Digital Business Security Development: Management Technologies

Don Kerr, University of the Sunshine Coast, Australia

John G. Gammack, Griffith University, Australia

Kay Bryant, Griffith University, Australia
Chapter 1
Overview of Digital Business Security Issues

Don Kerr
University of the Sunshine Coast, Australia

John Gammack
Griffith University, Australia

Richard Boddington
Murdoch University, Australia

ABSTRACT
This chapter provides an overview of digital business security. It is informed by a contemporary analysis of perceived threats through the eyes of information technology managers both from a representative public institution (a University) and from a private company (a retail sales company). A brief overview of malicious software leads into more general consideration of the risks and threats of security breaches, which are analysed from both a company and a customer perspective. Common to both sectors is the requirement to secure corporate records and other digital information and management and policy guidance is provided here. Cybercrime remains rife, but is both under-reported and under-prosecuted. As managers may become involved in legal issues associated with information technology security breaches, this chapter also overviews the special nature of digital evidence.

INTRODUCTION
For the majority of consumers, the Internet holds the promise of an environment that provides access to people and businesses on a global scale. For a few however,
the Internet provides an easy means of concealing illegal and malicious activities. Gold (2008) and BERR (2008) suggest this trend is increasing, as hacking and the development of botnets\(^1\) becomes more of an organized crime than an amateur hobby\(^2\). The security of digital business is therefore under constant threat, for public and private sector alike.

Digital business security is a very broad topic and a complete overview of the issues would be impossible in one chapter\(^3\); however, we will attempt to cover the areas perceived to be of most concern, according to interviews\(^4\) conducted with Information Technology (IT) managers from government and non-government sources. These contemporary interviews are reported in this chapter to illustrate the points at issue. While we acknowledge our sample is small, the managers selected were purposively chosen to represent real decision makers concerned with these issues and who may be therefore expected to have concerns similar to many other practicing managers responsible for IT security.

The whole issue of digital business security involves an understanding of the need to account for the use of data both internally, as well as externally. External threats relate to internet security, which can be defined as the protection of the internet account and files from both internal and external threats. At the basic level, this involves passwords, files backups, and setting up file access permissions. In fact, the respondents in the interviews, reported later in this chapter, consider the internal threats, such as the indiscriminate use of USB flash drives, as more of a threat than external factors.

The risks involved in conducting business on the Internet are different from those associated with the traditional face-to-face commerce environment. This chapter will provide an overview of the digital business environment and outline the specific business concerns associated with security for Internet enabled, e-commerce applications, and catering for the demands and rights of existing staff in the internal environment.

Digital security management covers many aspects and these are discussed throughout this chapter. Specific areas of interest include the following:

- Analysis of the risks and threats
- Development of security policies
- Management of the risks and threats
- Planning for possible contingencies
- Business continuity planning in case of a disaster
- Monitoring the effectiveness of existing security measures
- Collecting evidence to bring to justice those responsible for the misuse or misappropriation of an organization’s information resources.
Before looking in more detail at these aspects we begin by briefly reviewing some typical classes of risks and threats, and associated trends.

**Analysis of the Risks and Threats**

To commit a security breach cyber-criminals need two capabilities: access to the computer system and knowing how to manipulate it once access is gained. Whether personally initiated or otherwise, malicious software (malware) provides one of the most obvious security threats to any organization: a range of types commonly used includes:

- **Virus**: a computer program capable of attaching to disks or other files and replicating itself repeatedly, typically without the user’s knowledge or permission
- **Worm**: an independent program that replicates its own program files until it interrupts the operation of networks and computer systems
- **Trojan horse**: a program that appears to be useful but actually masks a destructive program
- **Logic bomb**: an application or system virus designed to “explode” or execute at a specified time and date
- **Keyloggers**: programs that record keystrokes, enabling capture of passwords and other sensitive data

These can destroy or compromise data or processes, and since they occur in many forms there is a constant battle between virus writers and virus protection software companies. Nikishin’s (2004) review outlined the history of malicious software attacks prior to 2004 and offered particularly disturbing predictions into the future. In his paper, Nikishin forecast a growth in virus behaviors and in proportion to the growth in the number and magnitude of services provided. In addition, the modes of entry into the system will be many and varied, for example through “email, copying themselves into network resources, attacking server software like Nimda, or a virus which infects files of different operating systems, for example Pelf, which infects the executable files for Windows and Linux” (Nikishin, p. 17). According to Nikishin, antivirus companies have the following problems:

- Unpredictable behavior with respect to methods of penetration of existing strains, as well as new strains of viruses;
- The possibility of new *flash* viruses that have the capability of infecting the World Wide Web in minutes, and this would mean that companies would not have the time to implement infection protection strategies quickly enough.
Nonetheless, protection provided through the services of professional organizations, or open source and free antivirus products are *de rigeur* for most corporations. Companies may also suffer *denial of service* attacks, where vast numbers of requests hit their website simultaneously and servers are unable to cope with the demand. Such attacks typically result in lost business and/or reputation, and even the biggest online companies are not immune. A threat that has become more prevalent since Nikishin’s 2004 paper is botnets: a hidden robot network that runs using infected computers often without the user’s knowledge. These are often likened to zombies, who rise when their master calls, and can form a vast army to instigate a denial of service attack, or a spam email.

These attacks are beyond human scale, enabled and perpetuated by technological processes, but many other forms of security breach are perpetrated at the human level. For example dumpster diving refers to simply retrieving printouts or other discarded material such as CDs or hard drives that have not been wiped first. Criminal hacking (cracking) is where the intellectual challenge presented by breaking system security (hacking) is used for criminal purposes. Although hacking can be a high level skill, and indeed one prized by banks and governments, in some case only a little knowledge is required, and malicious scripts, (freely available on the internet) can be used by almost anyone, often young teenagers known as script kiddies or script bunnies. Finally, *social engineering* is where a criminal gains an employee’s personal trust over time as part of a campaign to eventually abuse it, for example by asking for a system password, or being trusted to be left alone in the room with an unlocked computer.

In addition to these are scams and fraudulent activity, including spoof websites or emails, where the sender or website is forged and not what it appears to be in reality. Phishing and pharming are where official looking emails request personal details such as passwords or bank account numbers, or redirect users to fake websites. Personal details can then be used in identity theft crimes, where a person’s credit history, birthdate or other personal details are used fraudulently. This is not just a risk for individuals, but for companies too. Corporate identity theft can also involve credit card abuse, changing directors’ name or business addresses and the like.

Gold (2008) has provided an analysis of security issues and offered predictions of imminent issues to be considered. According to Gold, 2008 was a landmark year due to the rapid escalation of web 2.0 technologies, including social networking sites, which has also led to a spate of crimeware that use the technology to provide mechanisms for criminals to take control of computers and computer systems. Gold described the Botnet attack that, according to Kaspersky’s lab, was responsible for 5% of Internet traffic over the Valentine’s day period.
To provide predictions for the near future Gold (2008) consulted with acknowledged experts in the field from a variety of companies. The following aspects of security were noted:

- Botnets will become more decentralized, making them harder to detect and destroy the source;
- Malicious emails will increasingly use attachments or Web links in an effort to trick end users;
- Software is getting better with detection of unknown malware threats becoming increasingly effective.
- Companies will be doing “a lot more with a lot less” and this includes not “undertaking unnecessary upgrades such as Vista” (cited in Gold, p. 26);
- There will be an increasing demand for network access controls and data leakage prevention;
- There will be a surge in “cybercrime reports, mainly due to the downturn in the economy” (cited in Gold, p. 26).

The escalation predicted by Gold is corroborated by reported statistics. A UK survey conducted by Price Waterhouse Coopers for the Department for Business Enterprise and Regulatory Reform (BERR, 2008) showed that 45% of small businesses (with less than 50 employees), 72% of large businesses (with greater than 250 employees), and 96% of very large businesses (with greater than 500 employees), reported security breaches for their business in 2008. As reported by survey respondents the prevalence of four types of incidents where confidential information was exposed to risk, was as follows:

- Detection of unauthorized outsiders within the network (13%)
- Fake (phishing) emails sent asking customers for data (9%)
- Impersonated customers (identity theft) (9%)
- Suffered a confidentiality breach (6%).

The report (BERR 2008) indicated that in many cases companies were not doing enough to protect themselves from these breaches. The breaches that have a major influence on the chances of the above mentioned incidences occurring, and the associated percentage of companies that do not do enough to protect themselves and their customers was as follows:

- Websites that accept payment details but do not encrypt them (10%)
- Companies that spend less than 1% of their IT budget on information security (21%)
Overview of Digital Business Security Issues

- Companies that have no controls over staff use of instant messaging (35%)
- Companies that have not tested their disaster recovery plans in the last year (48%)
- Companies that do not carry out any formal security risk assessment (52%)
- Companies that do nothing to prevent confidential data leaving USB sticks, etc. (67%)
- Companies that had computers stolen did not encrypt hard disks (78%)
- Companies that are not aware of the contents of BS 7799/ISO 27001 (79%)
- Companies that do not scan outgoing emails for confidential data (84%).

Clearly security breaches are prevalent, and companies are doing too little to mitigate risk: risks that affect not only themselves, but also their customers.

Risks to Customers

The internet has significantly changed the way consumers engage in trade with businesses, government and enterprises worldwide. With online interaction being promoted by government, businesses and not-for-profit organizations, it can be argued that a duty of care exists to ensure clients of such services are not in danger of being victims of online fraud through the use of online activities. Fraud, especially online fraud, is an emotive issue that attracts significant public attention. Customers are increasingly being targeted by perpetrators of online fraud (Bajari & Hortaçsu, 2004). While an increase in awareness of fraud is occurring (ASIC 2007; Identify Security, 2008; Internet Scams 2008; Scams 2008), much is yet to be investigated. For example, at the time of writing (2009), ten prevalent online scams include (in order of received complaints) fake cheque scams, general merchandise sales (goods purchased but not delivered), auctions, Nigerian money offers, lotteries/lottery clubs, advance fees for loans, prize/sweepstakes claims, phishing, friendship and sweetheart swindles, and internet access services (*Internet Fraud Watch*, 2007). With the numerous ways fraud can occur nowadays, there are many opportunities for abuse.

The United States of America has investigated numerous online frauds received by the Federal Trade Commission (US Federal Trade Commission, 2007). These investigations involved cross-border states within America, as well as international investigations involving many countries. To demonstrate the problems that occur when the investigations go international, and by way of example, we will discuss the case of Australia. Currently, any online fraud prosecutions involving Australian companies, identified by the US Federal Trade Commission, are not enforced due to the costs associated with enforcing an American judgment in Australia. Furthermore, the information gained during the investigation is not able to be turned over to investigating Australian Federal police as there is no authorization currently in place for this to occur (US Federal Trade Commission, 2007).
Overview of Digital Business Security Issues

These problems are not just a concern to customers and consumers of internet services but also to the very companies that provide the services, as the system is built very much on trust. Unlike other business transactions, internet transactions require the customer to pay for the product upfront and the trust required for this type of transaction is much higher than traditional transactions. If this trust is betrayed, the company can find itself in a very difficult situation very quickly.

Risks to the Business

Whitman and Mattord (2009) identify twelve threats to information security in business and these are shown in Figure 1.

These categories of threat represent a combination of technical and human factors and are a good indication of the complexity of the issue with each category having to be considered and understood to varying degrees by managers.

Security breaches can also have a dramatic effect on a company’s reputation and even on its share price. The magnitude of the impact is usually a direct reflection on how heavily the company relies on the internet for their business activities. For example, a distributed denial of service attack on Amazon.com would have more severe impacts for the company and its customers, than a similar attack on a website for an oil company. Security breaches can impact on companies through direct effects on share prices, or through a loss of reputation, with respect to customer access or even the security of personal information, like addresses or credit card particulars.

It is difficult to quantify the exact cost of security breaches as companies tend to under report these events and the determining of losses associated with factors other than the breach is often difficult to estimate. However some research has been conducted on the impact of security breaches on companies’ share price and reputation and techniques such as event study methodology, have been used to some effect (Garg, Curtis, & Halper, 2003).

Garg et al. (2003) studied the impact of security breaches on the share prices of publically listed companies. In their study of 22 security breach events, the company share price fell by an average of 5.6 percent over a three day period after the security breach event was reported. It is apparent that company losses and net worth reductions of this magnitude could pay for a lot of security initiatives, yet many companies are not spending the required money. For example, the Price Waterhouse Coopers report quoted earlier indicated that 21 percent of companies spend less than 1% of their IT budget on security (BERR 2008).

Garg et al. (2003) also provided case examples of security breaches that affected company reputations and foremost was the denial of service (DoS) attack, especially with companies that are heavily dependent on the Internet, such as eBay and Yahoo. Garg et al.(2003) suggested that the year 2000 was a watershed for internet
security, as the DoS attack demonstrated to companies that the Internet had serious vulnerabilities, and that the true cost of doing business on the Internet included “the cost of downtime, recovery costs (systems and theft of proprietary information) and damage to brand reputation/customer perception”.

The purpose of this book is to provide an understanding of these threats from a managerial perspective. To provide an indication of concerns contemporary information technology managers have with respect to security, we interviewed selected individuals in both the public and the private sector. The results of these interviews are described in the following section.

### Information Technology Managers’ Perspective on Security

In order to gain some insights into the magnitude and complexity of security realities, interviews were conducted with executive staff in an Information Technology Service (ITS) division of an Australian University, and with an Information Technol-
ogy manager from an Australian nationwide retail company. Their concerns were considered representative of contemporary public and private sector organizations.

A PUBLIC SECTOR PERSPECTIVE ON SECURITY MANAGEMENT

Three IT managers at an Australian University were interviewed jointly. They were the Director of Information Technology Services, the Manager of Information Technology Services (ITS), and the Team Leader of the ICT Infrastructure Team (who is largely responsible for ICT Security within IT Services.)

The views of the director, with respect to security for ITS (Information Technology Services), were introduced as follows:

The most fundamental aspect of security is compliance with legislation and audits of the institution in relation to this...ITS is held responsible for the custodianship of financial data and ...ICT security at the most fundamental level in terms of being audited as an organization.

The Director further asserted that “The place that the auditors will go is ITS, to determine how secure the financial data is...This is extended to all assets associated with the university’s core business”. The Director considered security very important and suggested that there was a fundamental interest in how secure an organization’s financial systems are. The Director also suggested that security was very important because the University is audited every year. The Director summarized this line of thought by saying that “Security is about the whole governance regime. You need System Owners to determine who rightfully has access to what.”

The University is a relatively young institution and the maturity of the organization was an important factor when assessing security needs. The contemporary security standards suggest that the organization needs to go to a certain level but this has to be tempered against the available resources of the organization. As the Director stated:

[We look at] what are the practices across the organization, what is the maturity of the organization in so far as our ability to adopt that standard and we come back from a particular standard and not adopt it in its fullest extent because we quite simply haven’t got the resources.
The institution takes a risk management approach because “we do not have the resources of say a big bank ... We have a balanced approach to allow people to do their job, as well as providing systems security” (Director of ITS).

The Team Leader emphasized the difference between risk avoidance and risk management. He provided an example from the financial sector saying that “in the past financial institutions had a risk avoidance approach [of] locking everything down - buried inside the walls of the institution. Well we are not in an environment like that here”. He further went on to say that the University may require sensitive information from a source on the other side of the world and the risk management approach (along with improvements in software) allows the University to undertake this type of activity. He further distinguished between data and information, maintaining that data security is often mentioned but the real need is for information security. Data is not valuable, until it becomes information. The manager went on further to say:

Many of the tools available are based on structured information such as database; however, we not only consider structured digital data but increasingly we must consider unstructured information, such as multimedia content, so it’s gone beyond the traditional data processing model. For example, what do we do about email or remote access to email or mobile devices and with people who are increasingly mobile in the global context? (Director and Team Leader)

The Team Leader also suggested that a major challenge for the University was maintaining information security in a mobile world, and this is not so much the technology but the behavior pattern of staff and students. He went on to ask the question “How do we know if the person accessing the information is the person they claim to be?” This problem of identification is further complicated through human behavior with the Team Leader stating that “Human behavior is also a problem, for example walking away from a machine while in an Internet café.” This theme was expanded upon by all three respondents with statements, such as:

People have to understand the risks of not having adequate security. There is a great deal of frustration amongst academics in having to unlock a screensaver all the time, and ITS are very aware of this frustration, however, the risks of not doing this must be acknowledged.

The analogy was then given of a finance department and the security provided in terms of locked doors, simply to secure what may only be a small amount of petty cash, but data is accessible from computers everywhere. Not only is the remote access a problem, the fact that it is dynamic, adds further complications to the problem. In
addition, people change locations or positions in the organization and these moves require changes in the information systems infrastructure to reflect that. The data manager asked the question “How does ITS know when people have moved on to another role, for example?”

To the question of non-technical security issues, such as email scams, the interviewees spoke about their approach to handling the problem as being one of sensitivity to the requirements of staff. They stated that they do not want to pry or look like they are interfering but they do need to make people aware of the potential scams. The concern they had was that there was a perception amongst some members of the University that ITS should be protecting people from these scams. The reality is that the University cannot protect people from their own decisions relating to these types of scams.

Spam filtering is also a challenge in the University environment and they do use the services of a number of organizations who are acknowledged experts in this area. The University collects information from several sources for third party automated systems and they use AusCERT (Australian Computer Emergency Response Team) from the University of Queensland in Australia, which provides a subscription-based membership.

The University has automatic systems running 24 hours a day, seven days a week. Spam monitoring in general takes a considerable amount of time and effort for a small University, and one full time employee is assigned to this task for a significant amount of time every day. Malware, spam, and phishing (scam) emails are a constantly evolving threat. To provide effective protection, similarly agile and evolving systems are extensively employed. The security manager revealed that “up to 97 percent of emails are dropped every day and the system is being probed every second”.

The Team Leader indicated that there were unique aspects to the University environment and in this case, in particular, by suggesting that “under the University environment we have to be more flexible than many other corporate of government environments”. This uniqueness was further emphasized by the security manager who suggested that appliances designed to reduce security impacts are available but they cannot work in “set and forget mode” unless the organization has “incredibly simple business rules”. The “set and forget” mode will provide around 80 percent accuracy but this organization “expects 99 percent stopping the stuff [inappropriate email and phishing]”.

The Director provided an overview of how the security challenges have changed since 2004, with the major security concerns being relatively simple worms, but these are being replaced by sophisticated Botnets (explained by the Director as “methods of gathering PCs to be part of a herd to do some grand organized crime effort”. The Director further explained that these Botnets are examples of how the
ITS has a social responsibility, as well as an organizational responsibility, to deal with these things in a reasonable way. She suggested that the University was doing that quite well but there is always more that can be done. For example, Microsoft is doing a lot of work on targeting Botnets and looking to attack before the world of Microsoft itself gets attacked. The indication was that there was a lot more proactive work being done by the vendors now.

Relating to concerns about the relative new area of cloud computing\(^{10}\), the Director suggested that one of the threats faced by the University was in the multi-user virtual environment world. She went on to suggest that cloud computing is the next threat because, although systems can be locked down within your own environment, the problem is the accountability the University has over a service that is not housed on the campus. IT staff have no capability to control what is done in ‘the cloud’ by academic staff and students. The IT Director was referring to online multi-user virtual worlds, such as Second Life, and the use of these services for teaching and learning purposes. The IT director suggested that “these worlds exist and your IT group have absolutely no control over them what so ever … so how does the organization control its intellectual property? … That is content that is being distributed through that cloud.” Other questions related to who has access to these sites and to the information contained in them and how do you control that? The Director was concerned that nothing is done in “the cloud” until there is a security problem, and then it is fixed, but the industry is always in catch-up mode.

The Team Leader was most concerned about the unknown and he emphasized this through the following statement:

*We don’t know if a vulnerability exists... it is really those things that are going on ... that you don’t know about ... [for example] if a Botnet gets below the kernel, there is nothing you can do about it because it is below that layer, although the University does run root kit detectors on key exposed systems and have software tripwires installed [the layer of the tools used to detect it in the first place – the tool is sitting above that kernel layer].*

**A Private Sector Perspective on Security Management**

The information systems manager of a large national retail chain was interviewed and asked about his concerns with security. His response to the question, “What is the major concern in your organization with regards to information security?” was:

*Generally because we have very corporatized systems for [control of] viruses, [such as] antivirus spyware, malware [and] things like that, our biggest threat
is actually internally ... when people put a USB key in [to the computer], that is where we get most of our viruses from. We have files in place [to control external threats], where all but the best hackers would not be able to hack in externally so our threat is internal.

The manager further expanded saying that they have corporate tools that manage viruses, pushes out software to computers, and tells the IT department if any software has been changed without admin rights. The company uses a proprietary tool (Cisco works) and any infections are reported back to the central system. In addition, a content filtering system has been built into the proprietary tool. When asked about the use of services like Facebook and MySpace by staff, the response was, “No we have Facebook open, we are liberal with team members here that they are actually allowed to access sites such as banking or Facebook etc, as long as it is on your own time”. Like the previous interviews, the key concern was unintentional internal threats and this was exemplified in the following statement:

Some people pirate music or movies etc and bring them into work to share with everyone. Chances they have some spyware, malware\textsuperscript{11} Trojans\textsuperscript{12}, whatever happens to be on it and people have been known to put it on their computer, log into the LAN and infect every computer in the organization, and it might be two days before we can get a patch fit in to fix that.

As mentioned earlier, the company has software arrangements with companies that guarantee that they will manage threats for the company, and if something goes wrong, the provider of the software and service is liable. In addition, the company has an extensive disaster recovery plan, and if something really bad happens, they can “always go back to the tape” from their mirrored site. The IT manager works on the principle that:

Generally you will infect one not both sets of servers so we have always got multiple ways of backing up. We also have the independence of the stores themselves, we have 350 stores around the country... if head office got attacked by something bad they [the stores] can keep on running, the only thing they could not do is an end of day balance. Realistically they could carry on [independently] for a week if they had to.

The company has ecommerce capabilities with a Web store, import store and export store that people can go on and buy goods online if they so wished. This is externally hosted, so the hosting company will “get hit”, and not the retail company.
This retail company’s solution to its security concerns was to have third party providers to outsource. The IT manager stated, “We have also outsourced our Electronic Data Interchange (EDI) to a company called GXS inboard and outboard logistic information is forwarded regularly in a specified format back to us.” This effectively means that all the problems associated with different systems and different trading partners become GXS’s problem. The IT manager went on to say that “big companies like WalMart will only deal with vendors if they go through GXS for EDI”.

When asked about the social engineering aspects of security, in particular phishing attacks and other scams, the manager reinforced the third party propriety software solution the company had enacted. His response was:

The company has automatic filtering systems that stops a lot of this type of email traffic... most phishing attacks are targeting government [institutions]. I haven’t to my knowledge not received an email and had to go to our security engineer and ask to retrieve it... We don’t have any missing emails and no junk mail ... in my previous employment [government institution] there were bouts of up to 50 emails about Nigerian scams ... haven’t had any [here] which is interesting really.

When asked about cloud computing as a follow up from the concerns the director of ITS from the University had, the response was, “We have gone the VPN (virtual private network) route with each employee having secure access to the network.” The response to the final question, “Do you feel you have security under control?” was:

Since I have been here [12 months], I have seen one virus that swept through; it was brought in internally. The security engineer has said they have no high level security attacks detected like someone trying to hack in ... even if the network is down our monitoring tools would send you an SMS indicating the attack is occurring ... really it comes down to - we are more at risk from an internal source such as USB, CD or pirated games.

In summary, the way this company got around its security problems was to outsource. The final comment was, “Our outward facing Web site is outsourced so they are not actually attacking us anyway.”

Many of the concerns expressed by the respondents in the University interview are common across the University sector. For example, reports in The Chronicle of Higher Education confirm the internal threat concern with a study indicating that 21 percent of respondents, in a survey of 182 college officials in the United States of America, had said that their systems had suffered an intrusion from someone within
their college (Young, 2006). In the same study, 58 percent of those surveyed reported some kind of IT incident and nine percent reported losses of data related to students.

More generally, Gold (2008) predicts an increase in cybercrime due to “The combination of higher sophistication of both the cybercriminals and their crime tools, the low detection and prosecution rate, and the financial stakes [involved]” (p. 26). Protection through ongoing awareness of technical developments is therefore essential. No matter how much is spent on security, however, many initiatives fail because workers are in the main not very conscious of security (Workman, Bommer, & Straub, 2008) who suggest that managers also need to address human behavioral aspects through training and education. The literature and anecdotal evidence (for example from the interviewees quoted in this chapter) indicates that security problems are only going to become more difficult, and thus it is very important that companies keep up to date with the latest in security issues both from a technical and a human point of view. The next section examines these and other policy and planning issues for management.

Management of the Risks and Threats

Security policies and crime prevention are matters for national agencies as well as corporations and both regulation and organization level policies are implicated. For both commercial and government organizations, policies will be generally similar, as they involve a coordinated response to managing security risks associated with IT infrastructure and access. The framework developed through the US Department of Homeland Security provides a comprehensive guide to areas of IT security that remains under continuous review to ensure its currency. This framework can be used at organization level in developing appropriate management and technical competencies and roles in line with wider security policies.

Organizations rely increasingly on computer networks and information management systems to create, store, and transfer the information that forms an essential part of their operations. Threats to the security of digital assets may come from both expected and unexpected sources. Dramatic natural disasters or cyberattacks exist alongside more preventable (and thus manageable) instances of risk associated with technical or physical vulnerabilities. Policy frameworks provide guidance on areas of vulnerability, which require specific technical responses. Management involves generally understanding the potential threats and vulnerabilities in the context of the wider policy and external environment, and ensuring that appropriate technical responses are implemented.

Enterprises require IT security professionals whose competencies span both technical and managerial aspects. The IT Security Essential Body of Knowledge
(DHS-NCSD, 2008) comprehensively identifies several functional organizational roles and competencies associated with specific areas of vulnerability that apply to any organizational sector. Management’s role generally involves overseeing technical designs and implementations, whilst keeping abreast of technical developments, assessing the changing risk landscape and ensuring compliance with wider policy. Technical developments and standard include cryptographic practices such as public key infrastructure (PKI) and biometrics. PKI allows encrypted data to be exchanged over the insecure public environment of the internet, at a level of security adequate for everyday commerce. Whilst agencies such as America’s National Security Agency (NSA) have access to more powerful encryption methods (and the wherewithal to break commercial level PKI codes) PKI provides a global standard for electronic commerce and data exchange. Biometric techniques, which use personal physical characteristics to identify computer users are now becoming commonplace. A simple webcam with face recognizing software for example can prevent unauthorized computer access, and many biometric techniques such as fingerprint readers are becoming affordable and practicable as complementary levels of security to passwords.

Compliance with wider policy may be externally mandated – for example the Sarbanes-Oxley Act affecting public companies in the USA has far reaching implications for IT security (Byrum, 2003)\(^\text{15}\). External industry bodies may also provide specific guidelines that must be taken into account, depending on the organization and a manager’s functional role. For example, one identified competency area is “digital forensics”, relevant when a security incident has occurred and requires analysis and report. National bodies such as the Association of Chief Police Officers in the UK provide updated guidelines in this area (ACPO, 2007)\(^\text{16}\), in which relevant investigators at organization level would be required to be trained and whose practice should consistently follow. Whilst police investigators need to comply to preserve evidence that will be safe in court, many other organizations may also wish to form permanent incident response teams with similar expertise for handling security incidents. In any organization, management competencies and responsibilities in digital forensics might typically include ensuring investigative resources and establishing a specialized forensic team (whether ad hoc or more permanent); ensuring appropriate access levels and overseeing any emerging improvement actions (see DHS-NCSD, 2008, p 8).

In the dynamic area of IT security, however, the specific knowledge required will develop and change, and it is beyond the scope of any framework to detail this. Whilst the Essential Body of Knowledge (EBK) framework specifies the enduring types of competencies required in digital forensic investigation and 13 other fields of IT security, the responsible manager would expect to remain aware of the best current practice and knowledge, in order to organize specific activities in line with
the framework’s broad areas. Specialized courses, consulting services, publications, websites and conferences can provide relevant guidance. In the case of the digital forensics community, (as with other IT security fields) standards, rigor and consensus on practice is actively debated, and shared at specialized fora.

It is important in organizations that security knowledge and sensitive enterprise information is managed and not lost if experts move on – so documentation of processes, policies and resources becomes a management activity, along with sharing knowledge within a trusted community. The security of IT systems and applications is a key area for enterprises, whether the software used is third party or developed in-house, and integrating effective security practices into code development and ongoing risk evaluation is signalled here. Wikis provide a powerful mechanism for knowledge sharing, but there is a risk if identified vulnerabilities are shared before patches are in place, and before a root cause analysis preventing similar occurrences is conducted (Araujo, 2006).

If appropriate, forming a dedicated team can be considered. Such teams are usually called Computer Security Incident Response Teams (CSIRTs), or sometimes Computer Emergency Response Teams (CERTs). For example the computer emergency response team for the Netherlands’ Government is called GOVCERT NL, whilst, for Australia, AusCERT is the national computer emergency response team. CERT is a registered service mark, so the more general and internationally used term CSIRT is preferred here. Detailed guidance on setting up CSIRTs was proposed by West-Brown et al (1998) and was updated in 2003. The European network and Information Security Agency (ENISA) also provides detailed guidance for management setting up CSIRTs (ENISA, 2006) and Killcrece et al (2003) further expand on the variety of models for structuring a CSIRT and selecting a design appropriate to organizational practicalities.

Planning for Possible Contingencies

Management plays a key role in strategic business planning, and through anticipating threats to the business, acting to avoid or mitigate these before they occur. In IT security especially, this includes recognizing the various potential sources of threat, and protecting data and other content through appropriate measures. Good management includes not just technical but also human resource activities: data may normally be behind an enterprise firewall but if transferred to a USB stick and mislaid off-site, it is suddenly compromised. Workforce education and physical as well as technical security measures are indicated.

Unauthorized access to networked resources remains one of the main areas of security breaches. Policies on access within an enterprise will depend on the nature of the work, and who needs to know particular information held within files. Per-
missions are authorized in line with policies from higher organizational levels, and typically set to operate at individual, group and public levels. Security may be set at a file owner’s (e.g. document creator’s) discretion, or mandated by an administrator’s policy. A file may be set for the owner to read and modify, a trusted group to read only and inaccessible to the general public. A user with higher level clearance (such as a system administrator) can override these access privileges, but issues of privacy and confidentiality can then come into play and cause other problems.

This is a multi-level security approach, and operating systems or network protocols provide standard mechanisms for setting appropriate clearance to read, alter or execute files in a given folder or system area. Whilst both public and individual permissions are conceptually clear for single sites or named workforces, management must decide who belongs to groups with particular access levels, and this becomes further complicated when third-party networks are implicated.

Equally, certain documents may be layered to give permissions for accessibility depending on security clearance policies and associated settings. This facility is important in ensuring original copies are preserved, and not modified accidentally or deliberately. Also at the document level, passwords, encryption and permission settings can be managed for additional security. Products are available that can decrypt documents, using specialized algorithms or brute force if necessary, so access even to documents in encrypted form is another consideration implying any management approach to security must be multidimensional.

Apart from managing access and data and file protections inside an organization, threats from outside, including random or targeted malware attacks, and deliberate intrusions aimed at information theft or vandalism must be addressed. The most recently available Computer Crime and Security survey from the Computer Security Institute (CSI, 2006) found that “virus attacks, unauthorized access to networks, lost/stolen laptops or mobile hardware and theft of proprietary information or intellectual property ... account for more than 74 percent of financial loss”20. Firewalls, anti-malware products and Intrusion Detection Systems (IDS) are well known classes of software designed to mitigate specific threats and are outlined below. Specialist software for analyzing networks to identify security issues has been around for some time, such as SATAN (Security Administrator’s Tool for Analyzing Networks) and SARA, (Security Auditor’s Research Assistant) based on the classic SATAN model21, and others. Software permitted to scan a network or computer system must be trustworthy and up to date, since if it can detect a vulnerability it can also pass on this information for subsequent exploitation.

Firewalls are essentially a barrier between the outside (untrusted) and the inside (trusted) environment: often between the internet and the local machine or internal network. Like a physical protective wall a threat is identified and blocked before it affects sensitive material inside the wall. As barriers work both ways, by detecting
what is going in and out across the wall it can detect sensitive material escaping outwards to an untrusted or unknown environment.

The malware threats outlined earlier in the chapter each imply specific technical and managerial responses. Specialized software, from leading vendors or otherwise available provides protection against identified viruses, worms and other malware. Professional solutions are often provided together with associated technical information and update services describing vulnerabilities and recommendations for remedial or preventative action. Virus definitions for example are updated continually and thus both a product capable of responding rapidly and a management policy to enforce updates are needed. Applying disk or usage quotas for individual users can limit the amount of resources used by replicating worms. Removing inactive accounts after a grace period removes another potential vulnerability. Monitoring for unusual activity or patterns, using human intelligence or analytic tools also helps identify potentially malicious use. For example Birdi and Jansen (2006) provide valuable insight on the management aspects of Intrusion Detection Systems and make several practical recommendations.

Establishing the risks realistically whilst managing the security budget is a typical management dilemma. Perfect access (no security restrictions) and perfect security (no access possible) are limiting cases between which an optimal position must be found. Mayfield’s paradox (Mayfield & Cvitanic, 2001) mathematically characterizes the idea that beyond a certain point spending extra money on security improvements will produce diminishing returns: similarly, increasing the access levels becomes expensive at the limits. Similarly, overspending on security relative to the actual dangers reflects poor management so effective risk assessment in the business context is also signalled.

In considering internet security for businesses, Chang, Hwang, Yen and Huang (2006) reviewed the existing literature and established four factors that need to be considered (in their case in the financial sector, but the principles are more general). These were:

1. **Factors that affect hardware security.** These include:
   - Natural disasters such as earthquakes or storms;
   - Accidents, such as dropping a notebook computer or spilling coffee;
   - Malicious acts, such as deliberate intrusion into computer systems;
   - Hardware defects (bugs or software errors), such as security vulnerabilities found in software.

2. **Factors that affect software security:**
   - Improper design of operating Systems, for example, security loopholes of improper use of software;
3. **Human factors:**
   - Human negligence, such as not keeping up to date with the latest virus protection software or failing to install security patches in operating systems or web browsers;
   - Mistakes, such as opening malicious email attachments.

4. **External factors:**
   - Unauthorized intrusions, such as Botnet or denial of service attacks.

These four factors can and should serve as a checklist for planning for any security related contingency that may arise. The planning for contingencies is often referred to as continuity planning, and this book devotes a chapter to this topic: a critical decision area for any business.

Whilst developing policies and plans for managing digital information requires a certain skill set, perhaps one of the most daunting requirements for a manager is the possibility of becoming legally involved in the disputes, breaches in regulations, or criminal activity arising from digital security problems in the workplace. Without awareness of digital evidence issues, cybercrime detection and prosecution will remain low. With this in mind, we conclude this chapter by providing a background to the special nature of digital evidence, vis-a-vis traditional evidence categories.

**Digital Evidence**

Business managers rarely have a background or expertise in forensic investigations, yet increasingly they may be called on to undertake some form of investigative work in the event of some legal dispute, breach of personnel regulations, or criminal activity arising in the workplace (Stephenson, 2000). The inherent vulnerability of their digital information holdings means that weaknesses in their security exists and are constantly at risk of exploitation from internal and external threats (Stephenson, 2000). Consequently, the rise in computer-based crime and misuse of digital information for improper purposes has resulted in a concomitant reliance on digital evidence in criminal and civil investigations (Etter, 2001a; Palmer, 2001; Thompson, 1998).

Many legal practitioners and courts are still struggling to understand forensic science, notably evidentiary issues with DNA evidence, and more recently have been faced with new challenges posed by digital evidence (Bassett, 2006; Caloyannides, 2001; Edwards, 2005; Etter, 2001b; Losavio, 2006). Similarly, organizations are confused by digital evidence and may not clearly understand its potential benefits and limitations (Jordan, 2005).
Business managers may find themselves involved increasingly in the investigation environment with the responsibility of preserving the crime scene, locating, selecting, and validating digital evidence (Guidelines for the Management of IT Evidence, 2003). Having moved the evidence through the investigation process, business managers are likely to become involved with the process of constructing legal arguments that depend on the presentation of evidence in courts or other hearings. Significant issues also confront the legal fraternity over the use of evidence in court, especially when the evidence is based on digital exhibits.

**Digital Evidence in the Legal Domain**

Computer crime, or cyber crime, takes a variety of forms including unauthorized use of computers, fraud, forgery, damage and sabotage, unauthorized interception, unauthorized copying of software programs, data misappropriation, posting illegal material, industrial espionage, social engineering, and others (Berwick & Thompson, 1998; Carter, 1995). Recalling the collapses of large corporations, such WorldCom and Enron, that involved large-scale fraud, exemplifies the misuse and concealment of digital information for financial gain. Computers may also be incidental to other crimes by speeding up the computation of information or making it more difficult to detect crimes, such as money laundering and fraudulent banking transactions. The exponential growth of computers has engendered new variations of traditional crimes, such as breaches of copyright and software piracy.

While the Internet and modern communications provide many societies with personal and commercial benefits, users increasingly misuse these facilities for cheating, lying, stealing, and even crimes of violence (Mohay, 2003). So as cyber crime increases, law enforcement agencies try to play catch up with limited success. Increasingly, digital evidence forms an important part of criminal, civil cases and disciplinary proceedings; however, it is often notoriously too difficult to locate and analyze for it to be useful in such processes. The large size, complexity, and changing form of software applications and datasets, challenges experienced investigators. These challenges are normally far greater for legal practitioners and organizations’ personnel, who may be involved in collecting and using digital evidence and who possess negligible cyber forensic skills or understanding of the special nature of the evidence. Even with expert help, these investigations can be financially costly and time-consuming exercises that organizations may not consider viable (Sommer, 1998). In the event that such expertise was used, organizations would be well served if they possessed some basic understanding of the technical and the legal complexities of digital evidence.

Digital evidence is information found on a broad range of devices, and generally considered to consist of information held in digital data form, that has some
value to the investigator seeking to reconstruct the key events of an incident, and
the probative value of the evidence, if it is intended for use in legal proceedings.
It is sometimes referred to as IT evidence, electronic evidence, or computer evi-
dence (Ashcroft, 2001; Carrier & Spafford, 2005; Chaikin, 2006; Pollitt, 2001).
According to Carrier and Spafford (2004), digital data may be defined as numerical
representations, most usually in binary form. Digital evidence may be considered
to include any digital data that may be used to establish whether a crime had been
committed, or can establish a link between a crime and the victim of the crime, or
between a crime and the perpetrator of that crime (Casey, 2000; Saferstein, 1998).
Carrier and Spafford’s often quoted definition describes digital evidence as “any
digital data that contain reliable information that supports or refutes a hypothesis
about the incident” (p. 3). The definition of what reliable information may consist
of is examined in more detail in Chapter 3 in the context of evidence validation.

Sources of digital evidence include emails, electronic documents, spreadsheets,
databases, system logs, audit logs, application logs, network management logs,
network traffic capture, and file system data (Sommer, 1998). Digital evidence is
located in files stored on hard drives; memory cards; access control devices, such
as smart cards; biometric scanners; answering machines; digital cameras; personal
digital assistants; electronic organizers, printers; removable storage devices; and
media, such as CD-ROM and DVD discs; telephones; copiers; credit card skim-
mers; digital watches; facsimile machines; and global positioning systems (ACPO,
1999; Ashcroft, 2001). As new technologies emerge and existing ones converge,
new environments, where digital evidence may be found, are created.

Carrier (2003) advocates using conventional crime scene investigation techniques
to process digital evidence; however, digital evidence used in legal processes is
often problematic as its validity and usefulness may be diminished because of its
volatility, the complexity of the digital domain, large datasets, and rapid changes
to technology (Mercuri, 2005; Sommer, 2000).

Digital evidence is sometimes considered superior to conventional paper evi-
dence, as it is easier to locate and process (Caloyannides, 2001). Digital evidence
normally contains useful metadata, such as key dates, times, and a history of the
file, and because of its persistence in recording key data, it can provide proof of
past events that an offender may prefer did not exist (Caloyannides; Janes, 2000).
Moreover, digital evidence frequently provides metadata recorded from the date of
its creation, that is more revealing than paper-based evidence providing potentially
valuable information relating to a crime (Flusche, 2001; Janes).

Digital evidence shares characteristics with other forms of evidence, such as paper
documents, but its complex technical properties can be problematic for investigators
and auditors attempting to collect digital evidence for use in legal cases (Mercuri,
2005; Sommer, 2000). Lawyers and courts are often confused by these technical
complexities and may misinterpret digital evidence, potentially resulting in unsound and unfair judgments for various parties involved in legal cases (Caloyannides, 2001; Edwards, 2005; Etter, 2001b; Losavio, 2006).

There are some inherent differences between conventional forms of evidence and digital evidence. Most notable is the ease with which digital evidence may be altered and manipulated, which may be difficult or impossible to detect (Caloyannides, 2001). Digital evidence is mutable and can be altered far more easily than physical records, and consequently, is more susceptible to unauthorized manipulation, making it difficult to validate its admissibility and evidentiary weight in legal proceedings (Akester, 2004; Mattord & Whitman, 2004; Schneier, 2000).

Despite the pervasiveness of computers in society, few legal practitioners have sufficient knowledge about the properties and functions of computers, networks, and digital information to assist them to prepare legal cases based on digital evidence (Mercuri, 2005; Sommer, 2000). The legal fraternity and organizations rely heavily on computer forensic investigators and other computer experts to provide some insight and explanation about digital evidence and its properties (Yasinsac, Erbacher, Marks, Pollitt, & Sommer, 2003).

Digital Evidence and the Public and Private Sectors

There are commonly considered to be two broad categories where digital evidence exists: the public sector investigations, within the domain of criminal law, undertaken by government law enforcement or regulatory agencies; and private sector investigations, initiated by corporations and sometimes by individuals (Enfinger, 2006). Public sector investigations focus on breaches of criminal laws, whereas private sector investigations usually relate to torts and other civil litigation, or disciplinary proceedings against employees. In practice, there is much similarity between public and private sector investigations and it is common for investigations in the public sector to become a civil case, and vice versa.

Public sector investigations seek evidence in pursuit of criminal activity, including fraud, identity theft, blackmail, extortion and most other criminal activity; whereas, private sector investigations may seek evidence of abuse of an organization’s assets, such as sending malicious emails or abuse of Internet privileges in violation of company policy, and violations of intellectual property (Enfinger, 2006).

Criminal cases and civil actions rely increasingly on digital evidence for a range of events including theft of intellectual property, blackmail, unlawful access to confidential information, modification of the integrity of information, or making the targeted information unavailable for its intended use (Carter, 1995; Mattord & Whitman, 2003).
Evidence and Digital Evidence

Evidence used in legal cases may consist of witness testimony, hearsay, documents and things, and proves facts that are in dispute through directly proving the ultimate fact without relying on other evidence to prove any intervening, penultimate steps (Anderson & Twining, 1991; Tapper, 2004). Evidence is also used to prove the plausibility of facts from which facts that are being disputed may be understood: most notably, circumstantial evidence (Tapper, 2004). Circumstantial or indirect evidence, which includes documentary and digital evidence, is used to construct inferences that indirectly prove the ultimate fact in a legal case (Anderson & Twining, 1991; Stephenson, 2000).

Evidence of a legal nature proves facts that are in dispute and the weight that may be attached to the facts is examined and tested by various forms of legal argument (Anderson & Twining, 1991; Tapper, 2004). Developing legal argument can be a complex process taking in a broad range of evidentiary issues. Technically complex digital evidence used in constructing compelling legal arguments makes the process significantly more challenging for the stakeholders (Caloyannides, 2001; Mohay, 2003; Tapper; Wall, 2004; Yasinsac et al., 2003).

To Sommer (1998), legal proof relates to the admissibility and weight of evidence and is only distantly related to scientific proof that relies on generally recognized processes of scientific investigation. Evidence should be sufficiently relevant to the issues it is intended to prove to the court; if not relevant, or insufficient, it should be inadmissible (Tapper, 2004). Relevancy in a legal context is not universally defined, but Justice Stephen’s nineteenth-century definition, as cited in the Oxford Journal of Legal Studies (Ho, 1999), still holds currency in some jurisdictions and may be helpful when contextualizing digital evidence with other evidence:

Any two facts to which it is applied are so related to each other that according to the common course of events one either taken by itself or in connection with other facts proves or renders probable the past, present, or future existence or non-existence of the other. (Stephen, cited in Ho, 1999, p. 404)

Although no formal universal definitions exist, evidence may be categorized into a range of types depending on the jurisdiction and its stature in the local hierarchy, including direct evidence, indirect evidence, hearsay evidence, and evidence of opinion. The following sections describe the effects that different categories of evidence may have on legal cases, which potentially have implications for business managers.
Direct Evidence and Circumstantial Evidence

Direct evidence, sometimes called witness or testimonial evidence, depends on the credibility of a human witness, and most evidence used in legal cases has traditionally been based on testimony from a range of witnesses, whose credibility may be upheld or refuted if it proves to be fallible (Walton, 2000). Direct evidence that directly proves the ultimate fact in a legal case, such as what the eye-witness saw or heard which is accepted by the court, has a high inferential value. Provided witness testimony is not in itself hearsay, it may be admissible in legal proceedings (Anderson & Twining, 1991; Silverstone & Sheetz, 2007).

By its nature, digital evidence is not direct evidence but circumstantial evidence, and may be considered hearsay evidence, that may only be admitted in legal proceedings under established procedures (Anderson & Twining, 1991). Based on the inferences of some inanimate object that indirectly proves the ultimate fact, circumstantial evidence is often used to build up inferences to prove some fact in issue, such as a knife found at a murder scene, whose blade matches the stab wound and on whose handle the fingerprints are those of the assailant. By linking the body to the knife, and in turn the knife to the assailant, links are formed in the chain of evidence (Anderson & Twining; Silverstone & Sheetz, 2007; Tapper, 2004; Walton, 2000).

Circumstantial evidence is probabilistic in nature and often challenging when attempting to determine the truth of an issue because the examination processes used are poorly defined (Fiske, 1991; Nisbett & Ross, 1980; Nisbett, Krantz, Jepson & Kunda, 1983). Digital evidence is analogous to the more conventional forms of circumstantial evidence, most notably documentary evidence, and both forms are subject to the same degree of legal scrutiny afforded to direct evidence tendered by a human witness who has, for example, observed directly the events of a document forgery (Caloyannides, 2001; Tapper, 2004). Digital evidence is mute and cross-examination of the evidence is not possible, unlike a human witness who is able to offer explanation and comment to the court.

The common law and legislation in various jurisdictions accept that the contents of a document need not be treated as a separate item of judicial evidence, although in many jurisdictions, legal convention makes it expedient to do this because the admission of documents is governed by special rules (Tapper, 2004). A court would accept as real evidence a document tendered in evidence as a chattel which, according to Tapper, could occur in the case of a document, that has been allegedly stolen, being tendered as an exhibit during a trial. However, if tendered as a statement, the evidence would be circumstantial, as occurs when tendering documents.
during legal title challenges. These precedents and legal rules have implication for the admissibility of digital evidence.

Normally, computer-based crime consists of human witness-based evidence and physical exhibits, such as fingerprints lifted from a computer keyboard; however, much of the evidence is digital in form and circumstantial in nature (Stephenson, 2000). Although, each piece of circumstantial evidence may not always hold sufficient weight to prove a case in its own right, its worth becomes apparent when it can be used with other evidence to form part of a compelling legal case (Stephenson, 2000).

Physical documents are commonly used as exhibits in a trial and are treated usually as supporting evidence in tandem with other evidence that forms the combined testimony for the presenting party; because of some perceived similarity with physical documents, digital evidence is treated the same in the courts (Tapper, 2004). It is common that a documentary exhibit is not submitted as evidence in isolation, but is supported by other related evidence that enhances its admissibility and reliability (Tapper, 2004). For example, a drug sample may require some independent proof of its seizure, analysis and safe-keeping measures, to ensure that there is less chance of its validity being damaged by a challenge from the opposing party. This may include the evidence of expert witnesses, a register of case exhibits, a photograph, some other visual record, or a witness statement (Tapper, 2004).

The same expectation of supporting evidence is true when digital evidence used in a testimony requires some explanation from system administrators and information managers. For example, in the process of linking a suspect, believed to have sent a threatening email to another person, a witness observed the suspect typing at the computer terminal used to send the threatening email at that exact time of the offence. Presented with this prima facie evidence, the investigator would attempt to link the properties of the computer operating system, such as date and time stamps, and the email containing the threat, to the direct evidence from the human witness that confirms the suspect was using the computer at the exact time the email was dispatched to the victim.

Even in what looks like a straightforward reconstruction of the case, the case would fail if the digital evidence was inadmissible, or its evidentiary weight weakened because of anomalies or uncertainty about the computer operating system and application software (Sommer, 2000). Now the investigator may seek explanation from knowledgeable personnel in the organization about the computer network, its operating and application programs, user access controls, system security, and so forth. This corporate knowledge could well form part of the legal case and require the organization’s personnel to testify and provide explanation about the computer network and attest to the efficacy of its security.
Hearsay Evidence

Another commonly accepted form of evidence is hearsay evidence, and digital evidence may take the form of indirect evidence, or hearsay, depending on the context in which it is used (Casey, 2004). Hearsay evidence is any matter that a witness does not have direct experience of - something the witness has not observed through the five senses. For example, if John tells Ann about some event he witnessed but Ann did not witness the event, Ann cannot use that evidence, as she has no firsthand knowledge of what John observed. All Ann possesses is hearsay from John (Stephenson, 2000). Courts look to establish the credibility of the witness based on the perception of the witness, their memory and ability to recount their observation of relevant matter; hearsay evidence does not provide such credibility and the court cannot cross-examine a witness to satisfy itself of the credibility of the witness (Kenneally, 2004).

Hearsay evidence is usually inadmissible in common law jurisdictions, such as in Australia, the USA, the United Kingdom, and a number of other countries because its truthfulness cannot be verified; digital evidence falls within this convention (Casey, 2004; Kenneally, 2004). However, in these countries, because of special statutes, digital evidence is commonly admissible in civil proceedings and may be admitted as a matter of discretion in criminal cases, but this does raise claims that such leniency runs contrary to the interests of justice (Tapper, 2004). For example, business records, including electronic records, are admissible in evidence as an exception to the hearsay rule but are subject to certain requirements, such as would be maintained in normal business activities and assurances that reasonable measures were taken to protect the authenticity and accuracy of the records (Chaikin, 2006). It is common in cases, where this evidence is presented that the custodian of the records, or other qualified witness, is asked to provide some evidence that the records are trustworthy (Chaikin, 2006).

For private organizations, where the requirements for maintaining business records are less stringent than for a government organization, the courts may expect some additional evidence to attest to the trustworthiness of the computer system holding the records and the personnel managing the system. This could include testimony about the security and integrity of the system, and the existence of quality checks to verify the accuracy and authenticity of records (Marcella, 2002).

In terms of digital evidence, such as database records and audit logs, it has been argued that they are often automatically computer-generated and do not contain a statement of declaration from a human witness (Chaikin, 2006). Successful argument during some trials has allowed the admission of such records, but such admission is contingent on the reliability and accuracy of the computer software applications.
that create and record the evidence, and provided that they are created as part of the normal course of business (Chaikin, 2006).

Hearsay challenges have been avoided in trials by successful argument that digital evidence constitutes an outcome of a pre-programmed computer function, such as the processing of admissible data, like the automatic recording and processing of data by a radar gun recording the speed of passing vehicle (Kenneally, 2004).

**Expert Evidence**

Opinion of witnesses is not admissible in court hearings and witnesses are not permitted to present their own inferences and interpretation of their observations. The court would direct them to confine their evidence to recounting events they have directly observed. The rule is relaxed for expert and scientific witnesses, who may be allowed to provide their opinion that falls within their range of expertise (Tapper, 1999).

Other issues arise concerning the reliability of expert witnesses testifying in cases relying on digital evidence. For example, in courts in the United States of America, the Daubert standard requires that the expert witness must satisfy strict criteria including a requirement for them to establish their personal standing in the relevant discipline, such as in publication and teaching (Brodsky, 2000). Furthermore, an expert witness must also satisfy the court that methods and techniques used to form the expert’s opinion require empirical testing, that methodologies and techniques were subject to peer review, publication and were accepted in the corresponding scientific community, and that there should be known error rates for methodology and techniques.

The use of standards and controls in the course of cyber forensic analysis would assist courts in determining the credibility of the expert witness (Barbara, 2008). However, at the time of writing, there are no generally accepted tests for cyber forensics; such tests would need to describe the theory and methods used to explain the intricacies of how computers work (Mohay, 2003). The difficulties in providing meaningful tests or templates are overwhelming, as every test carried out individually would only reflect the interaction of the event of evidentiary interest with the entire system. As no two sequences of events would be identical, it may be difficult to explain the technical processes involved to the courts. Consequently, Mohay believes that a special case could be made for digital evidence to have its own standard, independent of the Daubert standard.

While enhanced information security reduces the risk of vexatious investigations and legal remedies, an analysis of what resources are at risk from a multitude of threats must be professionally analyzed.
CONCLUSION

This chapter has provided statistics and comments associated with real threats to business from security breaches and attacks on information resources and has also described the nature of digital evidence increasingly relied upon to support criminal, civil, and internal disciplinary proceedings. The chapter has also provided a basic overview of the security problem from a management of Information technology resources point of view, through interviews with IT personnel in a small Australian University, and from a mid-sized Australian wide retail organization. Both the statistics reported and insights of the IT professionals, whilst illustrative, are likely to be reflected in many other organizations in many other countries. The risks to businesses and to customers have also been addressed, with risks to businesses being identified not only in stock market fluctuations, but also in terms of brand reputation.

From the interviews, two approaches to security emerged; one of intensive lock down using third party propriety software tools, usually in some kind of outsource arrangement; and a more liberal view taking into account specific needs of employees. An alternative school of thought is also acknowledged in the literature, specifically of Workman et al. (2008); one that highlights the human behavioral aspects, and suggests that employees should be made more aware of the vulnerability of the organization to security breaches and how serious the implications may be for them. This is recommended as an educational program with follow up training to ensure that employees treat the security issue seriously. The philosophy of this approach is based on studies that indicate that employees are lax about security and lack motivation to use existing security features, resulting in some cases of breaches in security from “even modest and uninspired security attacks” (Workman, et al., p. 2813). Future predictions consistently indicate that cybercrime will increase and that organizations need to be aware of potential threats. Whilst technical solutions, policies and continuity planning all continue to be relevant responses, awareness by employees of the real threats and an understanding of the importance of security measures, both internally and externally, appears to be the best defense against a catastrophic security breach event.

ACKNOWLEDGMENT

The authors would like to thank all respondents, including Ms. Maureen Klinkert (Director, ITS - Information Technology Service of the University of the Sunshine Coast), Mr. Barry Mahoney (Manager, ITS - Information Technology Service) and Mr. Barry Pollard (ICT Infrastructure Team Leader - Information Technology...
Service University of the Sunshine Coast) for their insights into the problem from an educational industry perspective.

REFERENCES


Overview of Digital Business Security Issues


ENDNOTES

1. A Botnet is a term used to describe software robots or bots (usually malicious) that automatically run through a computer network and are controlled remotely.


3. For more information on the technical issues, readers are advised to refer to specialist publications that address this area in more detail. In addition, the rapidly changing environment of the internet, in particular, Web 2.0 technology makes a complete and up to date analysis of all aspects impossible.

4. The interviews of managers aspect of this study was approved by the ethics committee of the University of the Sunshine Coast and managers participated on the basis of informed consent.

5. A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is designed to make a website unavailable to customers. This is usually done through generating external requests for services that are not legitimate, thereby slowing down genuine requests.


8. The protocol used to define the specifications for an information security management system.

10. Cloud computing is computer technology that allows services to be provided over the Internet in such a way that the end user does not need to have any expertise or knowledge of the technology.

13. GXS provides Global Electronic Data Interchange and business to business e-Commerce & Data Synchronization Solutions.

Overview of Digital Business Security Issues


22 Although dated now, a still thrilling account of surveilling and tracking down a hacker is given in Stoll’s (1990) book The cuckoo’s egg (the Bodley Head, London)

23 Chapter three provides more details on how to address this situation, should a forensic investigation be required.

24 Cyber forensics is also known as computer forensics and digital forensics


Copyright © 2011, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.