JICLT
Journal of International Commercial Law and Technology
Vol. 6, Issue 2 (2011)

Defining the Current Corporate IT Risk Landscape

Verine Etsebeth
Senior Lecturer, University of Witwatersrand School of Law
School of Law, Private Bag 3
Wits 2050, Johannesburg, South Africa
Email: Verine.Etsebeth@wits.ac.za
Phone: +27-11-717-8446
Fax: +27-717-8539

Abstract. Information has always been one of the most important assets a company possesses. Trade secrets, patents and 'know-how' are important business assets. In a post-industrial economy, however, knowledge-based assets have become crucial not only for the survival of any company, but also for its continued existence. Every company decision is based on reliable and accurate information. Moreover, today companies retain a significant amount of sensitive, confidential and classified information on their computer systems and networks. It therefore follows that anything that threatens the information assets of the company will directly endanger the performance and efficiency of the company. Unfortunately, corporate information assets are susceptible to various forms/types of cyber attacks. These attacks range from unauthorised access, malicious mobile code and inappropriate use to disclosure and information and/or data theft. The increased use of the Internet by companies highlights these vulnerabilities and renders the effective protection thereof all the more relevant. It is submitted that adversaries no longer launch cyber attacks for fame, but rather for financial gain. Companies need to strike a balance between the protection of sensitive and confidential corporate information and the availability of such information to stakeholders. Corporate information must be available to stakeholders, and in some instances to the public, not only to encourage investment in the company, but also to comply with the company's statutory duty of disclosure and transparency. The importance of corporate information and the protection of its integrity against ever-increasing risks and threats necessitate that companies gain assurance that reasonable steps are taken to secure the corporate information assets. Failing this, the company and/or its employee(s) may face potential legal liability. This paper will first analyse the most prevalent cyber risks facing companies today before moving on to identify crucial legal questions that directors and members of top management must ask themselves in order to determine their potential legal exposure in instances of security breaches.

1. Introduction

"*Security is always excessive until it is not enough"* (Sinclair 2009).

As reiterated throughout this paper, information has always been one of the most important assets a company possesses. Trade secrets, patents and 'know-how' are important business assets. In a post-industrial economy, however, knowledge-based assets have become crucial not only for the survival of any company, but also for its continued existence. Every company decision is based on reliable and accurate information. Moreover, today companies retain a significant amount of sensitive, confidential and classified information on their computer systems and networks. It therefore follows that anything that threatens the information assets of the company will directly endanger the performance and efficiency of the company.

Unfortunately, corporate information assets are susceptible to various forms/types of cyber attacks. These attacks range from unauthorised access, malicious mobile code and inappropriate use to disclosure and information and/or data theft. The increased use of the Internet by companies highlights these vulnerabilities and renders the effective protection thereof all the more relevant. It is submitted that adversaries no longer launch cyber attacks for fame, but rather for financial gain (Getronics 2009). Companies need to strike a balance between the protection of sensitive and confidential corporate information and the availability of such information to stakeholders. Corporate information must be available to stakeholders, and in some instances the public, not only to encourage investment in the company, but also to comply with the company's statutory duty of disclosure and transparency.

The importance of corporate information and the protection of its integrity against ever-increasing risks and threats necessitate that companies must gain assurance that reasonable steps are taken to secure the corporate information assets. Failing to do this, the company and/or its employee(s) may face potential legal liability.

2. The Importance of Information Security

Information security is concerned with how management considers, applies and administers information security in their supervision, monitoring, control and direction of the company. Various benefits may be derived from information security, including enhanced economic performance, increased productivity and growth, adequate protection of corporate information assets, resources and systems and ensuring the continued viability and prosperity of the company.

Notwithstanding this, arguably the most important benefit is to be found in this discipline's ability to provide management with a mechanism to escape legal liability based failed or inadequate information security. Consequently, if directors can show the existence of an effective information security programme in the company, they would have gone a long way in convincing the court that they have fulfilled their duty of due diligence. This would hold true irrespective of the type or nature of the security breach/incident that may occur or has occurred in the past.

In the 1970's till 2001, information security was technology driven (Getronics 2009). Since 2001 till 2007 information security has been compliance driven (Getronics 2009). It is predicted that from 2008 onwards corporate information security will be risk driven (Getronics 2009).

3. The Current Risk Landscape in which Companies Function

"The world is a dangerous place" (Schneier 2000). Today more than ever, this statement holds true. Companies face a vast and ever-increasing number of cyber attacks on their corporate information assets. John Pironti observes that the reason why corporate information security is so difficult may be ascribed to the fact that adversaries have vast resources at their disposal, adversaries only need to master one attack, companies must, however, continuously comply with new security regulations and legislation while still aligning their information security efforts with business goals (Getronics 2009). In this paper three broad categories of cyber attacks are identified, which pose a very real danger to corporate South Africa's information assets, namely (i) interference with information and/or data - where an adversary compromises the confidentiality, integrity and availability (CIA) of corporate information assets; (ii) interception of information and/or data - where an adversary not only obtains unauthorised access to corporate information, but he/she is also able to delete, alter or modify it; and (iii) impersonation – where an adversary masquerades or impersonates an authorised user.

3.1 Attacks involving interference, interception and impersonation of information and/or data

3.1.1 Identity theft

Identity theft encompasses all three categories of cyber attacks and it is therefore not surprising that companies regard it as one of the biggest cyber threats facing them today. Management is likely to encounter this threat more than once if not more frequently during their term in office.

Bruce Schneier correctly remarks: "*Why steal from someone when you can just become that person? It's far easier, and can be much more profitable, to get a bunch of credit cards in someone else's name, run up large bills, and then disappear*" (Schneier 2000). Identity theft is often referred as the crime of our times (Koerner 2007). It is easy to execute and highly profitable. Moreover, the adversary has a good chance of escaping prosecution.

Identity theft can be performed in various ways. Some of the most popular ways include: shouldersurfing; eavesdropping; inappropriate access; after-hour activities of employees or even members of management; phone phonies; dumpster diving; electronic leftovers; company web sites; cookies; distributed password cracking attacks; internet Protocol (IP) address spoofing; sniffers; spoofing; web bugs; web spoofing; session hijacking; page jacking; phishing; and pharming.

3.1.2 Corporate and industrial espionage

Corporate and industrial espionage makes use of all three categories of cyber attacks. The information age, and more specifically the use of the internet by most companies, make corporate and industrial espionage faster, easier and more anonymous. It is not surprising that there has been a noticeable increase in corporate and industrial espionage in recent years (Konrad 2005).

Corporate and industrial espionage entails the process of collecting information pertaining to a specific target in order to obtain profit from this action. It can be defined as "operations conducted by one corporation against another for the purpose of acquiring a competitive advantage in domestic or global markets" (Wallace 2005). The individuals responsible for industrial and corporate espionage (also known as 'corporate raiders') are defined as "employees who attack computers of competitors for financial gain" (Wallace 2005). A key feature of this type of attack is the collection of information and the objective of making a profit. During the collection process, adversaries are willing to make use of any means possible (legal or illegal) to obtain the required information (Wallace 2005).

3.1.3 Social engineering

Social engineering is defined as "successful or unsuccessful attempts to induce one or more persons to either reveal information or to act in a manner that would result in unauthorised access, unauthorised use, or unauthorised disclosure, to an information system, network or data" (Tipton and Krause 2003). This type of attack exploits human characteristics such as the desire to be helpful or spiteful (Tipton and Krause 2003). It focuses on the individual rather than the group, thus exploiting individual fears, believes and hopes.

The success rate of social engineering is dismaying. Even more vexing is the fact that social engineering bypasses cryptography, computer security, network security and all other technological defences (Tipton and Krause 2003). It defeats information security without the use of technical security mechanisms. Companies often forget that computers and technology are merely tools used by human beings. The problem with these tools is that humans must use, configure, install and implement them. Ultimately, social engineering manipulates the weakest link in any company - its own employees.

3.2 Attacks involving interference with information and/or data

Certain cyber attacks do not have as their main objective the interception of information and/or data. These types of attacks merely desire to interfere with the workings of the corporate information assets. This does not mean that their consequences and impact are less pernicious. The contrary is in fact true. Companies incur vast financial losses because of interference with their information and/or data. Two of the best-known forms of cyber attacks in this category are dealt with in this section.

3.2.1 Denial of service attack (DoS)

Denial of service attacks (hereafter DoS) occur frequently in practice (CSI/FBI 2007). Companies are at present very reliant on e-commerce applications. A well-timed denial of service attack will therefore have a significant pernicious effect on any company.

DoS entails one user denying services to another legitimate user. This objective is achieved by flooding the site with so much traffic that no other traffic can get in or out. Consider for instance the situation where an adversary floods a system with bogus traffic causing the server to crash (SANS 2007). Physical danger can even ensue if the servers that control sensitive machinery, for instance in a hospital or other critical operating facility, are brought to a complete halt. Noteworthy is the fact that the adversary initiating this type of attack does not have the objective of trying to break into a system and steal information. The aims are rather to stop something or someone from working (Drummond and McClendon 2001). DoS attacks can thus be compared to strikes, boycotts and blockades in the physical world (O'Reilly 2001).

3.2.2 Distributed denial of service attacks (DDoS)

A distributed denial of service attack (hereafter DDoS) is a successor of DoS attacks (TechTarget 2009). The main difference between the former and the latter is that in a distributed denial of service attack "a multitude of compromised systems attack a single target, thereby causing denial of service for users of the target system" (TechTarget 2009). Consequently, hundreds and even thousands of computers are unknowingly used as zombies to attack a single target, ultimately facilitating the commissioning of a crime. A DDoS attack therefore, goes one step further than a DoS attack by using the power of distribution. It also bears certain advantages over an ordinary DoS attack, namely: (i) the attack is more difficult to detect; (ii) it is difficult to trace the attacker; and (iii) the attack is much more powerful and faster than an ordinary DoS attack (Tipton and Krause 2003).

3.3 Attacks involving interference and/or interception of information and/or data

3.3.1 Malicious mobile code

A malicious mobile code may be defined as "any software program designed to move from computer to computer and network to network to intentionally modify computer systems without the consent of the owner or operator" (O'Reilly 2001). This term includes viruses, Trojan Horses, worms, script attacks and rogue internet codes (O'Reilly 2001). In the past, malicious mobile codes only included viruses, Trojan horses and worms. They also now include "all harmful programs created by scripting language and powered by Internet technologies" (O'Reilly 2001).

Depending on their behaviour, malicious mobile codes may be subdivided into four categories, namely viruses, worms, Trojan horses, and logic bombs. Viruses, worms, Trojan horses and other categories of malicious mobile codes are often confused. Upon closer investigation, however, it becomes evident that they are distinctly divergent with respect to the techniques they employ and their host system requirements.

a) Viruses

Viruses are one of the best-known, yet widely feared, forms of malicious mobile codes. Management is saturated by feelings of fear, anxiety and helplessness at the mere mention of a virus infection. Even the most ferocious information security specialists share this sentiment. These feelings are not unfounded. Similar to its biological counterpart, a virus first infects other programs by including a copy of itself into the chain of command, thereby changing the underlying host structure (Schneier 2000). Infected host files become viruses themselves and begin to infect other files. When the user attempts to execute a legitimate program, he/she also executes the virus (Schneier 2000). Computer viruses are even able to transmute and evolve, like their biological counterparts, to resist anti-virus programs. A virus is a self-replicating program that can spread without outside help once released. It depends on a host program, and more specifically the resources of the host program, in order to replicate and spread (Hutt 1995).

A virus must be activated by some form of external action taken by the computer user (Hutt 1995). It might be something as superficial as switching on the computer. Depending on the type of virus, different degrees and forms of damage will be suffered by a victim. Some viruses are specifically designed to damage and destroy information assets (Schneier 2000). Others have as their sole purpose to crash a system, or to congest a system with unwanted or useless information.

(b) Worms

A worm is "a computer program that can run independently, propagate a complete working version of itself onto other hosts on a network, and consume computer resources destructively" (Tipton and Krause 2003). The main difference between a virus and a worm lies in the fact that a virus infects other computer program, while a worm infests a computer. Inherent in a worm is its ability to replicate (Hutt 1995). Unlike a virus, a worm is a self-contained program that uses its own coding to spread. It therefore does not attach itself parasitically to a host program (Hutt 1995). Worms are furthermore self-activating programs. The user consequently does not have to activate the worm before it starts doing damage. Worms generally operate by spreading functional copies of themselves, or their segments, to all parts of the computer and to other computers via network connections or email attachments (Goldberg 2003).

(c) Trojan horses

A Trojan horse attack involves a program "in which [a] malicious or harmful code is contained inside apparently beneficial or harmless programming or data in such a way that it can get control and do its chosen form of damage, such as running the file allocation table on a hard disk" (TechTarget 2009). Trojan horses are non-replicating programs that require some kind of action to be taken by their victim. As a result of this attribute, it generally includes some element of social engineering (O'Reilly 2001). Although Trojan horses represent the most common method of introducing viruses into computer systems, they are distinctly different from viruses (Drummond and McClendon 2001). The most important difference pertains to their replication methods. A virus copies its coding into a host file, whereas a Trojan begins its life by attaching to a host file and spreading by using that file (O'Reilly 2001). Trojan programs are generally spread via public-access electronic bulletin board systems (BBSs). They can be downloaded when one opens a file on the internet or an email attachment.

(d) Logic bomb

The logic bomb represents the oldest form of malicious programming. It involves the creation of a dormant code that is later activated or triggered by specific circumstances or events (Tipton and Krause 2003). It can be a component of a virus or a Trojan horse. It can also be inserted into a legitimate program as a predecessor to blackmail or pre-emptive revenge in anticipation of dismissal. The explosion of a logic bomb can result in the deletion or corruption of data or the display or printing of false messages.

3.4 The adversaries

Having now looked at the major types of attacks that companies are exposed to today, we must turn our attention to the people who initiate attacks. These instigators are known as adversaries (Hunter 2000). An adversary has the capacity to inflict damage and harm directly to corporate information assets, and indirectly to the company (Stoneburner et al 2001). Adversaries can furthermore pose an external or internal threat to a company.

3.4.1 The external threat

Adversaries who pose an external threat generally act intentionally. Their attacks are executed with a specific malevolent purpose or objective in mind. They know what they are doing is wrong. The most commonly found type of deliberate/intentional attack is the malicious attempt at unauthorised access. In this type of attack information is acquired by unauthorised means and without the collaboration of one rightfully in possession thereof (Funnel 2004).

Once access has been gained to one location in the digital network, access can easily be extended to the whole network. Everyone involved in the network can thus be hit by a cyber attack once it has commenced - partners, clients, customers, suppliers, outsourcers and even regulatory bodies. The risk to sensitive and confidential corporate information is thus amplified seven-fold.

3.4.2 The internal threat

The second category of adversaries is known as insiders. Research has shown that insiders have historically been responsible for the vast majority of security breaches and incidents (CSI/FBI 2007). Many companies nevertheless persist with the outdated belief that the external threat is much more significant than the internal threat (Funnel 2004). This erroneous mindset may be ascribed to the fact that the media focus their attention more on external attacks than on internal attacks. Attacks where hackers gain unauthorised access to a high profile company or government department sell more newspapers than incidents where company employees steal information (Gamertsfelder et al 2001). The reality is, however, that most threats are internal, irrespective of whether they are caused accidentally or intentionally. Schneier (Schneier 2000) observes: "*[C]yberspace is particularly susceptible to insiders, because it is rife with insider knowledge. The person who writes a security program can put a back door in it. The person who installs a firewall can leave a secret opening. The person whose job it is to audit a security system can deliberately overlook a few things.*"

Insiders are ideally placed in a company to launch a cyber attack. They have certain advantages over external adversaries. First, they are already inside the corporate information systems (IS system) with some level of authorised or legitimate IT access. The latter is one characteristic all insiders have in common. Secondly, insiders enjoy a certain level of trust as employees of the company, and finally, they possess insider knowledge that they can use to their full advantage (Funnel 2004). This insider knowledge usually involves the following information: (i) they know which information is of value; (ii) they have knowledge of how the system works; (iii) they know where the vulnerabilities in the system are located and how to exploit them; (iv) they are familiar with the company's structure; and (v) they know the procedure that will be followed from the moment that a security breach or incident is reported to the finalisation of the investigation (Schneier 2000). It is therefore easier for insiders to escape detection, identification and prosecution than for external adversaries. It is important to note the difference between insiders who act accidentally and those who act intentionally.

3.4.3 Accidental actions of insiders

Accidental actions of insiders are generally not accompanied by a specific malevolent purpose or illegal motives (Tudor 2001). These attacks materialise because of accidents that occur as a result of untrained or careless employees. Included in this category are employees who do not follow the prescribed corporate information security standards and best practices (Tudor 2001). Their actions can therefore be described as negligent. Malicious intent (dolus) is absent, but negligence (culpa) will be present.

3.4.4 Intentional Actions of Insiders

Intentional actions of insiders are deliberate attacks performed by individuals who have authorised access to definite levels of information. However, they exceed their level of authorisation in order to view, use, alter or modify classified information (Tudor 2001). These insiders can be subdivided into the following three categories: (a) masqueraders – users who profess to be another authorised user (this amounts to impersonation); (b) clandestine users – users who conceal their actions by way of evading access controls and auditing; and (c) abusers- users who are authorised to use the system, but misuses or abuses the authorisation (Funnel 2004).

4. Legal obligation to provide information security

The scope of a company's obligation to provide information security is two-fold: firstly, it encompasses situations where the company itself fall victim to an attack; and secondly, situations where the company's information assets are used by a malicious party to facilitate an attack against another. It should furthermore be borne in mind that an attack may emanate from an internal or external source. In situations where it emanates from an internal source, it may give rise to vicarious liability whereas in situations where it emanates from an external source, it may give rise to liability based on negligent information security.

What follows is a summary of the most prevalent cyber risks facing companies today. The legal questions that directors and members of top management respectively must ask themselves in order to determine liable are also indicated. Finally, recommended steps that may be taken to limit potential legal liability on each respective ground are provided.

4.1 Scenario 1

An external or internal attack takes place against the corporate information assets that result in losses and/or damage to third parties. As a result of the breach the company may now be faced with civil liability based on negligent information security.

Liability for negligent information security may successfully be established by making use of the existing doctrine of negligence found in the South African law of delict. The doctrine provides that a company and/or its employees will be deemed to have acted negligently if they fail to take reasonable steps to secure their corporate information assets prior to an information security breach/incident occurring. In such an instance a plaintiff who has suffered damages as a result of the information security breach will be able to hold the company liable based on negligent information security. On the other hand, if a company and/or employee took reasonable steps to secure the corporate information assets, but still fell victim to an attack, the company and/or its employee(s) will escape liability based on negligence. It is therefore submitted that the existing South African law of delict, and specifically, may without difficulty be extended to the digital corporate environment to establish legal liability.

To determine whether or not the company will be held liable in civil law, the following general question must be asked: Did the company fail to take reasonable steps to secure its corporate information assets? This general question may be broken down into three straight-forward questions:

- Question 1: Did the company act like a reasonable person (company) would have acted in the same circumstances? Therefore, did the company conform to the generally accepted information security practices of its industry? If the company's conduct did not conform to such practices this is indicative of the presence of negligence.
- Question 2: Were the consequences foreseeable? The forseeability test does not require that the exact nature or extent of the loss suffered or the precise manner of the harm should have been reasonably foreseeable. All that is required is that the general nature of the harm suffered and the general manner of the harm occurring were reasonably foreseeable.
- Question 3: Would a reasonable person (company) have taken steps to prevent the threat from materialising?

A. Recommendations to avoid legal liability in negligence – External attacks

Members of top management must:

(i) Realise and acknowledge that corporate information security is the responsibility of the board of directors;
(ii) ensure that reasonable steps are taken, on a continuous basis, to secure corporate information assets;
(iii) gain assurance that information security forms an integral part of the overall corporate structure;
(iv) ensure that a balanced approach between all three components of information security, namely physical, technological and procedural security, is adopted;
(v) align information security mission, goals and objectives with corporate mission, goals and objectives;
(vi) ensure that adequate physical security measures have been implemented;
(vii) ensure that adequate procedural security measures have been implemented; and
(viii) ensure that adequate technical security measures have been implemented.

B. Recommendations to avoid legal liability in negligence – Internal attacks

Companies must ensure that their employees receive the necessary information security awareness and training by developing, implementing and maintaining:

(i) information security documentation (policy, procedure, standards and guidelines) which are widely known and understood;
(ii) a comprehensive information security awareness and training programme;
(iii) a website terms and conditions policy;
(iv) a website privacy policy; and
(v) a website disclaimer.

4.2 Scenario 2

An internal attack takes place against the corporate information assets that result in losses and/or damage to third parties. As a result of this incident the company may now face potential civil liability based on vicarious liability. At present the international trend is to hold companies vicariously liable for the unintentional, as well as intentional acts of their employees committed inside or outside the scope of their employment. This will necessarily have far-reaching consequences for companies in the information age. Companies may now be held liable for, for instance inappropriate use/abuse of corporate Internet and email facilities, in the form of harassment, discrimination, defamation (resulting from ill-conceived wording in an email), copyright infringement (where the employee carelessly downloads and disseminates copyright material and software), criminal liability (if child pornography is downloaded), and even liability under contract law (where an employee inadvertently forms a contract through an email), to name but a few. Proponents of vicarious liability for failed/inadequate information security argue that enforcement of such liability will not only motivate companies to seriously consider the discipline from the outset, but also to dedicate adequate resources to its development and implementation.

To determine whether the company will be held liable in civil law, the following general question should be asked: Is there a sufficiently close connection between the employee and company to hold the company liable for the act(s) of the employee(s)? This general question can be broken down into three straight-forward questions:

- Question 1: Did an employer-employee relationship exist between the parties?
- Question 2: Was a wrongful human act committed?
- Question 3: Was the act committed in the scope of employment? (Determine: if the work relationship creates the risk or enhances such risk and if there was a sufficiently close connection between the wrongful act and the risk (generally foreseeable cost) created by the enterprise).

A. Recommendations to avoid vicarious liability - Internal attacks

The company must ensure that all employees receive the necessary information security awareness and training. This would entail the development, implementation and maintenance of:

(i) information security documentation (policy, procedure, standards and guidelines) which are widely known and understood;
(ii) a comprehensive information security awareness and training programme;
(iii) an e-mail disclaimer;
(iv) a website terms and conditions policy;
(v) a website privacy policy;
(vi) a website disclaimer; and
(vii) a risk management programme.

4.3 Scenario 3

An external or internal attack takes place against the corporate information assets that result in losses and/or damage to third parties. As a result of this breach the company may face potential civil liability based on privacy infringement.

Traditionally, it was relatively easy for an individual to protect his privacy. He would disclose his personal information, in written form only to a selected few. He would know exactly the purpose for which his information would be used and he would be able to control whether or not his personal information was shared with others. At present, however, individuals have lost complete control over their personal information. They have no control over who it is disclosed to, for what purpose it is used, or even whether or not it is transferred to unknown third parties. This chapter observes that legislatures world-wide have come to realise the dangers inherent in allowing companies to indiscriminately share the personal information of its citizens. Internationally, privacy and data protection statutes are being drafted and enacted at an aggressive pace. Unfortunately, South

Africa still lags far behind in the domain of online privacy and data protection. Currently, existing legislation is incompetent to deal with the challenges posed by online privacy and data protection. This is in part due to the fact that in the past, the South African legislature deemed it unnecessary to expressly provide for the right to privacy until 1993 with the introduction of the Interim Constitution and in part, to the fact that the drafter of the Constitution could never foresee the severity, intensity and frequency of the onslaught on privacy of individuals the digital environment would initiate.

To determine whether or not the company will be held liable in civil law, the following general question must be asked: Did inadequate information security of the company result in the unauthorised disclosure of confidential and/or sensitive information?

This general question may be broken down into the following specific questions:

Question 1: Was the information that was collected/stored necessary for, or directly related to, a lawful, explicitly defined purpose that does not intrude upon the privacy of an individual/group of individuals/business entity to an unreasonable extent?

Question 2: Was the information collected directly from and with the consent of the individual/group of individuals/business entity?

Question 3: Was the individual/group of individuals/business entity informed of the purpose of any such collection and of the intended recipients of the information, at the time of collection?

Question 4: Is information only kept for as long as is necessary for achieving the purpose for which it was collected?

Question 5: Was the information distributed in a way that is incompatible with the purpose for which it was collected?

Question 6: Were reasonable steps taken to ensure that the information processed was accurate, up to date and complete?

Question 7: Were appropriate technical, procedural and physical security measures taken to safeguard the individual/group of individuals/business entity against the risk of loss, damage, destruction of or unauthorised access to personal information?

Question 8: Are individuals/groups of individuals/business entities given the right to access their personal information and the right to demand correction if such information is inaccurate?

A. Recommendations to avoid legal liability for privacy infringement – External attacks

Companies must ensure that they have adequate information security measures in place. This entails:

(i) ensuring that physical security measures are implemented and re-evaluated on a continuous basis;

(ii) implementing and re-evaluating procedural security measures on a continuous basis; and

(iii) implementing and re-evaluating technological security measures on a continuous basis.

B. Recommendations to avoid legal liability for privacy infringement - Internal attacks

A company must ensure that it has adequate information security measures in place, and that its employees receive the necessary information security awareness and training. This entails the development, implementation and maintenance of:

(i) information security documentation (policy, procedure, standards and guidelines) which are widely known and understood;

(ii) a comprehensive information security awareness and training programme;

(iii) a website terms and conditions policy;

(iv) a website privacy policy; and

(v) a website disclaimer.

5. Conclusion

As this paper demonstrates the potential for legal liability for failed or inadequate corporate information security is vast. Although it is acknowledged that the law has not effectively dealt with the problems created by the information age, customers and clients alike will not accept this as an excuse for companies who fail to live up to their security promise. Knowing what to do and when to do it will mean the difference between failure and survival. Most companies will view the implementation of the recommendations in this paper as an insurmountable task. As the proverb states: "[T]he largest journey begins with a single step." Moreover, companies should remember that an effective and efficient corporate information security infrastructure is no longer optional. It is now mandatory.

Pursuant to the discussion contained in this paper, the holistic nature of information security is clearly evident. By following the recommendations made in this paper, companies can rest assured that the most important legal aspects of corporate information security have been considered and have been addressed. Moreover, companies will have gained the assurance that they have taken reasonable steps to secure the information assets of the company, and that if faced with legal action they are likely to be successful in their defence.

"In God we trust. All others we virus scan" – Unknown

References

Books

1. CSI/FBI (2007) *Computer Crime and Security Survey*
2. Harley David and Robert Slade (2001) *Viruses Revealed* McGeaw Hill Companies
3. Hunter (2000) *Information Security: Raising Awareness*
4. Hutt et al (1995) (eds) *Computer Security Handbook*
5. O'Reilly (2001) *Malicious Mobile Code – Virus Protection for Windows*
6. Schneier (2000) *Secrets and Lies: Digital Security in a Networked World* Wiley Publishers
7. Stoneburner et al (October 2001) *Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology* Special Publication 800-30 United States Government
8. Tipton and Krause (ed) (2003) *Information Security Management Handbook* Vol 3 Auerbach Publications
9. Tudor (2001) *Information Security Architecture: An Integrated Approach* Auerbach Publications

Journals

1. Drummond and McClendon (2001) "Cybercrime – alternative models for dealing with unauthorised use and abuse of computer networks" *Law and Internet* 3
2. Funnel (2004) "Enemies within: the problem of inside attacks" *Computer Fraud & Security* 7
3. Gamertsfelder et al (2001) "Under lock and keyboard – prevention of unauthorised use of corporate computer systems" *New South Wales Society for Computers and the Law Journal* Issue 46 1
4. Goldberg (2003) "Cyber risks confronting airlines: a practical approach to manage the risks and pursue the wrongdoer" *Air & Space Law* Vol XXVIII/6 295.

Website

1. Getronics "The future of information security: what is next?" www.getronics.com (last visited June 2009) 13. Koerner "Data breaches 2007"
2. http://idtheft.about.com/od/databreaches2007/a/Databreaches07.htm?p=1 1 (last visited June 2009)
3. Konrad "Leak and geeks: international espionage goes hi-tech" http://news.com.com/2102-1001_3-242620html?tag=st.util.print 2 (last visited March 2005).
4. SANS "Glossary of terms used in security and intrusion detection" http://www.sans.org/resources/glossary.php 24 (last visited June 2009)
5. Sinclair "Excessive security" http://www.patronusanalytical.com/files/Excessive%20Security.php 1 (last visited June 2009)
6. TechTarget "Distributed denial of service attacks" http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci557336,00.html 1 (last visited June 2009)
7. Wallace "Industrial espionage experts" http://www.newhaven.edu/california/CJ625/p6.html 2 (last visited March 2005)