INFORMATION SECURITY POLICIES – THE LEGAL RISK OF UNINFORMED PERSONNEL

Verine Etsebeth

Faculty of Law, University of Johannesburg

A Faculty of Law
University of Johannesburg
PO Box 524 Auckland Park 2006
Fax +27 11 489 2049
space_law@yahoo.com

ABSTRACT

The importance of information security policies are captures by the following quotation: "…the cornerstone of an effective information security architecture is a well written policy statement. This is the wellspring of all other directives, standards, procedures, guidelines, and other supporting documents" (Peltier 2002).

Although the development and deployment of an effective information security infrastructure within the company is imperative to the success of the overall information security discipline, it will be a futile exercise if those people who are expected to maintain and monitor information security in the company do not know what is expected and demanded of them. The importance of information security policies can not be overemphasised as it may be the most cost-effective action a company may take against information security breaches and incidents. The employees of a company may be viewed as the first line of defense when it comes to the early detection of problems. Consequently, employees on all levels of the company must be made aware of the pivotal role security, and specifically information security plays within a company. They need certainty on what their responsibility for information security within the company is, and what will happen if they do not comply with their security duties. Put differently employees need to be told what they may and may not do with corporate information assets, resources and systems. Furthermore, it should be kept in mind that although traditionally information security was viewed by the board of directors and top management as a necessary evil, at present companies are being placed under increased pressure by means of new laws and regulations to ensure that information security is effectively implemented within the company. Consequently, if an information security breach or incident occurs because of the actions of an uninformed or negligent employee, the board of directors and top management may be held personally liable for the conduct of that employees. It is therefore imperative that the information security policy of the company is formulated correctly in order to limit a company's potential legal liability for the negligent or even intentional acts of its employees.

The account contained in this contribution is meant to give a broad overview of information security policies having specific regard to the salient legal issues embedded in the development and implementation of these policies. More specifically the aim of this paper is to provide companies with a framework against which they may develop their own information security policy which they may adapt to provide for the specific needs of their individual company.

KEY WORDS

Information security, Awareness and Training, Security Policies and Procedures, Legal Liability

INFORMATION SECURITY POLICIES – THE LEGAL RISK OF UNINFORMED PERSONNEL

1 INTRODUCTION

Information security documentation is of specific importance from a legal and managerial viewpoint. The reason being that within this area the "human factor/threat" is embedded. Scheiner (2002) observes that securing digital data is not the biggest problem facing companies, but "securing the interaction between the data and the people" therein lies the problem.

Historically, a company's own employees or "insiders" have been responsible for the vast majority of security breaches, yet companies still persist in the outdated belief that the external threat is much more significant than the internal threat. This is despite research and surveys proving the contrary to be true (Funnel 2004). The erroneous corporate mindset may be ascribed to the fact that the media focuses its attention more on external attacks, such as hackers gaining unauthorised access to a high profile company or government department, than on internal attacks (Gamertsfelder *et al* 2001). The reality is, however, that the majority of threats are caused internally, whether they are caused accidentally (by an untrained employee), or intentionally (by a disgruntled employee) (Tudor 2001). In 2005 35% of all information security breaches and incidents originated from an internal source. This is compared to 14% in 2004 and 10% in 2003 (Beishon 2005). Therefore the insider threat is undeniably on the rise. Schneier (2000) observes: "… cyberspace 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 within a company to launch an attack. Moreover, insiders have three "advantages" over external attackers. First, they are already inside the corporate information system with some level of authorised or legitimate information technology access (Funnel 2004). The latter is the one characteristic that all insiders have in common. Secondly, they enjoy a certain level of trust as employees of the company; and finally, they possess insider knowledge, which they may use to their full advantage. Such knowledge includes: (i) Knowing which information is of value; (ii) Knowing how the corporate system works; (iii) Knowing where the vulnerabilities in the corporate system are located and how to exploit them; (iv) Being familiar with the company's structure; and (v) Knowing the procedure that will be followed from the moment that a security incident is reported to the finalisation of the investigation. Consequently, it is easier for an insider to escape detection, identification and prosecution than for an external attacker.

The reason why the insider threat is of such pivotal importance to a company may be ascribed to the doctrine of vicarious liability. In terms of this doctrine a company may be held liable for the acts/conduct of its employees performed within the scope of their employment. Consequently, if an employee uses any of the information assets, resources or systems of the company to launch or facilitate a cyber attack against another, the downstream victim will be able to hold the company legally liable. The only defense available to a company would be to prove to the court that it had, amongst other things, effective information security documents in place which expressly prohibited the conduct/actions of the employee. Is should therefore be evident that in order to counteract the human factor/"insider threat" companies inject information security documentation in the form of policies, standards, procedures and guidelines into the company. Certain important legal aspects must, however, be taken into consideration when drafting, implementing and enforcing these security documents.

2 INFORMATION SECURITY DOCUMENTATION HIERARCHY

The discussion which follows is based on the following hierarchy:

Legislation

(Legislation is established by government, which may create policies that may or may not be enacted in legislation).

Corporate Information Security Policy

(States corporate goal in general terms).

Information Security Standard

(Define what is to be accomplished in specific terms).

Information Security Procedure

(Step-by-step reference guide telling employees how to meet the standards)

Information Security Guidelines

(They are general recommendations of what companies would like to see its employees do).

2.1 Information Security Policies

2.1.1 The importance of information security policies from a legal perspective

The most important information security document in the corporate environment is the information security policy. The question may be asked why the need for an information security policy exist within an company? In general companies are motivated to implement information security policies by five major consequences that may ensue if they do not have this policy in place: (i) Loss of competitive advantage; (ii) Loss of customer and shareholder confidence; (iii) Increased

governmental interference; (iv) Non-compliance with legislative requirements; and (v) The risk of legal liability increases (Peltier 2002). The two latter points are of specific importance.

a. Non-compliance with legislative requirements - Certain legal requirements demand that policies and procedures are in place. Amongst these requirements we encounter the duty care and skill/due diligence. The importance of security documentation lies in the fact that they will come into play should an information security incident take place that calls the operation into question (Peltier 2002).

b. Risk of legal liability increases - Even if a company is not legally bound to develop and implement an information security policy, such a policy will prove to be beneficial to the company for the following reasons: (i) Information security policies will strive to find a way to best conduct business while simultaneously protecting the identity, authenticity, confidentiality and integrity of the information assets of the company (Mistry 2002); and (ii) The possibility of litigation is reduced over issues pertaining to wrongful termination; discrimination; unfair labour practices and theft (Voges 2002).

Voges (2002) observes that "Internet law is still very confusing, but enterprises with [information security] policies in place can protect themselves from unnecessary headaches." He goes on to observe that companies who have an effective information security policy that recognises and complies with internationally acceptable standards, will have a distinct advantage over those companies who adopt a "wait-and-see" attitude. Companies who do not have an information security policy in place, or do have such a policy, but the policy is not effectively enforced, are earmarked as being prone to fall victim to attacks from hackers, crackers and other threat agents (Voges 2002). This will ultimately result in loss of customer confidence and shareholder value.

After reviewing why the need for information security policies exist, it should be clear that companies (and specifically the board of directors) may be labelled as being reckless, negligent and irresponsible if they allow the company to function without having an effective information security policy in place. In practice however, we still encounter numerous companies that are willing to take this risk, be it out of arrogance or mere ignorance.

2.1.2 The dangers of conducting business in the information age without effective information security policies

It is common practice for some companies to function without a formally written information security policy (Peltier 2002). The unwritten information security policy is much like a custom passed on by one employee to the other by word of mouth. However, this results in uncertainty, confusion and possible grounds for legal action. One of the most prevalent problems experienced in this regard is that no roles or responsibilities are formally assigned to employees. Therefore problems will arise when top management wants the hold an employee liable for non-compliance. These problems include: (i) no explicit role or responsibility has been assigned to the employee, and/or (ii) if such a role or responsibility has been assigned, the employee may claim that he is unaware of his role or responsibility (Peltier 2002). The doctrine of legitimate expectation may also be utilised by the employee.

Unwritten policies, procedures and standards may open the company up to potential liability. The following citation from Tudor (2001) highlights the inherent dangers prevalent in not having a formal written information security policy: "…it is very difficult to test for the effectiveness or compliance anything that is undocumented. In addition, it has been set as a legal precedence that companies must show or prove due care when enforcing policies, in which case they have made an effort to be in compliance, in a minimum, with industry standards. From a legal perspective enterprises must be prepared to show that they have communicated to their employees, users of

their system, and business partners, appropriate use of those systems and resources as well as appropriate ways to effectively protect their business, information, and resources, from damage, theft, destruction, or unauthorized access. This will minimize the risk of legal liability due to negligence and breach of fiduciary responsibility."

Ultimately the question must be asked why companies would willingly open themselves up to potential legal liability in such a reckless manner if the implementation of an austere policy could effectively protect them? It should be evident from the preceding discussion that the primary reason for having an information security policy is to aid directors and top management alike in having concrete evidence to present in court that they had fulfilled their responsibility of due diligence.

Apart from the multitude of legal and regulatory reasons advanced to indicate the benefits attached to having an information security policy, the implementation of such a policy will result in better control over the company which ultimately makes good business sense. It is required of top management to exercise control over the company otherwise the company and/or the board of directors in their personal capacity, may face financial penalties in the form of fines and costs.

3 DEVELOPMENT AND IMPLEMENTATION – THE LEGAL CONSIDERATIONS

3.1 Constitutionality of information security policies

"E-commerce and related IT policies must be built on a constitutional foundation. In the light of the fact that South Africa is a developing contemporary constitutional state, one cannot develop policies in a vacuum, but must at all times consider their constitutional implications" (Jansen 2002).

Whenever drafting not only information security policies, but any information security document that might have legal implications, especially when working within the sphere of the employer-employee relationship, care must be taken not to infringe upon the employees guaranteed rights. Therefore, specific consideration must be given to rights guaranteed in the Constitution 108 0f 1996, as well as in Labour Law legislation. In order to ensure that the following rights are not unreasonably limited or infringed upon, in a direct, or indirect manner: A. Constitutionally guaranteed rights, such as (i) Section 9: The right to equality; (ii) Section 14: The right to privacy; (iii) Section 16: The right to freedom of expression; (iv) Section 18: The right to freedom of association; (v) Section 23: The right to fair labour practices; (vi) Section 32: The right of access to information; and (vii) Section 33: The right to just administrative action; and Labour law rights.

3.2 Labour law requirements for information security policies

In South Africa labour law-issues are regulated by the Labour Relations Act 66 of 1995 (henceforth LRA). Certain aspects of labour law are of specific value to an information security policy, as this is the only security document that contains a section on sanctions. Sanctions may ultimately result in the dismissal of an employee. Consequently, employers must keep the provisions of the LRA in mind when contemplating dismissing an employee for non-compliance with, for instance the information security policy, standard or procedure.

In practice, once a transgression has occurred the following procedure will be followed: (i) When committing his first transgression the employee must be given a written warning; (ii) If the same employee commits another transgression his supervisor must discus the incident with him personally; and (iii) If the same transgression of an information security policy occurs again termination may be considered by the employer. A serious transgression may therefore ultimately result in a dismissal (Du Toit *et al* 2000)

It should be kept in mind that a dismissal will only be justified if the employee is guilty of serious misconduct or repeated offence (Du Toit *et al* 2000). Three important issues pertaining to

the information security domain are embedded in the test to be applied when determining whether or not an employee is guilty of misconduct: (i) There must have been a valid or reasonable rule or standard which the employee contravened; (ii) The employee must have been aware, or could reasonably be expected to have been aware, of the rule or standard - this section emphasises the importance of an effective information security awareness and training program; and (iii) The rule or standard must have been applied consistently by the employer. The enforcement of a policy in a consistent manner is of pivotal importance. If an employer fails to do so and allows a transgression to occur a number of times before acting against it, the employee may use the defense of legitimate expectation. Therefore the employee will state that because of the fact that he was not disciplined the previous three or four times when he committed the same transgression, he had a legitimate expectation that the position would remain the same.

Even the best formulated policy is useless if it is not executed effectively. If policies are written but never implemented, or not followed, not enforced, or enforced but inconsistently it is worse than not having them at all."

The importance of enforcement is illustrated by Federal Sentencing Guidelines that states: "The standards must have been consistently enforced through appropriate disciplinary mechanisms, including as appropriate, discipline of individual responsible for the failure to detect an offence. Adequate discipline of individuals responsible for an offense is a necessary component of enforcement; however, the form of discipline that will be appropriate will be case specific " (Tipton and Kraus 2001).

The provisions of these guidelines are consistent with the Code of Good Practice found in South African Labour law which states that when determining if an employee may be dismissed on the ground of misconduct or non-compliance, one of the factors that must be taken into consideration is whether or not "the rule or standard has been consistently applied by the employer…Strict enforcement of policy and standards must become a way of life in business. Corporate policy making should consider adherence to them a condition of employment. Never adopt a policy unless there is a good prospect that it will be followed. Make protecting the confidentiality, integrity and availability of information 'the law" (Tipton and Kraus 2001).

Furthermore, keep in mind that the two notions of unfair dismissal and unfair discrimination are very tightly bound. Consequently, a well-formulated information security policy may potentially safeguard the company against lawsuits pertaining to, for instance an unfair dismissal or unfair discrimination where the employee's services were terminated because of non-compliance with the information security policy (Du Toit et al 2000).

3.3 Implementing an information security policy within the company

The responsibility for the development and implementation of the information security policy rests with the security team. Because of this, the composition of the security team is of pivotal importance. In the past it was common practice for management to assign the task of development and implementation solely to IT security professionals. This resulted in policies not reflecting legal and/or business aspects and concerns of the company. Furthermore these professionals often lacked the necessary writing skills to create readable, concise and effective written communication (Tipton and Kraus 2002).

The security team's first step would be to establish whether the company has any information security policy in place. If this is the case the security team will have to investigate whether or not the existing policy is aligned with the corporate mission, goals and objectives.

When writing the information security policy the security team must consider five basic questions: (i) What is the intent of the policy? (ii) Who is affected? (roles and responsibilities?) (iii)

Where does the policy apply? (scope?) (iv) When does the policy take effect? ” and (v) Why is it necessary to implement the policy? (Tipton and Kraus 2002).

From a legal perspective it is expected of every company to have at least two policy manuals in place to address the two broad issues, namely: (i) The use of the website; and (ii) The use of communication systems by employees (De Villiers 2003). These two issues may effectively be covered in two umbrella policy manuals, namely (i) Website use policy; and (ii) Communications systems policy.

The website use policy will regulate the use of the company’s website. Therefore, this policy will stipulate how a website user may use the website. This policy will address issues such as: (i) Who may use the website; (ii) How must the website be used; (iii) The liabilities of the website owners; (iv) The protection of the intellectual property rights of the websites; and (v) How disputes will be resolved.

The communication systems policy - This policy may be viewed as a general policy that dictates the overall use of communication systems within the company. The communication system policy may be viewed as the title of a manual which will contain other policies. This policy will be applicable to all employees, regardless of their position or level of employment within the company. This manual will result in subsequent policies being developed and implemented in the following areas: (i) Acceptable Internet usage policy; (ii) Information security; (iii) E-mail policy; (iv) Back-up and recovery policies (Disaster recovery); (v) Remote access policy; (vi) Contingency planning policy; (vii) Virus protection policy; (viii) Encryption policy; (ix) Incident response policy; (x) Wireless/PDAs policies; and (xi) Password policy (Tudor 2001)

3.4 A standard format for information security policies

It is important to establish a definite style/format in which all policies, standards, procedures and guidelines will be written. This will ensure consistency and will effectively rule out the possibility of confusion.

Although it is acknowledged that each company will design and write their procedures, policies, standards and guidelines in a manner that is pertinent to that specific company, the following configuration is considered to be the established format for all major headings and topics within information security policy documents: (i) Background why the policy exists: the importance of security as an enabling mechanism for information sharing; (ii) Scope: who the policy affects and where the policy is required; (iii) Definitions: explanation of terminology; (iv) References where people can look for additional information, eg. more detailed security policies and procedures; (v) Coordinator/policy author: who sponsored the policy, and where do people go to ask questions? (vi) Authorising officer: who authorised the policy? (vii) Effective date: when the policy takes effect; (viii) Review date: when the policy gets reviewed; (x) Policy statement: what must be done; (xi) Exceptions: how exceptions are handled; and (xii) Sanctions: what actions are available to management when a violation is detected.

3.5 Information security acknowledgement forms

From a legal perspective two important aspects still need to be addressed concerning information security policies: first, how to ensure that employees are legally bound to the corporate information security policy, standard, or procedure; and secondly, how to make employees aware of the information security policies, standard, procedure and guidelines.

It is generally required of all newly appointed employees to sign a service contract in which the information security policy will be incorporated. A problem, however, arises when the company has existing employees that did not sign the policy when they were first appointed. The reason for

this being that, for instance such a policy did not exist at the time of their appointment. An effective solution to this problem would be to require of existing employees to sign an information security acknowledgement form before he/she receives any future/further computing assets. By adopting the terms "computing assets" the company does not limit itself to specific applications or programs. Consequently, it may be required of an employee to sign the acknowledgement form regardless of whether he is receiving a new laptop, desktop, software or hardware. It may even be something as small as a network cord (Tudor 2001).

The implementation of the acknowledgement form would entail the following: (i) A summarised version of the information security policy may be developed into a Security Policy Acknowledgement Form; (ii) All new employees are required to read and sign this form upon employment at the company and prior to receiving computing assets; (iii) It is required of existing employees to read and sign this form prior to receiving any new or further computing assets; (iv) It is desirable that the acknowledgement form is signed on a periodical basis to remind the employees of their responsibilities to protect the confidentiality, integrity and availability of the information and processing resources; and (v) The signature may serve as proof that the user has been informed and understands his/her responsibilities (Tudor 2001).

Content of this form would include (i) Defines what the user is to protect; (ii) Scope of resources; (iii) What the employee's responsibility is to protect the resources; and (iv) Acknowledgement statement of the user's understanding.

It is very important that the information security acknowledgement form is reviewed by both the human resource and the legal department of the company in order to ensure that it is in line with existing corporate policies, and will be considered legally binding by a court of law.

4 CONCLUSION

Information security documents will provide the foundation on which any information security initiative in a company must be build. Moreover, information security policies provide directors and members of top management with a mechanism to enforcement information security within the company while simultaneously proving to stakeholders of the company, as well as to the court, where required, that it has taken reasonable steps to secure its information assets, resources and systems.

5 REFERENCES

Beishon "Information security" (last visited 28 August 2005) http://www.iod.com

De Villiers "Website and e-mail policies" (August 2003) *E-Commerce Law 3*

Du Toit et al *Labour Relations Law* (2000)

Employment Equity Act 55 of 1998 section 5, 6(1)

Funnel "Enemies within: the problem of inside attacks" *Computer Fraud & Security* July (2004)

Gamertsfelder, Handelsmann and Sivanesarajah "Under lock and keyboard – prevention of unauthorised use of corporate computer systems" 2001 *New South Wales Society for Computers and the Law Journal* 1.

Jansen "IT policies must be constitutionally sound" (last visited 5 June 2002) http://www.derebus.co.za

Kaleewoun "An overview of corporate computer user policy" (last visited 24 July 2002) http://www. sans.org

Mistry “Developing security policies for protecting corporate assets” (last visited 24 July 2002) http://www.sans.org

Peltier *Information security Policies, Procedures, and Standards* (2002)

Schneier *Secrets and Lies* (2000)

Tipton and Kraus *Information Security Management Handbook* Vol 2 (2001)

Tipton and Kraus *Information Security Management Handbook* Vol 3 (2002)

Tudor *Information Security Architecture: An Integrated Approach* (2001)

Voges “IT needs security partnership with HR” (last visited 20 February 2002) http://www.computingsa.co.za