws.[2] While Australian copyright laws have a reputation for being concise, regulated and adhered to, the same cannot be said for US copyright laws, which may be why an Australian company would prefer to be regulated under the US system.

The Australian copyright laws, designed decades before the invention of the Internet, make file sharing and many other Internet technologies illegal. Although some individuals use file sharing in unethical ways, such as downloading music and movies illegally, file sharing has many positive benefits, such as improving drug research, software development and the flow of information.[3]

The ethical issues surrounding copyright infringement and intellectual property rights are consuming the e-business world. Advances in technology make it easier for people to copy everything from music to pictures. Technology poses new challenges for our **ethics**—the principles and standards that guide our behaviour toward other people. Table 4.1 presents an overview of concepts, terms and ethical issues stemming from advances in technology.

Intellectual property	The collection of rights that protect creative and intellectual effort.
Copyright	The exclusive right to do, or omit to do, certain acts with intangible property such as a song, video game and some types of proprietary documents.
Fair use doctrine	In certain situations, it is legal to use copyrighted material.
Pirated software	The unauthorised use, duplication, distribution, or sale of copyrighted software.
Counterfeit software	Software that is manufactured to look like the real thing and sold as such.

TABLE 4.1
Technology-related ethical issues

In 2002, the Victorian Supreme Court awarded $400 000 to dying 51-year-old smoker Rolah McCabe. Justice Geoffrey Eames struck out the defence of British American Tobacco on the basis that it had deliberately destroyed or removed documents that would have been relevant to the case. From 1989 onwards, American lawyers had come to Australia to oversee the British American Tobacco's 'document retention policy'. The judge found that the company, and its solicitors Clayton Utz, acted 'with the deliberate intention of denying a fair trial to the plaintiff, and the strategy to achieve that outcome was successful'. This decision was largely overturned on appeal, but negative publicity led to new Victorian legislation that outlawed the destruction of certain documents.

Regardless of who is to blame, the bigger issue is that the destruction of files after litigation has begun is both unethical and illegal. A direct corporate order to destroy information which is the basis for litigation poses a dilemma for any professional. Comply, and you participate in potentially unlawful activities; refuse, and you might find yourself looking for a new job.

Privacy is one of the largest ethical issues facing organisations. **Privacy** is the interest of a person in protecting their life from unwanted intrusion and public scrutiny. In Australia, there is no general right to privacy. However, unlawful interference with an individual's privacy, family, home or correspondence is protected by the commonwealth *Privacy Act 1988*. Privacy is related to **confidentiality,** which is the principle that certain information will remain outside the public domain. Some of the most problematic decisions facing organisations lie in the murky and turbulent waters of privacy. The burden comes from the knowledge that each time employees make a decision regarding issues of privacy, the outcome could potentially sink the company.

Trust between companies, customers, partners and suppliers is the support structure of e-business. One of the main ingredients in trust is privacy. Privacy continues to be one of the primary barriers to the growth of e-business. People are concerned their privacy will be violated because of interactions on the web. Unless an organisation can effectively address this issue of privacy, its customers, partners and suppliers might lose trust in the organisation, which would hurt its business. In keeping with its mandate to gather intelligence, the Australian Security and Intelligence Commission (ASIO) has stated that the Internet 'can provide valuable input to ASIO's analytical and investigative work'.[4] In America, the CIA is watching YouTube. US spies, working for the Director of National

Intelligence (DNI), are looking increasingly online for intelligence; they have become major consumers of social media. 'We're looking at YouTube, which carries some unique and honest-to-goodness intelligence', said Doug Naquin, director of the DNI Open Source Center. 'We're looking at chat rooms and things that didn't exist five years ago, and trying to stay ahead. We have groups looking at what they call "Citizens Media": people taking pictures with their cell phones and posting them on the Internet.' Table 4.2 displays some relevant community attitudes towards privacy on the Internet.

TABLE 4.2
Attitudes towards privacy issues on the Internet[5]

1	Sixty-two per cent of respondents were more concerned about the security of their personal information than usual when using the Internet.
2	Two-thirds of respondents reported that they had read the privacy policy attached to an Internet site.
3	Three in ten respondents admitted to having provided false information when filling out a form online. This is relevant for organisations which ask for customer information when selling products online.

INFORMATION ETHICS

Information ethics concern the ethical and moral issues arising from the development and use of information technologies, as well as the creation, collection, duplication, distribution and processing of information itself (with or without the aid of computer technologies). Individuals determine how to use information and how information affects them. How individuals behave toward each other, and how they handle information and technology, are largely influenced by their ethics. Ethical dilemmas usually arise not in simple, clear-cut situations but out of a clash between competing goals, responsibilities and loyalties. Inevitably, the decision-making process has more than one socially acceptable 'correct' decision. Table 4.3 contains examples of ethically questionable or unacceptable uses of information technology.

TABLE 4.3
Ethically questionable or unacceptable information technology use

Examples of questionable information technology use
Individuals copy, use and distribute software.
Employees search organisational databases for sensitive corporate and personal information.
Organisations collect, buy and use information without checking the validity or accuracy of the information.
Individuals create and spread viruses that cause trouble for those using and maintaining IT systems.
Individuals hack into computer systems to steal proprietary information.
Employees destroy or steal proprietary organisation information such as schematics, sketches, customer lists and reports.

People make arguments for or against—justify or condemn—the behaviours in Table 4.3. Unfortunately, there are few hard and fast rules for always determining what is and is not ethical. Knowing the law will not always help because what is legal might not always be ethical, and what might be ethical is not always legal. For example, American Joe

Reidenberg received an offer for a mobile phone service from AT&T Wireless. The offer revealed that AT&T Wireless had used Equifax, a credit reporting agency, to identify Joe Reidenberg as a potential customer. Overall, this strategy seemed like good business. Equifax could generate additional revenue by selling information it already owned and AT&T Wireless could identify target markets, thereby increasing response rates to its marketing campaigns.

Unfortunately, the *Fair Credit Reporting Act* (FCRA) in the US forbids repurposing credit information except when the information is used for 'a firm offer of credit or insurance'. In other words, the only product that can be sold based on credit information is credit. A representative for Equifax stated, 'As long as AT&T Wireless (or any company for that matter) is offering the cell phone service on a credit basis, such as allowing the use of the service before the consumer has to pay, it is in compliance with the FCRA'.[6]

In Australia, the position would likely be different. In 2008, the Australian Privacy Commissioner found that a betting agency that obtained access to consumer credit information files held by a credit reporting agency breached the *Privacy Act 1988*. Under the *Privacy Act*, credit providers can obtain access to credit information in the possession or control of a credit reporting agency. The Commissioner found that the betting agency was not a credit provider, even though the agency provided betting services to its customers on credit.[7] However, the American scenario raises an important question—is an act ethical just because it is legal?

Technological advancements, and newfound ways of collecting and presenting customer information, are providing new ethical dilemmas for organisations. Because much technology is so new and pervasive in unexpected ways, the ethics surrounding information are still being defined. Figure 4.1 displays the four quadrants of ethical and legal behaviour. The ideal goal for organisations is to make decisions within quadrant I that are both legal and ethical.

FIGURE 4.1 Acting ethically and legally are not always the same

Information has no ethics

Jerry Rode, CIO of Saab Cars USA, realised he had a public relations fiasco on his hands when he received an email from an irate customer. Saab had hired four Internet marketing companies to distribute electronic information about Saab's new models to its customers. Saab specified that the marketing campaign be opt-in, implying that it would contact only the people who had agreed to receive promotions and marketing material via email. Unfortunately, one of the marketing companies apparently had a different definition of opt-in and was emailing all customers regardless of their opt-in decision.

Rode fired the errant marketing company and immediately developed a formal policy for the use of customer information. 'The customer doesn't see ad agencies and contracted marketing firms. They see Saab USA spamming them', Rode said. 'Finger-pointing after the fact won't make your customers feel better.'[8]

Information has no ethics. Information does not care how it is used. It will not stop itself from spamming customers, sharing itself if it is sensitive or personal, or revealing details to third parties. Information cannot delete or preserve itself. Therefore, it falls on the shoulders of those who own the information to develop ethical guidelines on how to manage the information. Table 4.4 provides an overview of some of the important laws that individuals must follow when they are attempting to manage and protect information.

TABLE 4.4 Established information-related Australian laws

Crimes Act 1914	It is an offence to unlawfully access or use data held by the Australian government.
Freedom of Information Act 1982	The object of this Act is to extend as far as possible the right of the Australian community to access information in the possession of the Australian government.
Privacy Act 1988	This Act sets national standards for dealing with personal information by organisations and ensures that personal information of those organisations will be stored, used and disclosed in a fair and appropriate way.
Credit Reporting Code of Conduct 1991	The Code imposes legally binding obligations on credit reporting agencies and credit providers. Companies must inform individuals how their personal information will be used and how it will be protected. All personal information must be accurate and up to date. Irrelevant or useless information cannot be kept indefinitely.
Data-Matching Program (Assistance and Tax) Act 1990	The Act authorises the transfer of information between government agencies about persons and allows the matching of information held by other agencies with the information held by the Department of Social Security. Similar provisions exist in the *National Health Act 1953*, Income *Tax Assessment Act 1936*, *Taxation Administration Act 1953*, *Freedom of Information Act 1982* and *Archives Act 1983*.
Patents Act 1990	Subject to this Act, a patent gives the owner of the patent the exclusive rights, during the term of the patent, to exploit the invention and to authorise another person to exploit the invention.
Electronic Transactions Act 1992	Any requirement (such as signing or producing a document) imposed under an Australian Commonwealth law can be met in electronic form.
Corporations Act 2001	Companies must keep the records which explain their financial statements (such as profit and loss statements and balance sheets) for 7 years.
Sarbanes-Oxley Act 2002 (USA)	Seeks to protect investors by improving the accuracy and reliability of corporate disclosures and requires companies to (1) implement extensive and detailed policies to prevent illegal activity within the company, and (2) to respond in a timely manner to investigate illegal activity.

▶ Continued

Designs Act 2003	The registered owner of a registered design has the exclusive right, during the term of registration of the design, to exploit the design and to authorise another person to exploit the design.
Spam Act 2003	Sets a scheme for regulating commercial electronic messages. These must include information about the individual or organisation who authorised the sending of the message and must contain a functional unsubscribe facility. Unsolicited commercial electronic messages must not be sent.

DEVELOPING INFORMATION MANAGEMENT POLICIES

Treating sensitive corporate information as a valuable resource is good management. Building a corporate culture based on ethical principles that employees can understand and implement is responsible management. In an effort to provide guidelines for ethical information management, *CIO* magazine (along with over 100 American CIOs) developed six principles for ethical information management, which are displayed in Table 4.5.

Organisations should develop written policies establishing employee guidelines, personnel procedures and organisational rules for information. These policies set employee expectations about the organisation's practices and standards and protect the organisation from misuse of computer systems and IT resources. If an organisation's employees use computers at work, the organisation should, at a minimum, implement e-policies. **e-Policies** are policies and procedures that address the ethical use of computers and Internet usage in the business environment. These policies typically embody the following:

- ethical computer use policy;
- information privacy policy;
- acceptable use policy;
- email privacy policy;
- Internet use policy;
- anti-spam policy.

1	Information is a valuable corporate asset and should be managed as such, like cash, facilities, or any other corporate asset.
2	The CIO is steward of corporate information and is responsible for managing it over its life cycle—from its generation to its appropriate destruction.
3	The CIO is responsible for controlling access to and use of information, as determined by governmental regulation and corporate policy.
4	The CIO is responsible for preventing the inappropriate destruction of information.
5	The CIO is responsible for bringing technological knowledge to the development of information management practices and policies.
6	The CIO should partner with executive peers to develop and execute the organisation's information management policies.

TABLE 4.5
CIO magazine's six principles for ethical information management

Ethical computer use policy

In a case that illustrates the perils of online betting, a leading Internet poker site reported that a hacker exploited a security flaw to gain an insurmountable edge in high-stakes, no-limit Texas hold-'em tournaments—the ability to see his opponents' hole cards. The scam was eventually discovered by an Australian IS graduate Michael Josem, but not before much damage had been done.[9] The cheater, whose illegitimate winnings were estimated at between US$400 000 and US$700 000 by one victim, was an employee of AbsolutePoker.com, who hacked the system to show that it could be done. Regardless of what business a company operates—even one that many view as unethical—the company must protect itself from unethical employee behaviour.

One of the essential steps in creating an ethical corporate culture is establishing an ethical computer use policy. An **ethical computr use policy** contains general principles to guide computer user behaviour. For example, the ethical computer use policy might explicitly state that users should refrain from playing computer games during working hours. This policy ensures the users know how to behave at work and the organisation has a published standard by which to deal with user infractions. For example, after appropriate warnings, the company may terminate an employee who spends significant amounts of time playing computer games at work.

There are variations in how organisations expect their employees to use computers but, in any approach, the overriding principle when seeking appropriate computer use should be informed consent. The users should be informed of the rules and, by agreeing to use the system on that basis, consent to abide by the rules.

An organisation should make a conscientious effort to ensure all users are aware of the policy through formal training and other means. If an organisation were to have only one e-policy, it should be an ethical computer use policy since it is the starting point and the umbrella for any other policies the organisation might establish.

Information privacy policy

Scott Thompson is the executive vice president of Inovant, the company Visa set up to handle its technology. Thompson errs on the side of caution in regard to Visa's information: he bans the use of Visa's customer information for anything outside its intended purpose—billing.

Visa's customer information details how people are spending their money, in which stores, on which days, and even at what time of day. Sales and marketing departments around the country no doubt are salivating at any prospect of gaining access to Visa's databases. 'They would love to refine the information into loyalty programs, target markets, or even partnerships with Visa. There are lots of creative people coming up with these ideas. This whole area of information sharing is enormous and growing. For the marketers, the sky's the limit', Thompson said. Privacy specialists along with Thompson developed a strict credit card information policy, which the company follows.

The question now is can Thompson guarantee that unethical use of his information will not occur? Many experts do not believe that he can. In a large majority of cases, the unethical use of information happens not through the malicious scheming of a rogue marketer, but rather, unintentionally. For instance, information is collected and stored for

some purpose, such as record keeping or billing. Then, a sales or marketing professional figures out another way to use it internally, share it with partners, or sell it to a trusted third party. The information is 'unintentionally' used for new purposes. The classic example of this type of unintentional information reuse is the Australian Medicare card, which started simply as a way to access government-provided universal healthcare and is now used as a sort of substitute personal ID.

An organisation that wants to protect its information should develop an information privacy policy. An **information privacy policy** contains general principles regarding information privacy. Table 4.6 highlights a few guidelines an organisation can follow when creating an information privacy policy.

TABLE 4.6
Creating an information privacy policy

1	**Adoption and implementation of a privacy policy.** An organisation engaged in online activities or e-business has a responsibility to adopt and implement a policy for protecting the privacy of personal information. Organisations should also take steps that foster the adoption and implementation of effective online privacy policies by the organisations with which they interact, for instance, by sharing best practices with business partners.
2	**Notice and disclosure.** An organisation's privacy policy must be easy to find, read and understand. The policy must clearly state: › What information is being collected. › The use of information being collected. › Possible third-party distribution of that information. › The choices available to an individual regarding collection, use and distribution of the collected information. › A statement of the organisation's commitment to information security. › What steps the organisation takes to ensure information quality and access.
3	**Choice and consent.** Individuals must be given the opportunity to exercise choice regarding how personal information collected from them online may be used when such use is unrelated to the purpose for which the information was collected. At a minimum, individuals should be given the opportunity to opt out of such use.
4	**Information security.** Organisations creating, maintaining, using or disseminating personal information should take appropriate measures to assure its reliability and should take reasonable precautions to protect it from loss, misuse or alteration.
5	**Information quality and access.** Organisations should establish appropriate processes or mechanisms so that inaccuracies in material personal information, such as account or contact information, may be corrected. Other procedures to assure information quality may include use of reliable sources, collection methods, appropriate consumer access and protection against accidental or unauthorised alteration.

Acceptable use policy

An **acceptable use policy (AUP)** is a policy that a user must agree to follow in order to be provided access to a network or to the Internet.

Many businesses and educational facilities require employees or students to sign an acceptable use policy before gaining network access. When signing up with an Internet

service provider (ISP), each customer is typically presented with an AUP, which states that they agree to adhere to certain stipulations (see Table 4.7).

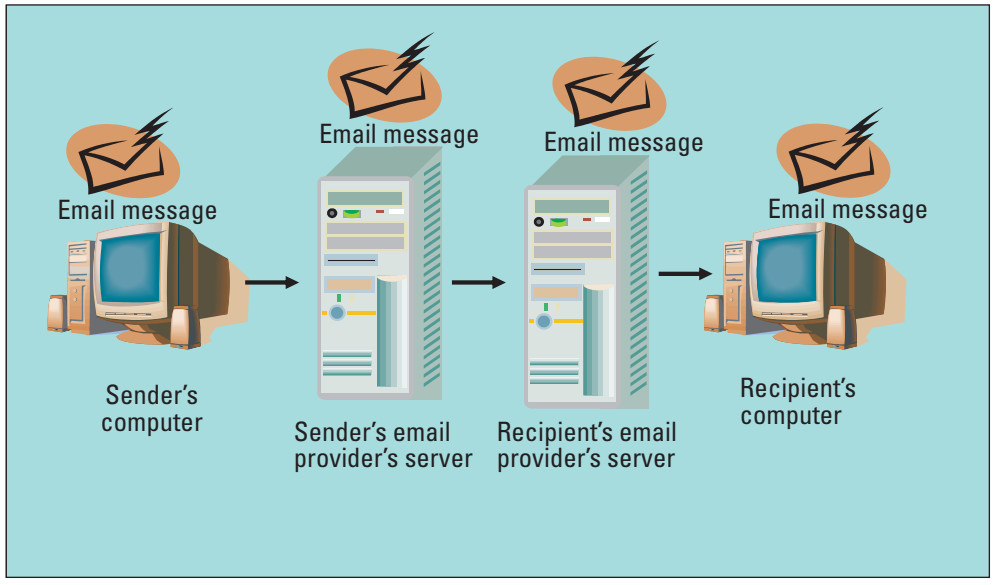
TABLE 4.7
Acceptable use policy stipulations

1	Not using the service as part of violating any law.
2	Not attempting to break the security of any computer network or user.
3	Not posting commercial messages to groups without prior permission.
4	Not attempting to send junk email or spam to anyone who does not want to receive it.
5	Not attempting to mail bomb a site. A **mail bomb** is sending a massive amount of email to a specific person or system resulting in filling up the recipient's email disk space, which, in some cases, may be too much for the server to handle and may cause the server to stop functioning.

Email privacy policy

Email is so pervasive in organisations that it requires its own specific policy. According to experts in the field such as David Thompson, Managing Director of AXS-One Pty Ltd, 80 per cent of corporate communication is done electronically via email and instant messaging (IM). While email and IM are common business communication tools, there are risks associated with using them. For instance, a sent email is stored on at least three or four different computers (see Figure 4.2). Simply deleting an email from one computer does not delete it from the other computers. Companies can mitigate many of the risks of using electronic messaging systems by implementing and adhering to an **email privacy policy**.[10]

FIGURE 4.2
Email is stored on multiple computers



Deleting an email from the recipient's computer does not delete it from the sender's computer or the provider's computers.

One of the major problems with email is the user's expectations of privacy. To a large extent, this expectation is based on the false assumption that email privacy protection exists somehow analogous to that of Australia Post's Registered Mail service. This is simply not true. Take the example of London lawyer Richard Phillips. After his secretary spilled a little ketchup on his pants, Phillips demanded restitution from her—via email—in the amount of a measly £4 (approximately $10). The subject line of that email: 'Ketchup Trousers'. The secretary failed to pay immediately, owing to her mother's sudden death, but quickly made the David versus Goliath matter public, humiliating Phillips. His firm later said Phillips had resigned, but it was careful to note that the departure had nothing to do with the trousers incident.

The issue of employers monitoring emails sent by their employees is one that has received considerable attention—however the surveillance of employees' emails is an unclear legal area. Under the *Privacy Act 1988*, organisations must collect, use and store information obtained by tracking an employee's emails in a certain way. To overcome these obstacles organisations should have a robust email privacy policy. Organisations should have a policy that:

- clearly sets out how employees may use email and the Internet for private and non-employment purposes;
- states what activities are permitted and those which are not permitted;
- details the type of information that will be recorded and the members of the organisation that will have access to that information; and
- provides for the monitoring and auditing process that will consider the information.[11]

Organisations must create an email privacy policy. Table 4.8 displays a few of the key stipulations generally contained in an email privacy policy.

TABLE 4.8
Email privacy policy stipulations

1	The policy should be complementary to the ethical computer use policy.
2	It defines who legitimate email users are.
3	It explains the backup procedure so users will know that at some point, even if a message is deleted from their computer, it will still be on the backup media.
4	It describes the legitimate grounds for reading someone's email and the process required before such action can be taken.
5	It informs that the organisation has no control of email once it is transmitted outside the organisation.
6	It explains what will happen if the user severs his or her connection with the organisation.
7	It asks employees to be careful when making organisational files and documents available to others.

Internet use policy

Similar to email, the Internet has some unique aspects that make it a good candidate for its own policy. These include the large amounts of computing resources that Internet

users can expend, thus making it essential that such use be legitimate. In addition, the Internet contains numerous materials that some believe are offensive and, hence, some regulation is required. An **Internet use policy** contains general principles to guide the proper use of the Internet. Table 4.9 lists a few important stipulations that might be included in an Internet use policy.

TABLE 4.9
Internet use policy stipulations

1	The policy should describe available Internet services because not all Internet sites allow users to access all services.
2	The policy should define the organisation's position on the purpose of Internet access and what restrictions, if any, are placed on that access.
3	The policy should complement the ethical computer use policy.
4	The policy should describe user responsibility for citing sources, properly handling offensive material and protecting the organisation's good name.
5	The policy should clearly state the ramifications if the policy is violated.

Anti-spam policy

Spam is unsolicited email. An **anti-spam policy** simply states that email users will not send unsolicited emails (or spam). Spam plagues all levels of employees within an organisation from receptionists to CEOs. Estimates indicate that spam accounts for 40 to 60 per cent of most organisations' email traffic. According to Ferris Research, spam cost the major global economies $64 billion in 2005, and organisations in developed economies without spam filtering software face costs of US$1000 per mailbox.[12]

SunRice, a popular producer of Australian rice and rice products, has approximately 800 employees and a presence in about 60 national markets. The company receives somewhere between 50 000 and 60 000 legitimate work-related emails a month, but in 2006 it received up to 350 000 emails a month. That amount of spam was taking up a lot of the IT department's time and effort.

After introducing a spam filter, the company made significant productivity gains. All employees spent less time perusing junk mail, but the impact on the company's IT department was the most pronounced. 'We've gone from spending three or four days a week managing email problems to maybe one hour all up each week', says Col Thompson, SunRice's IT business services team leader.[13]

Spam clogs email systems and siphons IT resources away from legitimate business projects. It is difficult to write anti-spam policies, laws or software because there is no such thing as a universal litmus test for spam. One person's spam is another person's newsletter. End users have to be involved in deciding what spam is because what is unwanted can vary widely not just from one company to the next, but from one person to the next. What looks like spam to the rest of the world could be essential business communications for certain employees.

John Zarb, CIO of Libbey, a manufacturer of glassware, china and flatware, tested Guinevere (a virus and subject-line filter) and SpamAssassin (an open source spam filter). He had to shut them off after 10 days because they were rejecting important legitimate emails. As Zarb quickly discovered, once an organisation starts filtering email, it runs the risk of blocking legitimate emails that look like spam. Avoiding an

unacceptable level of 'false positives' requires a delicate balancing act. The IT team tweaked the spam filters and today, the filters block about 70 per cent of Libbey's spam. According to Zarb the 'false positive' rate is far lower, but still not zero. At SunRice, 'the software is so accurate we probably get around 20 (wrongly quarantined files) a week', says Col Thomson. The 'false positives' at SunRice are so low because their software allows administrators to easily set exceptions and bypasses which handle anomalies that would otherwise get categorised as spam.[14] Table 4.10 highlights a few methods an organisation can follow to prevent spam.

TABLE 4.10
Spam prevention tips

› Disguise email addresses posted in a public electronic place. When posting an email address in a public place, disguise the address through simple means such as replacing 'jsmith@domain.com' with 'jsmith at domain dot com'. This prevents spam from recognising the email address.
› Opt out of member directories that may place an email address online. Choose not to participate in any activities that place email addresses online. If an email address is placed online be sure it is disguised in some way.
› Use a filter. Many ISPs and free email services now provide spam filtering. While filters are not perfect, they can cut down tremendously on the amount of spam a user receives.

ETHICS IN THE WORKPLACE

Concern is growing among employees that infractions of corporate policies—even accidental ones—will be a cause for disciplinary action. The whitehouse.gov Internet site displays the US president's official website and updates on bill signings and new policies. However, whitehouse.com leads to a parody site that lampoons the famous office, and before that, whitehouse.com was a trashy, pornographic website. A simple mistype from .gov to .com could once have potentially cost someone her or his job if the company had a termination policy for viewing illicit websites. Monitoring employees is one of the largest issues facing CIOs when they are developing information management policies.

Legal precedents that hold businesses financially responsible for their employees' actions drives the decision of whether to monitor what employees do on company time with corporate resources. Increasingly, employee monitoring is not a choice; it is a risk-management obligation. Michael Soden, CEO of the Bank of Ireland, issued a mandate stating that company employees could not surf illicit websites with company equipment. Next, he hired Hewlett-Packard to run the IT department. A Hewlett-Packard employee soon discovered illicit websites on Soden's computer. Soden resigned.[15]

Surveillance of employees in the workplace remains a controversial topic. A survey conducted on behalf of the Australian Privacy Commissioner found that 23 per cent of people believe that employers should be able to read emails sent to their employees' work accounts whenever they choose. However, 34 per cent believe they should not have this right at all and 38 per cent believe they should only be able to do so if they suspect the employee of wrong-doing. Respondents to the survey had similar feelings regarding employers monitoring what is typed into a work computer or using surveillance equipment.[16]

Monitoring technologies

Many employees use their company's high-speed Internet access to shop, browse and surf the web. Fifty-nine per cent of all 2004 web purchases in the United States were made from the workplace, according to ComScore Networks. Vault.com determined that 47 per cent of employees spend at least half an hour a day surfing the web.[17]

According to a 2008 University of Melbourne study, workers who are allowed to use the Internet for personal reasons during the working day are actually 9 per cent more productive than workers who have restricted use.[18] However, there are negatives to surfing while using work computer infrastructure and time, as the Adelaide Metropolitan Fire Service (MFS) discovered. After an investigation into employee Internet usage found that many staff were using the Internet for 'well over 10 hours per month ... [and] ... accessing inappropriate sites', staff were warned that the MFS had 'zero tolerance' when it came to viewing inappropriate sites. 'All staff Internet usage is monitored, making us confident our workforce does not misuse the Internet', said the MFS senior public affairs officer Nicole Ely.[19]

This research indicates that managers should monitor what their employees are doing with their web access. Most managers do not want their employees conducting personal business during working hours. For these reasons many organisations have increasingly taken the Big Brother approach to web monitoring with software that tracks Internet usage and even allows the boss to read employees' email. However, it's debatable whether or not this is a good thing. Table 4.11 highlights a few reasons the effects of employee monitoring are worse than the lost productivity from employee web surfing.

TABLE 4.11
Employee monitoring effects

1	Employee absenteeism is on the rise. The Australian Bureau of Statistics research indicates that 37 per cent of absences from work are either sick leave or unapproved leave.[20] The lesson here might be that more employees are missing work to take care of personal business. Perhaps losing a few minutes here or there—or even a couple of hours—is cheaper than losing entire days.
2	Studies indicate that electronic monitoring results in lower job satisfaction, in part because people begin to believe the quantity of their work is more important than the quality.
3	Electronic monitoring also induces what psychologists call 'psychological reactance': the tendency to rebel against constraints. If you tell your employees they cannot shop, they cannot use corporate networks for personal business, and they cannot make personal phone calls, then their desire to do all these things will likely increase.

This is the thinking at SAS Institute, a private software company consistently rated as an employer of choice in the US. SAS does not monitor its employees' web usage. The company asks its employees to use company resources responsibly, but does not mind if they occasionally check sports scores or use the web for shopping.

Many management gurus advocate that organisations whose corporate cultures are based on trust are more successful than those whose corporate cultures are based on distrust. Before an organisation implements monitoring technology it should ask itself, 'What does this say about how the organisation feels about its employees?' If the organisation really does not trust its employees, then perhaps it should find new ones. If

FIGURE 4.3
Big Brother eyes: workplace monitoring has risks and rewards

an organisation does trust its employees, then it might want to treat them accordingly. An organisation that follows its employees' every keystroke is unwittingly undermining the relationships with its employees.[21]

Information technology monitoring is tracking people's activities by such measures as number of keystrokes, error rate and number of transactions processed. Table 4.12 displays different types of monitoring technologies currently available.

TABLE 4.12
Common monitoring technologies

Key logger, or key trapper, software	A program that, when installed on a computer, records every keystroke and mouse click.
Hardware key logger	A hardware device that captures keystrokes on their journey from the keyboard to the motherboard.
Cookie	A small file deposited on a hard drive by a website containing information about customers and their web activities. Cookies allow websites to record the comings and goings of customers, usually without their knowledge or consent.
Adware	Software that generates ads that install themselves on a computer when a person downloads some other program from the Internet.
Spyware (sneakware or stealthware)	Software that comes hidden in free downloadable software and tracks online movements, mines the information stored on a computer, or uses a computer's CPU and storage for some task the user knows nothing about.
Web log	Consists of one line of information for every visitor to a website and is usually stored on a web server.
Clickstream	Records information about a customer during a web surfing session such as what websites were visited, how long the visit was, what ads were viewed and what was purchased.

Monitoring employee behaviour should not just extend to the employee, but to how employees monitor each other. In 2002 a 14-year-old Canadian boy named Ghyslain Raza innocently swung a golf-ball retriever around in a quiet corner of his high school, pretending he was *The Phantom Menace's* Darth Maul. He videotaped it and left the tape at school, where it was found several months later. Not long after, Raza became an Internet sensation, known today as the 'Star Wars kid', with fans adding lightsabre effects and music and creating video revisions that number over a hundred. The embarrassing footage has since become one of the Internet's most popular, having been spoofed on TV shows ranging from *American Dad* to *The Colbert Report* to *Arrested Development*. In 2003, Raza sued the individuals who posted the video online, and the case was settled.

Employee monitoring policies

Employees are known to engage in a little private chitchat with their co-workers, but how would they feel if the conversation was broadcast during a live newscast? When newsreader Marie-Louise Thiele chatted to her co-anchor, complaining that her husband was an 'arsehole' for wanting to go on a ski trip, she didn't realise that she was live on television. Although Thiele was able to apologise publicly on air the following evening, an organisation must ensure its employees are comfortable with any monitoring it is undertaking, including during work breaks.

The best path for an organisation planning to engage in employee monitoring is open communication surrounding the issue. A recent survey discovered that communication about monitoring issues is weak for most organisations. One in five companies did not even have an acceptable use policy and one in four companies did not have an Internet use policy. Companies that did have policies usually tucked them into the rarely probed recesses of the employee handbook, and they tended to be of the vague and legal jargon variety: 'XYZ company reserves the right to monitor or review any information stored or transmitted on its equipment'. Reserving the right to monitor is materially different from clearly stating that the company does monitor, listing what is tracked, describing what is looked for and detailing the consequences for violations.

An organisation must formulate the right monitoring policies and put them into practice. Employee monitoring policies explicitly state how, when and where the company monitors its employees. Chief security officers (CSOs) who are explicit about what the company does in the way of monitoring and the reasons for it, along with actively educating employees about what unacceptable behaviour looks like, will find that employees not only acclimate quickly to a policy, but also reduce the CSO's burden by policing themselves. Table 4.13 displays several common stipulations an organisation can follow when creating an employee monitoring policy.

In response to *Privacy at Work: A Guide to the* Privacy Act *for Employers and Employees,* organisers of New Zealand's 2008 Privacy Awareness Week published a small booklet titled *Is your Info Floating Around out There?* The book gives tips on use of technology in the workplace, such as monitoring staff email and Internet use, or GPS tracking and finger-scanning. It also offers guidance about handling personal information on databases—including unauthorised employee 'browsing' of client records.[22]

1	Be as specific as possible.
2	Always enforce the policy.
3	Enforce the policy in the same way for everyone.
4	Expressly communicate that the company reserves the right to monitor all employees.
5	Specifically state when monitoring will be performed.
6	Specifically state what will be monitored (email, IM, Internet, network activity, etc.).
7	Describe the types of information that will be collected.
8	State the consequences for violating the policy.
9	State all provisions that allow for updates to the policy.
10	Specify the scope and manner of monitoring for any information system.
11	When appropriate, obtain a written receipt acknowledging that each party has received, read and understood the monitoring policies.

TABLE 4.13 Employee monitoring policy stipulations

Case Study

Keeping a record: your record retention obligations

1. Explain how an effective record retention system can also help an organisation to act ethically.
2. Why is records management an area of concern for the entire organisation and not just the IT department?
3. Identify two issues an organisation must consider when implementing a record retention system.
4. What costly legal issue could organisations avoid by implementing a record retention system?
5. What is the biggest ethical roadblock for organisations attempting to implement a record retention system?

4.2 INFORMATION SECURITY

LEARNING OUTCOMES

- Describe the relationship between information security policies and an information security plan.
- Summarise the five steps to creating an information security plan.
- Provide an example of each of the three primary information security areas: (1) authentication and authorisation, (2) prevention and resistance and (3) detection and response.
- Describe the relationships and differences between hackers and viruses.

HOW MUCH WILL DOWNTIME COST YOUR BUSINESS?

The old business axiom 'time is money' needs to be updated to more accurately reflect the crucial interdependence between IT and business processes. To reflect the times, the phrase should state 'uptime is money'. The leading cause of downtime is a software failure followed by human error, according to Infonetics research. Unplanned downtime can strike at any time from any number of causes, ranging from cyclones to sink overflows to network failures to power outages. Although natural disasters may appear to be the most devastating causes of IT outages, they are hardly the most frequent or biggest threats to uptime. Table 4.14 highlights sources of unplanned downtime.

According to the Gartner Group, on average, enterprises lose US$108 000 of revenue every hour their IT infrastructure is down. Figure 4.4 displays the four categories associated with downtime, according to the Gartner Group. A few questions companies should ask when determining the cost of downtime include:

- How many transactions can the company afford to lose without significantly impacting business?
- Does the company depend upon one or more mission-critical applications to conduct business?
- How much revenue will the company lose for every hour a critical application is unavailable?
- What is the productivity cost associated with each hour of downtime?
- How will collaborative business processes with partners, suppliers and customers be affected by an unexpected IT outage?
- What is the total cost of lost productivity and lost revenue during unplanned downtime?

TABLE 4.14
Sources of unplanned downtime

Bomb threat	Fraud	Shredded data
Burst pipe	Hacker	Snowstorm
Chemical spill	Hail	Static electricity
Construction	Ice storm	Strike
Corrupted data	Insects	Terrorism
Cyclone	Lightning	Theft
Earthquake	Network failure	Train derailment
Electrical short	Plane crash	Smoke damage
Epidemic	Frozen pipe	Vandalism
Equipment failure	Power outage	Vehicle crash
Explosion	Power surge	Virus
Fire	Rodents	Water damage (various)
Flood	Sabotage	Wind

The reliability and resilience of IT systems have never been more essential for success as businesses cope with the forces of globalisation, 24/7 operations, government and trade regulations and overextended IT budgets and resources. Any unexpected IT downtime in today's business environment has the potential to cause both short- and long-term costs with far-reaching consequences. Section 4.2 explains how you can use security to combat the threat of downtime. Understanding how to secure a business network is critical to keeping downtime to a minimum and uptime to a maximum.

PROTECTING INTELLECTUAL ASSETS

Organisational information is intellectual capital. Just as organisations protect their assets—keeping their money in an insured bank or providing a safe working environment for employees—they must also protect their intellectual capital. An organisation's intellectual capital includes everything from its patents to its transactional and analytical information. With security breaches on the rise and computer hackers everywhere, an organisation must put in place strong security measures to survive.

Health service providers appear to be having the most difficulty complying with the *Privacy Act 1988*. Of the cases considered by the Federal Privacy Commissioner in 2008, health service providers appeared before the Commissioner more than any other group.

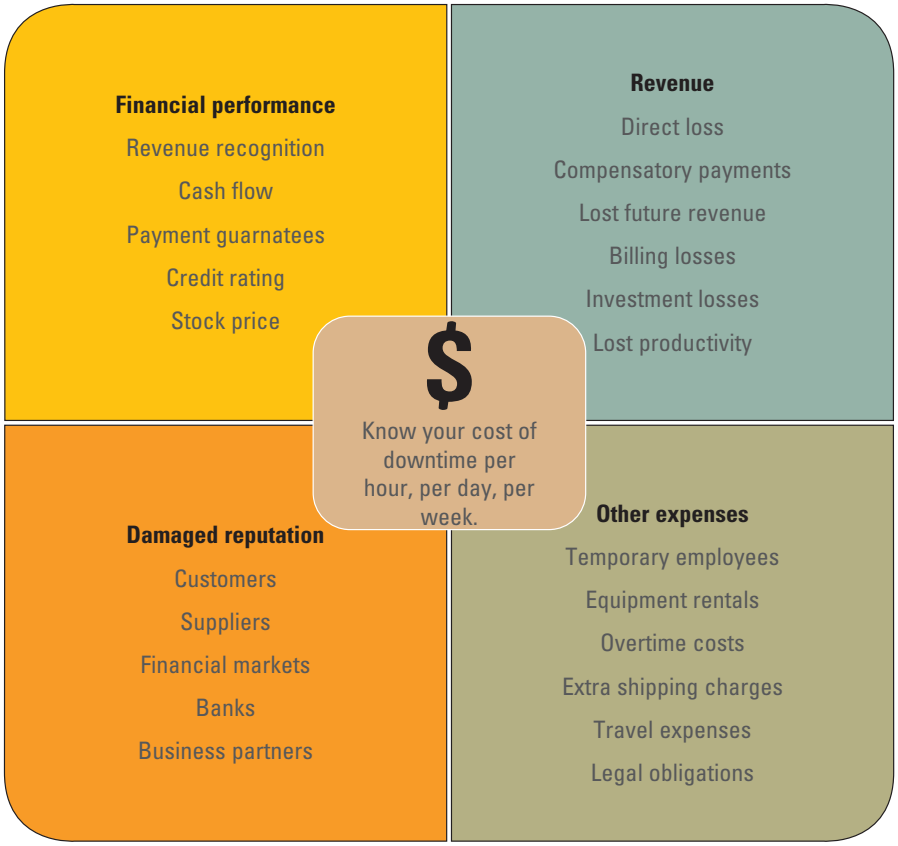


FIGURE 4.4 The cost of downtime

Providers have been accused of improper disclosure of personal information, unauthorised access to personal information, failing to destroy personal information after it is no longer needed and failing to keep personal information secure.

Beyond the health care industry, all businesses must understand the importance of information security, even if it is not enforceable by law. **Information security** is a broad term encompassing the protection of information from accidental or intentional misuse by persons inside or outside an organisation. The 2007 Global State of Information Security Study, conducted jointly by *CIO* and *CSO* magazines with PricewaterhouseCoopers, 'elicits insights on security and privacy practices from 7200 IT, security and business executives across all industries and more than 100 countries'. The study found that information technology accounted for 65 per cent of information security funding for the year.

A survey conducted by IDC, a subsidiary of International Data Group, with Australian and New Zealand CIOs[23] found that security has fallen down the list of CIO top concerns, and the level of security confidence has increased significantly. The survey shows that 63 per cent of Australian and 51 per cent of New Zealand respondents are very or extremely confident in their organisations' level of IT security. Interestingly, according to a 2008 report by research house Gartner, IT security professionals in Asia-Pacific organisations spend a larger proportion of their IT budget on security than their North American and European counterparts.[24] The average percentage of the IT budget dedicated to security in the Asia Pacific region is around 15 per cent, according to the survey. Despite an economic downturn in the US, 40 per cent of Asia-Pacific organisations surveyed said their 2008 IT security budget has increased over 2007 levels, while 45 per cent claimed it had remained roughly the same.

Security is perhaps the most fundamental and critical of all the technologies/disciplines an organisation must have squarely in place to execute its business strategy. Without solid security processes and procedures, none of the other technologies can develop business advantages.

THE FIRST LINE OF DEFENCE—PEOPLE

With current advances in technologies and business strategies, organisations are able to determine valuable information such as who are the top 20 per cent of the customers that produce 80 per cent of all revenues. Most organisations view this type of information as valuable intellectual capital, and they are implementing security measures to prevent the information from walking out the door or falling into the wrong hands. Enterprises can implement information security lines of defence through people first and through technology second.

Adding to the complexity of information security is the fact that organisations must enable employees, customers and partners to access information electronically to be successful in this electronic world. Doing business electronically automatically creates tremendous information security risks for organisations. Surprisingly, the biggest issue surrounding information security is not a technical issue, but a people issue.

Most information security breaches result from people misusing an organisation's information either advertently or inadvertently. For example, many individuals freely give

up their passwords or write them on sticky notes next to their computers, leaving the door wide open to intruders.[25]

The director of information security at a large health care company discovered how easy it was to create an information security breach when she hired outside auditors to test her company's security awareness. In one instance, auditors found that staff members testing a new system had accidentally exposed the network to outside hackers. In another, auditors were able to obtain the passwords of 16 employees when the auditors posed as support staff; hackers frequently use such 'social engineering' to obtain passwords. **Social engineering** is using one's social skills to trick people into revealing access credentials or other information valuable to the attacker. Dumpster diving, or looking through people's trash, is another way social engineering hackers obtain information.[26]

Information security policies identify the rules required to maintain information security. An information security plan details how an organisation will implement the information security policies. Table 4.15 is an example of the University of the Sunshine Coast's information and communication technology (ICT) security policy.[27]

The first line of defence an organisation should follow is to create an **information security plan** detailing the various **information security policies**. A detailed information security plan can alleviate people-based information security issues. Table 4.16 displays the five steps for creating an information security plan.

TABLE 4.15
Sample Information Security Plan

University of the Sunshine Coast Security Plan, 2009 draft version
Purpose This policy creates a framework that reduces the risks of an ICT security incident occurring and promotes the ability to recover effectively and efficiently in the event of an ICT-related service disruption. Furthermore, it aims to ensure that information systems are managed in accordance with the principles outlined in the State Government's Information Standard IS18 and the ISO/IEC 27001 standard. This policy applies to all staff, students and other members of the University community who may access the University's ICT resources. (The information and communication technology (ICT) resources of the University include information systems and associated computer devices, networks and communications facilities.) **POLICY (excerpt)** **Information System Classification** Each Information System will require its own level of security based on its Information Classification. The University classifies Information Systems within the following categories: public, internal and restricted. **Physical and System Access Control** › Physical access controls for the University premises are to be implemented in accordance with the risk and the importance of the Information Asset to be protected. › Security risks should be assessed as part of the decision for locating the Information Assets, particularly where this is to occur offsite from University premises. › Appropriate control mechanisms (e.g. username and password) must be in place for authenticating access to all non-Public Information Systems and Information Assets. Access control must be in accordance with the Information Classification.

Continued

- In assessing risks to Information Systems, the Business Systems Owner must consider the security of the information in all media formats that are used (e.g. hardcopy). Furthermore, consideration is required when information may be stored on mobile equipment which can be transported offsite.
- Remote access to Restricted Information Systems will only be provided with the explicit authorisation of the Business System Owner.
- **Operations Management**
- Appropriate systems will be in place to facilitate the detection and prevention of malicious software into the University's ICT environment (e.g. the use of antivirus software).
- Appropriate activity logging will be in place for all Information Systems.
- ICT Security incidents will be dealt with in a manner consistent with the University's Critical Incident Management—Institutional Operating Policy.
- Confidential information is only to be transmitted across any accessible part of the network in an encrypted manner.

Compliance

- The University monitors and logs activity on its Information Systems and carries out security audits as required. These activities may be used to investigate faults, security breaches, inappropriate use or unlawful activity. For the diagnosis of problems, investigation of issues or for security audits, the University reserves the right to access individual files.
- Breaches of this policy shall be treated as misconduct or serious misconduct and are dealt with under relevant University statutes, rules and policies including the Code of Conduct and the Student Conduct and Discipline Policy.

TABLE 4.16
Creating an information security plan

Five steps for creating an information security plan	
1 Develop the information security policies	Identify who is responsible and accountable for designing and implementing the organisation's information security policies. Simple, yet highly effective types of information security policies include requiring users to log off their systems before leaving for lunches or meetings, never sharing passwords with anyone and changing personal passwords every 60 days. The chief security officer (CSO) will typically be responsible for designing these information security policies.
2 Communicate the information security policies	Train all employees on the policies and establish clear expectations for following the policies. For example, let all employees know that they will receive a formal reprimand for leaving a computer unsecured.
3 Identify critical information assets and risks	Require the use of user IDs, passwords and antivirus software on all systems. Ensure any systems that contain links to external networks have the appropriate technical protections such as firewalls or intrusion detection software. A firewall is hardware and/or software that guards a private network by analysing the information leaving and entering the network. **Intrusion detection software (IDS)** searches out patterns in information and network traffic to indicate attacks and quickly responds to prevent any harm.
4 Test and re-evaluate risks	Continually perform security reviews, audits, background checks and security assessments.
5 Obtain stakeholder support	Gain the approval and support of the information security polices from the board of directors and all stakeholders.

Businesses consider desktop users to be the biggest security risk to their networks, despite increased concern over outsourced labour and remote users. Recent breaches of privacy regulations governing the Australian Commonwealth public sector have resulted in both the warning and firing of Centrelink staff. Investigations found 547 instances where breaches occurred and 367 'proven breaches'. The majority of breaches in this instance occurred by way of staff accessing client records. In response, Centrelink issued written warnings, fines and reprimands. Twenty-four staff resigned as a consequence (this came on top of 100 resignations for the same reason the previous year).[28]

Table 4.17 provides the top 10 questions that managers should ask to ensure their information is secure, according to Ernst & Young.

TABLE 4.17
Top 10 questions managers should ask regarding information security

1	Does our board of directors recognise information security is a board-level issue that cannot be left to the IT department alone?
2	Is there clear accountability for information security in our organisation?
3	Do our board members articulate an agreed-upon set of threats and critical assets? How often do we review and update these?
4	How much is spent on information security and what is it being spent on?
5	What is the impact on the organisation of a serious security incident?
6	Does our organisation view information security as an enabler? (For example, by implementing effective security, could we enable our organisation to increase business over the Internet?)
7	What is the risk to our business of getting a reputation for low information security?
8	What steps have we taken to ensure that third parties will not compromise the security of our organisation?
9	How do we obtain independent assurance that information security is managed effectively in our organisation?
10	How do we measure the effectiveness of our information security activities?

THE SECOND LINE OF DEFENCE—TECHNOLOGY

The University of Western Sydney (UWS) recently completed a major network upgrade that facilitates network access and provides IT support for staff and UWS's 38 000 students. UWS has installed an 'active' Intrusion Detection System (IDS) that deals with an attack on the network by shutting off access to the system. A 'passive' system simply logs the intrusion and alerts IT support. 'Universities don't want to be denied access to anything [on the Internet] ... so we need an active IDS to monitor traffic', said UWS IT security coordinator Darren Geddes.[28]

Once an organisation has protected its intellectual capital by arming its people with a detailed information security plan, it can begin to focus its efforts on deploying the right types of information security technologies such as the IDS installed at the University of Western Sydney.

Organisations can deploy numerous technologies to prevent information security breaches. When determining which types of technologies to invest in, it helps to understand the three primary information security areas:

1 authentication and authorisation;

2 prevention and resistance;

3 detection and response.[30]

Authentication and authorisation

Authentication is a method for confirming users' identities. Once a system determines the authentication of a user, it can then determine the access privileges (or authorisation) for that user. **Authorisation** is the process of giving someone permission to do or have something. In multiple-user computer systems, user access or authorisation determines such things as file access, hours of access and amount of allocated storage space. Authentication and authorisation techniques are broken down into three categories, and the most secure type involves a combination of all three:

1 Something the user knows, such as a user ID and password.

2 Something the user has, such as a smart card or token.

3 Something that is part of the user, such as a fingerprint or voice signature.

Something the user knows, such as a user ID and password

The first type of authentication, using something the user knows, is the most common way to identify individual users and typically consists of a unique user ID and password. However, this is actually one of the most ineffective ways for determining authentication because passwords are not secure. All it typically takes to crack a password is enough time. More than 50 per cent of help-desk calls are password related, which can cost an organisation significant money, and passwords are vulnerable to being coaxed out of somebody by a social engineer.[31]

Identity theft is the forging of someone's identity for the purpose of fraud. The fraud is often financial fraud, to apply for and use credit cards in the victim's name or to apply for a loan. By 2003, online banking was not yet ubiquitous but everyone could see that, eventually, it would be. 'Everyone' in this case includes Internet criminals, who by then had already built software capable of surreptitiously grabbing personal information from online forms, like the ones used for online banking. The first of these so-called form-grabbing viruses was called Berbew and was wildly effective. Lance James, a researcher with Secure Science Corporation, believes it operated undetected for as long as nine months and grabbed as much as 113 GB of data—millions of personal credentials. Like all exploits, Berbew was eventually detected and contained, but, as is customary with viruses, strands of Berbew's form-grabbing code were stitched into new viruses that had adapted to defences. The process is not unlike horticulturalists' grafting pieces of one plant onto another in order to create hardier stock. Table 4.18 displays several examples of identity theft.

The 2007 Australian Bureau of Statistics survey found that 800 000 Australians experienced a form of personal fraud in the past year, with total losses of almost $1 billion. Over 500 000 were victims of identity fraud, the majority of which was credit or bank card fraud, followed by identity theft.[32]

A Melbourne offender was able to obtain the birth certificates of four babies who passed away in the 1970s. During an eight-month period the offender claimed $20 857 in unemployment benefits. He was able to support his unemployment claims using a variety of identity documents (learner driver permits, mobile phone accounts, student cards, rental documents and bank cards).
A Sydney man was sentenced to six years imprisonment in 2006 after pleading guilty to 55 charges of tax fraud. He used the identities of 17 former clients to create false payment summaries, and lodged 51 income tax returns on their behalf. He will serve four and a half years before being eligible for parole.
An Englishman immigrated to Western Australia. Identity thieves, who obtained his credit card information from an online flower purchase, then contacted his credit card company and informed them that the man had moved back to England, forwarding a new address in East London. The thieves increased the credit card limit and spent $15 000 in computer shops around the UK.

TABLE 4.18
Identity theft examples

Phishing is a common way to steal identities online. **Phishing** is a technique used to gain personal information for the purpose of identity theft, usually by means of fraudulent email. One way to accomplish phishing is to send out email messages that look as though they come from legitimate businesses such as Australian Tax Office, universities, eBay or Amazon. The messages appear to be genuine with official-looking formats and logos. These emails typically ask for verification of important information like passwords and account numbers. The reason given is often that this personal information is required for accounting or auditing purposes. Since the emails look authentic, up to one in five recipients respond with the information, and subsequently become a victim of identity theft and other fraud.

Something the user has, such as a smart card or token

The second type of authentication, using something that the user has, offers a much more effective way to identify individuals than a user ID and password. Tokens and smart cards are two of the primary forms of this type of authentication. **Tokens** are small electronic devices that change user passwords automatically. The user enters his or her user ID and token-displayed password to gain access to the network. A **smart card** is a device that is around the same size as a credit card, containing embedded technologies that can store information and small amounts of software to perform some limited processing. Smart cards can act as identification instruments, a form of digital cash or a data storage device.

Something that is part of the user, such as a fingerprint or voice signature

The third kind of authentication, using something that is part of the user, is by far the best and most effective way to manage authentication. **Biometrics** (narrowly defined) is the identification of a user based on a physical characteristic, such as a fingerprint, iris, face, voice, or handwriting. Unfortunately, biometric authentication can be costly and intrusive, for example, iris scans. Fingerprint authentication is less intrusive and expensive but is also not 100 per cent accurate.

Biometrics are now being used to help make sure that people applying for and using passports are who they say they are. The Australian and New Zealand ePassport uses

biometrics to automatically recognise someone by measuring just one physical trait—the face. The card works by digitising the photograph supplied with a passport application. That digital information is stored in a computer chip within the passport and in a passport database. Biometric technology is then used to check that the image on the passport matches the person trying to use it.[33]

Terms and conditions

There is some difficulty in determining the terms and conditions of online purchases. Companies commonly use two types of methods: 'Clickwrap' and 'Browsewrap'. The latter is where terms and conditions are made available via a web link, but customers are not required to view these conditions when purchasing. The former is where the customer is forced to click on a button or hyperlink, affirming that they have read and agreed to the terms and conditions.

The better of the two methods is the 'Clickwrap' method as it provides greater protection to companies against uncertainty surrounding the nature of the agreement.

Prevention and resistance

Prevention and resistance technologies stop intruders from accessing intellectual capital. A division of Sony Inc., Sony Pictures Entertainment (SPE), defends itself from attacks by using an intrusion detection system to detect new attacks as they occur. SPE develops and distributes a wide variety of products including movies, television, videos and DVDs. A compromise to SPE security could cost the company valuable intellectual capital as well as millions of dollars and months of time. The company needed an advanced threat-management solution that would take fewer resources to maintain and require limited resources to track and respond to suspicious network activity. The company installed an advanced intrusion detection system allowing it to monitor all of its network activity including any potential security breaches.[34]

The cost of downtime or network operation failures can be devastating to any business. For example, eBay experienced a 22-hour outage in June 2000 that caused the company's market cap to plunge an incredible US$5.7 billion. Downtime costs for businesses can vary from $100 to $1 million per hour. An organisation must prepare for and anticipate these types of outages, which result most commonly from the work of hackers and viruses. Technologies available to help prevent and build resistance to attacks include content filtering, encryption and firewalls.[35]

Content filtering

Content filtering occurs when organisations use software that filters content to prevent the transmission of unauthorised information. Organisations can use content filtering technologies to filter email and prevent emails containing sensitive information from transmitting, whether the transmission was malicious or accidental. It can also filter emails and prevent any suspicious files from transmitting such as potential virus-infected files. Email content filtering can also filter for spam, a form of unsolicited email. Organisational losses from spam worldwide were expected to be about US$198 billion in 2007 (see Figure 4.5).[36]

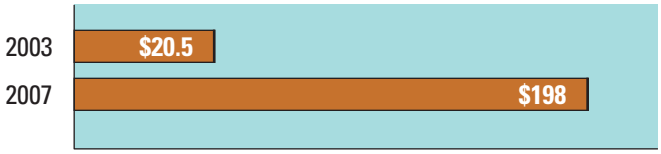


FIGURE 4.5 Worldwide corporate losses caused by spam (2003 and 2007 in US$ billions)

Sean Lane's purchase was supposed to be a surprise for his wife. Then it appeared as a news headline, 'Sean Lane bought 14k white gold 1/5 ct diamond eternity flower ring from overstock.com', on the social networking website Facebook. Without Lane's knowledge, the headline was visible to everyone in his online network, including 500 classmates from Columbia University and 220 other friends, co-workers and acquaintances. And his wife. The wraps came off his Christmas gift thanks to an advertising feature called Beacon, which shares news of Facebook members' online purchases with their friends. The idea, according to the company, is to allow merchants to effectively turn millions of Facebook users into a word-of-mouth promotion service. Lane called it 'Christmas ruined', and more than 50 000 other users signed a petition calling on Facebook to stop broadcasting people's transactions without their consent.

Encryption

Encryption scrambles information into an alternative form that requires a key or password to decrypt the information. If there is an information security breach and the information was encrypted, the person stealing the information will be unable to read it. Encryption can switch the order of characters, replace characters with other characters, insert or remove characters, or use a mathematical formula to convert the information into some sort of code. Companies that transmit sensitive customer information over the Internet, such as credit card numbers, frequently use encryption. Some encryption technologies use multiple keys like public key encryption. **Public key encryption (PKE)** is an encryption system that uses two keys: a public key that everyone can have and a private key for only the recipient (see Figure 4.6). When implementing security using multiple keys, the organisation provides the public key to all of its customers (end consumers and other businesses). The customers use the public key to encrypt their information and

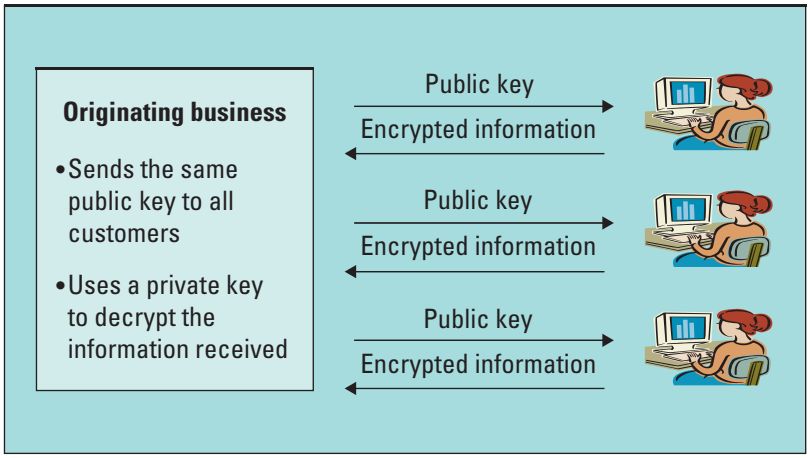


FIGURE 4.6 Public key encryption (PKE) system

send it along the Internet. When it arrives at its destination, the organisation would use the private key to unscramble the encrypted information.

Firewalls

One of the most common defences for preventing a security breach is a firewall. A **firewall** is hardware and/or software that guards a private network by analysing the information leaving and entering the network. Firewalls examine each message that wants entrance to the network. Unless the message has the correct markings, the firewall prevents it from entering the network. Firewalls can even detect computers communicating with the Internet without approval. As Figure 4.7 illustrates, organisations typically place a firewall between a server and the Internet.

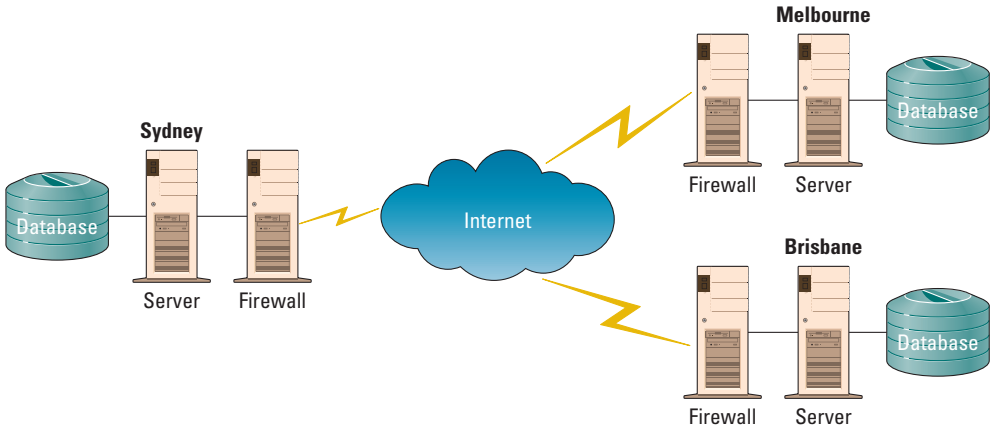


FIGURE 4.7
Sample firewall architecture connecting systems located in Sydney, Melbourne and Brisbane

Detection and response

The final area where organisations can allocate resources is in detection and response technologies. If prevention and resistance strategies fail and there is a security breach, an organisation can use detection and response technologies to mitigate the damage. The most common type of defence within detection and response technologies is antivirus software.

A single worm can cause massive damage. In August 2003, the 'Blaster worm' infected over 50 000 computers worldwide and was one of the worst outbreaks of the year. Jeffrey Lee Parson, 18, was arrested by US cyber investigators for unleashing the damaging worm on the Internet. The worm replicated itself repeatedly, eating up computer capacity, but did not damage information or programs. The worm generated so much traffic that it brought entire networks down.

The FBI used the latest technologies and code analysis to find the source of the worm. Parson, charged with intentionally causing or attempting to cause damage to a computer, was sentenced to 18 months in prison, three years of supervised release and 100 hours of community service. 'What you've done is a terrible thing. Aside from injuring people and their computers, you shook the foundation of technology', US District Judge Marsha Pechman told Parson.

'With this arrest, we want to deliver a message to cyber-hackers here and around the world', said US Attorney John McKay in Seattle. 'Let there be no mistake about it, cyber-hacking is a crime. We will investigate, arrest, and prosecute cyber-hackers.'[37]

The global fight against Internet hackers has reached Australian shores. Hew Griffiths, of New South Wales' central coast region, spent three years in an Australian gaol fighting extradition to the United States on a charge of conspiring to commit a criminal copyright infringement. Eventually, Griffiths was sentenced by a US court to 51 months' jail, backdated to the time of his arrest in Australia.[38]

Typically, people equate viruses (the malicious software) with hackers (the people). While not all types of hackers create viruses, many do. Table 4.19 provides an overview of the most common types of hackers and viruses.

TABLE 4.19 Hackers and viruses

Hackers—people very knowledgeable about computers who use their knowledge to invade other people's computers.

- **White-hat hackers**—work at the request of the system owners to find system vulnerabilities and plug the holes.
- **Black-hat hackers**—break into other people's computer systems and may just look around or may steal and destroy information.
- **Hactivists**—have philosophical and political reasons for breaking into systems and will often deface the website as a protest.
- **Script kiddies or script bunnies**—find hacking code on the Internet and click-and-point their way into systems to cause damage or spread viruses.
- **Cracker**—a hacker with criminal intent.
- **Cyber-terrorists**—seek to cause harm to people or to destroy critical systems or information and use the Internet as a weapon of mass destruction.

Viruses—software written with malicious intent to cause annoyance or damage.

- **Worm**—a type of virus that spreads itself, not only from file to file, but also from computer to computer. The primary difference between a virus and a worm is that a virus must attach to something, such as an executable file, in order to spread. Worms do not need to attach to anything to spread and can tunnel themselves into computers.
- **Denial-of-service attack (DoS)**—floods a website with so many requests for service that it slows down or crashes the site.
- **Distributed denial-of-service attack (DDoS)**—attacks from multiple computers that flood a website with so many requests for service that it slows down or crashes. A common type is the Ping of Death, in which thousands of computers try to access a website at the same time, overloading it and shutting it down.
- **Trojan-horse virus**—hides inside other software, usually as an attachment or a downloadable file.
- **Backdoor programs**—viruses that open a way into the network for future attacks.
- **Polymorphic viruses and worms**—change their form as they propagate.

Some of the most damaging forms of security threats to e-business sites include malicious code, hoaxes, spoofing and sniffers (see Table 4.20).

Implementing information security lines of defence through people first and through technology second is the best way for an organisation to protect its vital intellectual capital. The first line of defence is securing intellectual capital by creating an information

security plan detailing the various information security policies. The second line of defence is investing in technology to help secure information through authentication and authorisation, prevention and resistance and detection and response.

TABLE 4.20
Security threats to e-business

Elevation of privilege is a process by which a user misleads a system into granting unauthorised rights, usually for the purpose of compromising or destroying the system. For example, an attacker might log onto a network by using a guest account, and then exploit a weakness in the software that lets the attacker change the guest privileges to administrative privileges.
Elevation of privilege is a process by which a user misleads a system into granting unauthorised rights, usually for the purpose of compromising or destroying the system. For example, an attacker might log onto a network by using a guest account, and then exploit a weakness in the software that lets the attacker change the guest privileges to administrative privileges.
Hoaxes attack computer systems by transmitting a virus hoax, with a real virus attached. By masking the attack in a seemingly legitimate message, unsuspecting users more readily distribute the message and send the attack on to their co-workers and friends, infecting many users along the way.
Malicious code includes a variety of threats such as viruses, worms and Trojan horses.
Spoofing is the forging of the return address on an email so that the message appears to come from someone other than the actual sender. This is not a virus but rather a way by which virus authors conceal their identities as they send out viruses.
Spyware is software that comes hidden in free downloadable software and tracks online movements, mines the information stored on a computer, or uses a computer's CPU and storage for some task the user knows nothing about. There are no statistics specific to Australia regarding spyware, but anecdotally there has been a significant increase in the amount of spyware on the Internet that has begun to infect Australian computer users.[39] According to a US study conducted by the National Cyber Security Alliance, 91 per cent of respondents had spyware on their computers that can cause extremely slow performance, excessive pop-up ads, or hijacked home pages.
A **sniffer** is a program or device that can monitor data travelling over a network. Sniffers can show all the data being transmitted over a network, including passwords and sensitive information. Sniffers tend to be a favourite weapon in the hacker's arsenal.
Packet tampering consists of altering the contents of packets as they travel over the Internet or altering data on computer disks after penetrating a network. (In the telecommunications arena, a 'packet' is a discrete unit of information transmitted through a data network.) For example, an attacker might place a tap on a network line to intercept packets as they leave the computer. The attacker could eavesdrop or alter the information as it leaves the network.

Case Study

Keeping a record: your record retention obligations

6 What information security dilemmas are solved by implementing a record retention system?

7 How can a record retention system help protect a company's information security?

8 What impact does implementing a record retention have on information security in a small business?

9 What is the biggest information security roadblock for organisations attempting to implement a record retention system?

Summary

SUMMARY OF KEY THEMES

The purpose of this chapter was to highlight the need for organisations to protect information from misuse. Discussion first centred on the concept of information ethics and how organisations need to be aware of the moral issues surrounding the development and use of information and information technology. Information privacy was examined with an emphasis placed on understanding the legal obligations and general expectations on organisations in terms of how personal information is collected, shared and stored. Information security includes the two levels of defence that organisations have to protect their information resources: people and technology.

You, the business student, must understand that ethics and security of information and information technology are of paramount importance in organisations today. Organisations that fail to meet these obligations not only face legal repercussions, but also the wrath of consumers who have high expectations on how their personal information is handled by companies.

Business Link One

Banks banking on security

Revised and updated by redchip lawyers

ANZ Bank

ANZ Bank was the victim of a multi-million dollar scam where a former Vietnamese refugee, 48-year-old Ho Van Nguyen, was gaoled for attempting fraud using stolen cheques. The perpetrator had been using stolen blank bank cheques and depositing large sums into various accounts in Vietnam. He used various methods to transfer the money including using a stolen cheque to deposit $856 050 into the account of a business which remits money from Australia to Vietnam. He then visited a Melbourne office of the business, compelling staff members to transfer the money for him immediately.

Nguyen attempted to defraud the bank of AU $5 million. A Melbourne court found him guilty of two counts of attempting to obtain financial advantage by deception and two counts of attempted theft. He was sentenced to three years in gaol.

This highlights how increasingly difficult it is to protect information against fraud schemes as the market value of personal information grows. In the past, banks were wary of the cost or customer backlash from adopting network security technologies. Today, banks are beefing up network security as more customers begin to view security as a key factor when choosing a bank.

Westpac Bank

Westpac Bank has strengthened its online protection procedures recently via an added layer of security known as Extended Validation Certificates. A green address bar will be revealed to Westpac's customers when using compatible browsers, ensuring them that they're on legitimate and safe Westpac websites.

Extended Validation Certificates require organisations to complete a thorough documentation process verifying their current business licensing and incorporation paperwork. They also require proof of the entity named on the certificate having authorised the issuing of the certificate.

Westpac aims to increase customer confidence in their online transactions and to reduce the threat of hacker attacks.

National Bank of Australia (NAB)

NAB has enabled its customers to bank online with more confidence and security with the implementation of an extra layer of protection called Password Lock. The customer is able to manually lock or unlock their Internet banking password, thus making their bank account available only when they need it to be.

NAB introduced this security mechanism for times when the computer environment is not within the customer's control. It enables customers to lock their password before

logging out. They can then only access or unlock the account again by calling a number and entering their Internet banking password. This method allows control for customers and peace of mind over the level of protection they wish to have over their banking.

e-Trade Financial Corporation

e-Trade Financial Corporation provides customers with account balances exceeding US$50 000 with a free Digital Security ID for network authentication. The device displays a new six-digit code every 60 seconds, which the customer must use to log on. Customers with accounts under US$50 000 can purchase the Digital Security ID device for US$25.

Barclay's Bank

Barclay's Bank instituted online-transfer delays of between several hours and one day. The delays, which apply the first time a transfer is attempted between two accounts, are intended to give the bank time to detect suspicious activity, such as a large number of transfers from multiple accounts into a single account. The online-transfer delay was adopted in response to a wave of phishing incidents in which thieves transferred funds from victims' bank accounts into accounts owned by 'mules'. Mules are people who open bank accounts based on an email solicitation, usually under the guise of a business proposal. From the mule accounts, the thieves withdraw cash, open credit cards, or otherwise loot the account.

Barclay's also offers accounts of customer's actions to compare them with historical profile data to detect unusual behaviour. For instance, the service would alert the bank to contact the customer if the customer normally logs on from England and suddenly logs on from New York and performs 20 transactions.[40]

Questions

1. What reason would a bank have for not wanting to adopt an online-transfer delay policy?
2. What are the two primary lines of security defence and why are they important to financial institutions?
3. Explain the differences between the types of security offered by the banks in the examples above. Which bank would you open an account with and why?
4. What additional types of security, not mentioned in the examples above, would you recommend a bank implement?
5. Identify three policies a bank should implement to help it improve information security.
6. Describe monitoring policies along with the best way for a bank to implement monitoring technologies.

Business Link Two

Sarbanes-Oxley: Where information technology, finance and ethics meet

Revised and updated by Peter Blakey, Massey University

US Congress is cleaning up the way companies do business after accounting and governance scandals rocked investor confidence and damaged the reputation of companies large and small. The high-profile Enron, Tyco and WorldCom financial scandals, among others, exposed significant problems with conflicts of interest and incentive compensation practices. The *Sarbanes-Oxley Act* (SOX) of 2002 was enacted in response to these scandals, to protect shareholders and the public from accounting errors and fraudulent practices by organisations.

Sarbanes-Oxley

One primary component of the SOX is the definition of which records are to be stored and for how long. For this reason, the legislation not only affects financial departments but also IT departments, whose job it is to store electronic records. SOX states that all business records, including electronic records and electronic messages, 'must be saved for not less than five years'. The consequences for non-compliance are fines, imprisonment, or both. Three rules of Sarbanes-Oxley affecting the management of electronic records address the following areas:

- the destruction, alteration, or falsification of records;
- the retention period for records storage;
- the business records and communications that need to be stored, including electronic communications.

American IT departments are facing the challenge of creating and maintaining a corporate records archive in a cost-effective fashion that satisfies the requirements put forth by the legislation. Essentially, any public organisation that uses IT as part of its financial business processes must implement IT controls to comply with SOX. The cost of implementing SOX is high, estimated to be US$35 million per year for large companies. William D. Zollars, CEO of Yellow Roadway Corporation, the US's largest trucking firm, said, 'It requires an army of people to do the paperwork'. Zollars dispatched 200 people to work on SOX compliance, paying more than US$9 million for the work—roughly 3 per cent of annual profits.

Benefits from *Sarbanes-Oxley*

Many businesses are promoting the benefits they received from implementing SOX. General Electric Co., which spent about $30 million on SOX compliance, has added controls that

boost investors' confidence in the company. United Technologies used SOX to standardise bookkeeping audits in its disparate businesses around the world. The biggest advantage of all, though, may be the greater confidence investors have in financial results.

Some officials expected it to take until 2008 for companies, auditors and regulators to apply the law efficiently. That might appear to be a long time, and it may seem to be expensive; however, it is a small price to pay to help organisations run smoothly and renew investor confidence.

Debate continues over the perceived benefits and costs of SOX. Supporters contend that the legislation was necessary and has played a useful role in restoring public confidence in the nation's capital markets by, among other things, strengthening corporate accounting controls. Opponents of the Act claim that it has reduced America's international competitive edge against foreign financial service providers, claiming that SOX has introduced an overly complex and regulatory environment into US financial markets.

The effect of *Sarbanes-Oxley* on non-US companies

The *Sarbanes-Oxley Act's* effect on non-US companies cross-listed in the US is different for firms from countries with developed and well-regulated economies than for firms from less developed or poorly regulated countries. Companies from less developed countries benefit from better credit ratings by complying with regulations in a highly regulated country (for example, the US). Companies from developed countries incur the cost of compliance with but, as transparency is adequate in their home countries, they reap few benefits. On the other hand, the benefit of better credit rating also comes with listing on other stock exchanges such as the London Stock Exchange.

The effect on smaller public companies

The cost of complying with SOX impacts smaller companies disproportionately, as there is a significant fixed cost involved in completing the assessment. For example, during 2004 US companies with revenues exceeding US$5 billion spent .06 per cent of revenue on SOX compliance, while companies with less than $100 million in revenue spent 2.55 per cent.

An extension was granted by the Securities and Exchange Commission for the outside auditor assessment until years ending after 15 December 2009. The reason for the timing disparity was to address the concern of the House Committee on Small Business that the cost of complying with the *Sarbanes-Oxley Act* of 2002 was still unknown and could be disproportionately high for smaller publicly held companies.[41]

Questions

1. Define the relationship between ethics and the *Sarbanes-Oxley Act*.
2. Why is records management an area of potential concern for the entire organisation and not just the IT department?
3. What impact does implementing *Sarbanes-Oxley* have on information security in a small business?
4. What ethical dilemmas could be solved by implementing *Sarbanes-Oxley*?
5. How can *Sarbanes-Oxley* help protect a company's information security?

Business Link Three

Executive dilemmas in the information age

The vast array of business initiatives from supply chain management, customer relationship management, business process re-engineering and enterprise resource planning makes it clear that information technology has evolved beyond the role of mere infrastructure to the support of business strategy. Today, in more and more industries, IT is a business strategy and is quickly becoming a survival issue.

Board and executive team agendas are increasingly peppered with, or even hijacked by, a growing range of IT issues from compliance to ethics and security. In most companies today, computers are key business tools. They generate, process and store the majority of critical business information. Executives must understand how IT can affect a business by successfully addressing a wide range of needs—from large electronic discovery projects to the online review of document collections by geographically dispersed teams. A few examples of executive IT issues follow.

Stolen proprietary information

A computer company investigated to determine whether an executive who accepted a job with a competitor stole proprietary information. The hard drive from the executive's laptop and desktop machine were forensically imaged. The analysis established that the night before the executive left, he downloaded all of the company's process specifications and distributor agreements, which he then zipped and emailed to the competitor. Additionally, reconstruction of deleted files located emails between the executive and the competitor discussing his intent to provide the proprietary information if he was offered additional options in the new company.

Sexual harassment

A woman employed by a large defence contractor accused her supervisor of sexual harassment. The woman was fired from her job for poor performance and subsequently sued her ex-boss and the former employer.

A computer company was retained by the plaintiff's attorneys to investigate allegations of the former supervisor's harassing behaviour. After making a forensic image backup of the ex-boss's hard drive, the forensic company was able to recover deleted electronic messages that showed the ex-boss had a history of propositioning women under his supervision for 'special favours'. A situation that might have been mired in a 'he said/she said' controversy was quickly resolved; the woman got her job back, and the real culprit was sacked.

Stolen trade secrets

The board of directors of a technical research company demoted the company's founder and CEO. The executive, disgruntled because of his demotion, was later terminated. It was subsequently determined that the executive had planned to quit about the same time he was fired and establish a competitive company. Upon his termination, the executive took home two computers; he returned them to the company four days later, along with another company computer that he had previously used at home. Suspicious that critical information had been taken, the company's attorneys sent the computers to a computer forensic company for examination.

After making a forensic image backup of the hard drives, the forensic analysis identified a file directory that had been deleted during the aforementioned four-day period. This directory had the same name as the competing company the executive had established. A specific search of the deleted files in this directory identified the executive's 'to do list' file. This file indicated the executive planned to copy the company's database (valued at US$100 million) for his personal use. Another item specified the executive was to 'learn how to destroy evidence on a computer'.

The computer forensic company's examination also proved that the executive had been communicating with other competing companies to establish alliances, in violation of the executive's non-disclosure agreement with the company. It was also shown that numerous key company files were located on removable computer storage media that had not been turned over by the executive to the company.[42]

Questions

1. Explain why understanding technology, especially in the areas of security and ethics, is important for a CEO. How do a CEO's actions affect the organisational culture?
2. Identify why executives in non-technological industries need to worry about technology and its potential business ramifications.
3. Describe why continuously learning about technology allows an executive to better analyse threats and opportunities.
4. Identify three things that a CTO CPO or CSO could do to prevent the above issues.

Making Business Decisions

1. Firewall decisions

You are the CEO of Inverness Investments, a medium-sized venture capital firm that specialises in investing in high-tech companies. The company receives over 30 000 email messages per year. On average, there are two viruses and three successful hackings against the company each year, which result in losses to the company of about $250 000 per year. Currently, the company has antivirus software installed but does not have any firewalls.

Your CIO is suggesting implementing 10 firewalls for a total cost of $80 000. The estimated life of each firewall is about three years. The chances of hackers breaking into the system with the firewalls installed are about 3 per cent. Annual maintenance costs on the firewalls is estimated around $15 000. Create an argument for or against supporting your CIO's recommendation to purchase the firewalls. Are there any considerations in addition to finances?

2. Preventing identity theft

The Australian Bureau of Statistics states that identity theft is a major source of personal fraud throughout Australia. If you are a victim of identity theft, your financial reputation can be ruined, making it impossible for you to cash a cheque or receive a bank loan. Learning how to avoid identity theft can be a valuable activity. Research the following websites and draft a document stating the best ways to prevent identity theft.

- the Australian Competition and Consumer Commission Scamwatch website at www.scamwatch.gov;
- the Australian Institute of Criminology website at www.aic.gov.au
- the Australian Federal Police website at www.afp.gov.au/national/e-crime/internet_scams.html;
- Australian Communications and Media Authority website at www.acma.gov.au.

3. Discussing the three areas of information security

Great Granola Pty Ltd is a small business operating out of Perth, Western Australia. The company specialises in selling homemade granola, and its primary sales vehicle is through its website. The company is growing exponentially and expects its revenues to triple this year to $12 million. The company also expects to hire 60 additional employees to support its growing number of customers. Joan Martin, the CEO, is aware that if her competitors discover the recipe for her granola, or who her primary customers are, it could easily ruin her business. Joan has

hired you to draft a document discussing the different areas of information security, along with your recommendations for providing a secure e-business environment.

4. Information privacy

The Privacy Act gives all Australians the right to view the personal information companies hold about them on request. Research also shows that 57 per cent of home Internet users incorrectly believe that when a website has an information privacy policy it will not share personal information with other websites or companies. In fact, research found that after showing the users how companies track, extract and share website information to make money, 85 per cent found the methods unacceptable, even for a highly valued site. Write a short paper arguing for or against an organisation's right to use and distribute personal information gathered from its website.

5. Spying on email

Technology advances now allow individuals to monitor computers that they do not even have physical access to. New types of software can capture an individual's incoming and outgoing email and then immediately forward that email to another person. For example, if you are at work and your child is home from school and she receives an email from John at 3.00 pm, at 3.01 pm you will receive a copy of that email sent to your email address. A few minutes later, if she replies to John's email, within seconds you will again receive a copy of what she sent to John. Describe two scenarios (other than the above) for the use of this type of software: (1) where the use would be ethical, (2) where the use would be unethical.

6. Stealing software

The software industry fights against pirated software on a daily basis. The major centres of software piracy are in places like Russia and China, where salaries and disposable income are comparatively low. People in developing and economically depressed countries will fall behind the industrialised world technologically if they cannot afford access to new generations of software. Considering this, is it reasonable to blame someone for using pirated software when it could potentially cost him or her two months' salary to purchase a legal copy? Create an argument for or against the following statement: 'Individuals who are economically less fortunate should be allowed access to software free of charge in order to ensure that they are provided with an equal technological advantage.'

7. Acting ethically

Assume you are an IT manager and one of your projects is failing. You were against the project from the start; however, the project had powerful sponsorship from all of the top executives. You know that you are doomed and that the project is doomed. The reasons for the failure are numerous, including: the initial budget was drastically understated; the technology is evolving

and not stable; the architecture was never scaled for growth; and your resources do not have the necessary development skills for the new technology. One of your team leades has come to you with a plan to sabotage the project that would put the project out of its misery without assigning any blame to the individuals working on it. Create a document detailing how you would handle this situation.

Apply Your Knowledge

1. Grading security

Making The Grade is a non-profit organisation that helps students learn how to achieve better marks in school. The organisation has 40 offices in five states and more than 2000 employees. The company wants to build a website to offer its services online. Making The Grade's online services will provide parents with seven key pieces of advice for communicating with their children to help them achieve academic success. The website will offer information on how to maintain open lines of communication, set goals, organise teachers, regularly track progress, identify trouble spots, get to know their child's teacher and celebrate their children's successes.

Project Focus

You and your team work for the director of information security. Your team's assignment is to develop a document discussing the importance of creating information security policies and an information security plan. Be sure to include the following:

a the importance of educating employees on information security;

b a few samples of employee information security policies specifically for Making The Grade;

c other major areas the information security plan should address;

d signs the company should look for to determine if the website is being hackedl;

e the major types of attacks the company should expect to experience.

2. Eyes everywhere

The movie *Minority Report* chronicled a futuristic world where people are uniquely identifiable by their eyes. A scan of each person's eyes gives or denies them access to rooms, computers and anything else with restrictions. The movie portrayed a black market in new eyeballs to help people hide from the authorities. (Why did they not just change the database entry instead? That would have been much easier, but a lot less dramatic.)

The idea of using a biological signature is entirely plausible since biometrics is currently being widely used. In fact, it is expected to gain wider acceptance in the near future because

forging documents has become much easier with advances in computer graphics programs and colour printers. The next time you get a new passport, it may incorporate a chip that has your biometric information encoded on it.

Project Focus

In a group, discuss the following:

a How do you feel about having your fingerprints, facial features and perhaps more of your biometric features encoded in documents like your passport? Explain your answer.

b Would you feel the same way about having biometric information on your driver's license as on your passport? Why or why not?

c Is it reasonable to have different biometric identification requirements for visitors from different nations? Explain your answer. What would you recommend as criteria for deciding which countries fall into what categories?

d The checkpoints that US citizens pass through upon returning to their country vary greatly in the depth of the checks and the time spent. The simplest involves simply walking past the border guards who may or may not ask them their citizenship. The other end of the spectrum requires putting up with long waits in airports, lining up with hundreds of other passengers while each person is questioned and must produce a passport to be scanned. Do you think that the disadvantages of the reduction in privacy, caused by biometric information, outweigh the advantages of better security and faster border processing? Explain your answer.

3. Setting boundaries

Even the most ethical people sometimes face difficult choices. Acting ethically means behaving in a principled fashion and treating other people with respect and dignity. It is simple to say, but not so simple to do since some situations are complex or ambiguous. The important role of ethics in our lives has long been recognised. As far back as 44 BC, Cicero said that ethics are indispensable to anyone who wants to have a good career. Having said that, Cicero, along with some of the greatest minds over the centuries, struggled with what the rules of ethics should be.

Our ethics are rooted in our history, culture and religion, and our sense of ethics may shift over time. The electronic age brings with it a new dimension in the ethics debate—the amount of personal information that we can collect and store, and the speed with which we can access and process that information.[43]

Project Focus

In a group, discuss how you would react to the following situations:

a A senior marketing manager informs you that one of her subordinates is looking for another job and she wants you to give her access to look through that employee's email.

b A sales manager informs you that he has made a deal to provide customer information to a strategic partner, and he wants you to burn all of the customer information onto a DVD.

c You are asked to monitor a subordinate's email to discover if he is sexually harassing another employee.

d You are asked to install a video surveillance system in your office to see whether employees are taking office supplies home with them.

e You are looking on the shared network drive and discover that your boss's entire hard drive has been copied to the network for everyone to view. What do you do?

f You have been accidentally copied on an email from the CEO, which details who will be the targets of the next round of redundancies. What would you do?

4. Contemplating sharing

Bram Cohen is the creator of BitTorrent one of the most successful peer-to-peer (P2P) programs ever developed. BitTorrent allows users to quickly upload and download enormous amounts of data, including files that are hundreds or thousands of times bigger than a single MP3. BitTorrent's program is faster and more efficient than traditional P2P networking.

Cohen showed his code to the world at a hacker conference, as a free, open-source project aimed at computer users who need a cheap way to swap software online. But the real audience turns out to be TV and movie fanatics. It takes hours to download a ripped episode of *Heroes* or the movie *Black Knight* from KaZaA, but BitTorrent can do it in minutes. As a result, more than 20 million people have downloaded the BitTorrent application. If any one of them misses a favourite TV show, no worries. surely someone has posted it as a 'torrent'. As for movies, if you can find it at Blockbuster, you can probably find it online somewhere—and use BitTorrent to download it. 'Give and ye shall receive' became Cohen's motto, which he printed on T-shirts and sold to supporters.[44]

Project Focus

There is much debate surrounding the ethics of peer-to-peer networking. Do you believe BitTorrent is ethical or unethical? Justify your answer.

Endnotes

1 David Thompson, AXS-One Pty Ltd; www.axsone.com.
2 Pursuant to Title 17, United States Code, Section 512(c)(3); www.kazaa.com/us/eula.htm.
3 Michael Schrage, 'Build the Business Case', *CIO* magazine, www.cio.com, accessed 17 November 2003.
4 ASIO Report to Parliament 2007–2008, p. 32, www.asio.gov.au/Publications/content/CurrentAnnualReport/Content/Cover.aspx, accessed 6 May 2009.
5 The Office of the Federal Privacy Commissioner, *Community Attitudes Towards Privacy 2004*, 18 June 2004.
6 Scott Berianato, 'Take the Pledge', *CIO* magazine, www.cio.com, accessed 17 November 2003.
7 *U v Betting Agency* [2008] PrivCmrA 21.
8 Scott Berianato, 'Take the Pledge', *CIO* magazine.
9 www.smh.com.au/news/biztech/dogged-aussie-detective-work-reveals-10m-ripoff/2008/09/30/1222651059903.html, accessed 6 May 2009.
10 AMA Research, 'Workplace Monitoring and Surveillance', www.amanet.org, accessed 1 March 2004.
11 Office of the Privacy Commissioner, *Guidelines on Workplace E-mail, Web Browsing and Privacy, March, 2000*, available at www.privacy.gov.au/internet/email/index.html.
12 AMA Research, 'Workplace Monitoring and Surveillance', www.amanet.org.
13 K. Dearne, 'SunRice says you can can spam, curb web use', *The Australian*, 28 August 2007.
14 Business First, 'Counting the Cost of Spam', *The Australian*, 1 March 2005.
15 Andy McCue, 'Bank Boss Quits after Porn Found on PC', www.businessweek.com, accessed June 2004.
16 Office of the Federal Privacy Commissioner, *Community Attitudes Towards Privacy 2004*.
17 www.vault.com, accessed January 2006.
18 http://news.digitaltrends.com/news-article/19631/personal-internet-use-at-work-increases-productivity, accessed May 2009.
19 www.news.com.au/adelaidenow/story/0,22606,25119220-2682,00.html, accessed May 2009.
20 Australian Bureau of Statistics, *Working Arrangements*, November 2003.
21 AMA Research, 'Workplace monitoring and surveillance', www.amanet.org.
22 The booklet is available from www.privacy.org.nz.
23 www.marketresearch.com/product/print/default.asp?g=1&productid=1939741, accessed 6 May 2009.
24 www.gartner.com/it/page.jsp?id=751215, accessed 6 May 2009. This research, carried out in March 2008, surveyed 156 IT security professionals (50 in Australia, 54 in China and 52 in India).
25 '2005 CSI/FBI computer crime and security survey', www.gocsi.com, accessed 20 February 2006.
26 www.ey.com, accessed 25 November 2003.
27 Courtesy of Barry Mahoney, Manager IT Services, USC, March 2009.
28 www.zdnet.com.au/news/hardware/soa/Staff-sacked-after-widespread-privacy-breaches-at-Centrelink/0,130061702,339282381,00.htm?feed=pt_security, accessed 6 May 2009.
28 Darren Pauli, 'Uni fortifies Western Front with IDS', *CIO* magazine (Australia), 22 February 2008.
30 'Losses from Identity Theft to Total $221 Billion Worldwide', www.cio.com, accessed 23 May 2003.
31 P. Yacano and K. Lynch, 'Once is enough: single sign on', Australasian Conference on Information Systems, Toowoomba, Queensland, 5–7 December 2007.
32 Australian Bureau of Statistics, *Personal Fraud*, 27 June 2007.

33 Department of Foreign Affairs and Trade, 'ePassport', accessed 12 December 2008.
34 'Sony Fights Intrusion with "Crystal Ball"', *CIO* magazine, www.cio.com, accessed 9 August 2003.
35 Mark Leon, 'Keys to the Kingdom', www.computerworld .com, accessed 8 August 2003.
36 'Spam Losses to Grow to $198 Billion', *CIO* magazine, www.cio.com, accessed 9 August 2003.
37 'Teen Arrested in Internet "Blaster" Attack', www.cnn.com, accessed 29 August 2003.
38 M. Kelly, 'Software pirate puts days of plundering behind him: illegal files to jail files', *The Newcastle Herald*, 3 May 2008.
39 Department of Broadband Communications and the Digital Economy, 'Outcome of review of the legislative framework on spyware', www.dbcde.gov.au/communications_for_consumers/security/spyware/outcome_of_review, accessed 6 May 2009.
40 www.norcrossgroup.com/casestudies.html, accessed October 2004.
41 'Sarbanes-Oxley Act', www.workingvalues.com, accessed 10 March 2009.
42 Alice Dragoon, 'Eight (not so) simple steps to the HIPAA finish line', *CIO* magazine, www.cio.com, accessed 7 July 2003.
43 'What Is BPR?', http://searchcio.techtarget.com/sDefinition/0,,sid182_gci536451,00.html, accessed 6 May 2009; BPR Online, www.prosci.com/mod1.htm, accessed 6 May 2009; Business Process Reengineering Six Sigma, www.isixsigma.com/me/bpr/, accessed 10 October 2005.
44 Ibid.