Towards a framework to guide compliance with IS Security policies and Regulations in a university

Michael Kyobe
Department of Information Systems
University of Cape Town
Cape Town, South Africa

Abstract— **Compliance with computer security policies and legislation is critical to educational institutions today. Universities offer Internet services to users, store personal information of learners, staff, conference and attendees. which exposes them to potential risks and legal liabilities. Failure to ensure compliance with information security laws poses significant financial and reputation risk and may invite serious scrutiny of university activities by law enforcement bodies [24].**

While universities have sought various measures to achieve compliance (e.g. self-regulations, security policies, staff/student handbooks, public relation campaigns, Web and email reminders and audits.), these have had limited success in influencing user behaviours. The rate of electronic abuse and lack of compliance with policies is simply on the rise. The August 2009 EDUCAUSE Review indicates that security remains one of the top strategic issues facing higher education institutions [2]. [20] claims that half of all personal identity breaches occur in higher education. The recording industry and motion picture associations are increasingly holding institutions liable for illegal downloading of copyright materials [11] and students have also been accused of privacy violations [8]. So, what makes compliance with policies and regulations in universities difficult and how can compliance be measured and achieved effectively?

This study examines the factors that influence compliance with security policies and regulations in universities. First, some key regulations governing information security in South Africa are introduced, followed by a review of the security environment and compliance behaviours in universities. A framework aligning regulatory requirements with control standards is developed to guide compliance behaviours in universities.

Keywords-IS security compliance;security regulations & policies, universities, control frameworks)

I. THE REGURATORY ENVIRONMENT

Legal obligations to implement and comply with security measures are set forth in an ever-expanding patchwork of national and international regulations, common law duties and codes of practice. Some of the key laws and regulations are discussed in the present paper and the potential liabilities for non-compliance are indicated.

A. Common law

This is the law developed through decisions of courts rather than through statutes. Prior to the enactment of the Electronic Communications and Transactions Act (2002) in South Africa, common law regulated crimes of defamation, indecency (online child pornography), crimen injuria (also known as cyber-smearing), fraud (cyber fraud), defeating the ends of justice, contempt of court (in the form of publishing any court proceedings without the courts permission online or by other electronic means), and forgery to these cyber offences [22].

At common law, a director owes two duties to the company: A fiduciary duty and a duty of skill and care. A fiduciary is a person who is in a special position of trust. This person has a duty to act in good faith, should exercise his powers for a proper purpose, must avoid conflicts of interest, and should not misuse the organisation's property. Further, a duty of skill and care requires that this person should possess reasonable skills and should devote his full attention to the business of the organization. This duty of care includes responsibility for mitigating risks and protection of the organisation's information assets. [25] state that "it is becoming increasingly evident that a court of law may go behind the 'corporate personality' of the company and find individuals particularly members of management who can be held accountable for the breaches in information security policy". Indeed, following the judgment in the case " Minister of safety & security v Van Duivenboden [2002] 3 All SA 741", an institution may be held liable for the damages caused by its students or staff, if a person in a responsible position would have foreseen the risk and have acted to prevent that risk [26].

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

B. *The Electronic Communications & Transactions (ECT) Act) (2002)*

The ECT Act of 2002 is a wide legislation dealing with any form of electronic communication (e.g. by email, the internet or SMS) and other issues relating to cyber inspectors, service provider liability and prevention of information resource abuse [13]. According to [13] one does not have to comply with the entire Act but with sections relating to incorporation by reference; electronic signatures; electronic evidence; production of information; record retention; automated transactions; website architecture and content; contract formation; cryptography service providers; secure payment systems; SPAM and protection of critical data.

The problems relating to cyber crime are addressed by the cyber crime section in Chapter XIII of the ECT Act, 2002. According to [13], this chapter introduces statutory criminal offenses relating to unauthorized access to data (e.g., through hacking), interception of data (e.g., tapping into data flows or denial of service attacks), interference with data (e.g., viruses) and computer related extortions, fraud and forgery. They also state that a person aiding those involved in these crimes will be guilty as an accessory. A person convicted of an offence related to the above is liable to a fine or imprisonment for a period not exceeding five years.

Universities are increasingly engaged in e-business and e-commerce with (e.g., external suppliers) and also with e-learning which means this regulation applies to them. The legislation dealing with service provider liability has implications for educational institutions providing internet access and information storage facilities for staff and students. While these institutions do not operate like businesses charging for internet services, they do provide internet and network services and therefore are obliged to meet the legal requirements that prohibit electronic abuse, illegal download of material and copyright infringement.

C. *Protection of Personal Informations*

Organisations like universities that collect and process personal information are referred to as data controllers and have to comply with the following nine principles: The Act requires that they obtain express written permission from data subjects for collection, processing, disclosure of their information; Information may not be requested or collected for unlawful purpose; Data controller must disclose in writing to data subject specific purpose for which personal information is being collected; Data controller may not use the personal information for a purpose other than the disclosed purpose, unless written consent is obtained; Record of the personal information and purpose for which it was collected, to be kept by the Data controller for the period of use and for a period of at least one year thereafter; Data controller may not disclose personal information to a third party unless specifically authorised to do so in writing by the data subject or required or permitted by law; Data controller must for as long as the personal information is in use and for a period of at least one year thereafter, keep record of any third party to whom the personal information was disclosed and the date on which and the purpose for which it was disclosed; Obsolete personal information must be deleted; Party controlling personal information may use personal information to compile profiles for statistical purposes – provided that specific data cannot be linked to specific data subject. With regard to critical databases, the State may declare certain databases critical in the interests of national security or "the economic and social well-being" of South Africans. Once declared, the controller of such database is required to disclose certain information about the database and conform to database management standards stipulated by the State. Non-compliance with the provisions of this Act may result in criminal fines and award of civil damages [12].

This Act makes its imperative for universities to take necessary precautions in the way they handle and disclose personal information about students and staff. They have to ensure permissible uses and disclosure of information and consent from information owners need to be obtained in a manner that supports validity. It is also necessary that institutions put in place a clear process for authorising permissible disclosure. Some of these requirements are also prescribed in the Health Insurance Portability and Accountability Act (HIPAA) discussed below.

D. *HIPAA (The Healthcare Information Portability & Accountability Act*

This Act mandates that healthcare information become "portable" and "available". Title II, Subtitle F, seeks to force uniform standards in electronic interchange, security and privacy of information whether in transit or stored. HIPAA generally requires covered entities to (i) adopt written policy procedures that describe, among other things, who has access to protected information, how such information will be used, and when the information may be disclosed; (ii) require their business associates to protect the privacy of health information; (iii) train their employees in their privacy policies and procedures; (iv) take steps to protect against unauthorised disclosure of personal health records; and (v) designate an individual to be responsible for ensuring the procedures are followed. Educational institutions are obligated to comply with HIPAA.

E. *Protection of Personal Informations*

Promotion of Access to Information Act 2, 2000 (PAIA) This legislation was passed in order to comply with the obligations contained in section 9 (4) and section 32 (2) of the South African Constitution. Section 32 of the constitution of 1996 states that "everyone has he right of access to (a) any information held by the state or any of its organs … in so far as such information is required for the exercise o protection of any of his or rights" [3]. In terms of Sections 14 and 51 of the PAIA, public and private bodies are required to compile a manual that details the subjects and categories of information held by that public/private body and the procedure that should be adopted in requesting access to the records. Section 14(1)(d) of the Act allows access to the following records: Governance records (Council, Senate, Institutional Forum, SRC,

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

Convocation and university Committees); Records of individual students; Human Resources records (individual staff members, staff recruitment and other staff related policies); Research records (undertaken by staff and/or students); Financial Records (budgets, financial statements, assets register, procurement policies). The Higher Education Act (Act 101 of 1997) as amended also states in Chapter 7 (section 56(1), that any person may inspect the register of Higher Education, and auditors' reports. This emphasises again the need to ensure that information kept by universities is compiled accurately and stored safely and while there are some exemptions that apply in certain circumstances, it is prudent to work on the assumption that all records are accessible.

F. Regulation on Interception of communication related information Act 70, 2002

This Act provides in section 2 that 'no person may intentionally intercept or attempt to intercept, or authorise or procure any other person to intercept or attempt to intercept, at any place in the Republic, any communication in the course of its currency or transmission, subject to certain exceptions; An employer may monitor or intercept an employee's communication if the employee harbours illegitimate expectation of privacy in respect of that communication and also if the employee's expectation of privacy in relation to such communications is unreasonable. (Cases : Bernstein v Bester 1996 (4) BCLR449 (CC) Protea Technology Ltd v Wainer 1997 (9) BCLR 1225 (W)

G. King III

King III Identified several characteristics of good Corporate Governance e.g., Discipline, transparency, independence, accountability, responsibility, fairness and social responsibility. It addresses the accountability and responsibilities of boards, directors and the processes of auditing and accounting. Chapter 4, principle 4.16 addresses IT governance issues. According to this section, the board is required to operate with IT governance in mind; IT should be on the board agenda; IT performance should be measured and reported to the board; the board should set a management framework for IT governance based on common approach such as COBIT; and audit committees should oversee IT risks and controls.

H. FICA

Financial Intelligence Centre Act - provides that an accountable institution, may not conclude a business transaction with a client, nor may we establish an ongoing business relationship with a client, without having complied with information gathering and reporting duties imposed by FICA. These obligations include: Proof of identity; Proof of residential address; and Proof of banking account. Universities are increasingly involved in e-business, e-commerce (e.g., with suppliers through e-procurement) and e-learning. They therefore need to abide by the requirements of FICA.

II. INFORMATION SECURITY IN UNIVERSITIES

The need to protect information in universities and the implications of non-compliance with the above regulations are increasingly acknowledged by institutions of learning as evidenced by the number of self-regulations, security policies, staff/student handbooks and audits. However, even with these measures in place, institutions fail to comply and security abuse persists. The author examines some of these challenges and the theoretical concepts explaining non-compliance behaviours in these institutions.

In their theory of Social Information Processing, [18] argue that the context and consequences of past choices influence people's attitudes and perceptions. They claim that since humans are adaptive organisms, they tend to display those behaviours and beliefs that are in alignment with their social context. The academia community sees itself as a community of scholars and researchers and as such engage in those activities that contribute or promote knowledge development and sharing. Students and academics for instance engage in collaborative and explorative activities through social networking. Research is traditionally guided by the values of tolerance, individual autonomy and experimentation. While these values contribute to the development of learning and knowledge, they paradoxically conflict with the development of a security culture and make compliance challenging. Further, in their quest for knowledge and its dissemination, institutions have developed high bandwidth links to the internet, and in many cases allow a disparate mix of technologies to be used on their networks. They also collect personal information and data from internal users and external partners such as alumni, research partners, donors, conference attendees. Consequently, this increases their exposure to large targeted cyber-attacks (from internal and external sources); identify theft; and legal liabilities.

[5] on page 3 argue that specific climates in organisations are predictive of specific outcomes. Following Campbell et al., (1970), they define organisational climate as the perceptions of organisational policies, practices and procedures both formal and informal and distinguish it from organisational culture which refers to the beliefs, values and assumptions held by members, found in the deep structure of organizations. They maintain that these perceptions mediate 'the relationship between objective characteristics of working conditions (organizational policies, practices, and procedures) and individual's working behavior".

Policies and regulations on security are often perceived in academia to be major impediments to academic freedom (i.e., the right to pursue controversial topics, ideas, lines of research), which is essential for learning and pursuit of knowledge [5]. [10] observed that the desire for free and unfettered exchange of information across organisational boundaries is a major cause of poor information protection in universities.

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

The Protection Motivation Theory (PMT) also proposes that protection from fear stems from two appraisals: threat appraisals (i.e., an assessment of the severity of a threatening event and the perceived probability of the occurrence of the event (vulnerability)) and coping appraisal. Coping appraisal is determined by (i) the efficacy of the recommended preventive behavior (i.e., the individual's expectancy that carrying out recommendations can remove the threat) and (ii) Self-efficacy (i.e., the belief in one's ability to execute the recommended courses of action successfully) [16] and [4]. According to Rogers, information about a threat causes a cognitive mediating process in individuals that appraises maladaptive (e.g., non-compliance behaviour) or adaptive responses (compliance behaviour).

[10] states that security challenges may arise in universities due to incorrect perceptions of the university community. For instance, they may not understand the severity of the risks and its implications to the stakeholders due to a lack of awareness; they may believe that the threats are unrealistic; they may think that someone in another building is taking care of the security problem for them (and as such they need not bother about it). [14] also share a similar view. They observed that people are not security compliant because of security illusions (i.e., they fail to apply security measures because they believe that others are acting in a manner conducive to security requirements, when in reality they are not). In his study of compliance with security requirements, [9] found a significant gap between desired and actual awareness of information security risks across the university community. His findings attributed this to the intangibility of security and the low perception of threat level by the university community. He states further that "this in turn impacted a broad number of other issues including work practices, allocation of resources and funding, prioritization of security, acceptance of the reality of risk, development of clearly written and communicated policy and general compliance with security". [19] also observed that those whose understanding of information systems is limited to the communication functionality fail to focus on the risks and consequences of system damage. He argues further that decision makers who perceive security risks to be minimal will be less likely to devote resources to address those risks. Sometimes ineffective coping strategies are adopted because of limited understanding of how to deal with situations. For instance, [1] observed that, faced by the growing legal obligations and regulatory requirements for their institutional departments (e.g., research facilities and medical services), many universities have responded by adopting disintegrated and piecemeal approaches to compliance resulting in incomplete, redundant and expensive efforts.

[1] argues further that such piecemeal approach may also undermine the integration of information security compliance into other institutional compliance programs, such as information privacy and institutional governance.

The aim of behavioral aspects of security governance is to ensure that employees show conformity with rules and policies set by management. According to [7], an agency relationship exists whenever one party (principal) entrusts some decision making authority to another party (agent). This theory assumes that agents incur personal costs as they devote their time, knowledge and effort, to the firm; and given an opportunity they can retract the level of effort, skill, and knowledge they provide. [7] state further that in organisational information security, responsibility of whether to adhere to organisational security policies or ignore them is delegated to employees. Employees may choose to break security policies for malicious purposes or choose to evade them for mere convenience. Abuse of privacy by students on social networks, bullying, spread of malicious code and gossip are well documented [8]. There are also recent findings suggesting that higher level of information security may be counter productive since it restricts employees' ability to follow flexible operation routines [7].

Summary

The discussion above reveals a number of issues facing universities in their effort to ensure compliance with security laws and regulations. The nature and tradition of these institutions makes it difficult to introduce necessary changes. It is also clear that the challenges in the implementation of security and compliance are not only experienced at user levels (e.g., staff and students), but also at senior management levels in their planning processes. Finally, there appears to be limited effort to facilitate the development of a security culture. This could be attributed to the problems above but also to a lack of proper awareness of the laws and the difficulties involved in measuring compliance. Further there is also a lack of knowledge of the liabilities involved and limited security training. In the following section, the author proposes a framework universities can use to address some of these issues and ensure compliance.

III. TOWARDS A FRAMEWORK TO GUIDE COMPLIANCE WITH SECURITY REGULATIONS IN UNIVERSITIES

Although the laws and regulations noted above prescribe compliance requirements, they rarely specify or provide specific directions on how the information security procedures may be established to achieve compliance. [1] states that the lack of hard-and-fast rules regarding which specific information security measures an institution should implement to satisfy its legal obligations has also puzzled many lawyers and compliance officers. [6] also concur and argue further that organisations need to ensure accountability, transparency and measurability if they are to demonstrate compliance effectively. Measures or metrics in particular promote visibility, informed decision making, predictability, proactive planning and help avert surprises [17].

Many of the recent statutes, regulations and court cases demonstrate regulatory requirements for security that closely resemble established information security standards (e.g. NIST 800-63, ISO 17799, Cobit v4, ITIL [1]. It has therefore been recommended that compliance can be enhanced by the alignment of the regulatory requirements with these control standards and identification of appropriate metrics for these controls. Since many of the laws suggest similar security risk analysis and management practices, [1] proposes a unified

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

approach to information security compliance whereby desired security practices (security safeguards) are mapped to appropriate the laws and regulations. In the current paper, this idea is taken further by suggesting the metrics that could be used to measure or implement compliance.

In the following framework, the researcher therefore identifies good control practices recommended by standards and codes of practice. These are then mapped to the information security laws and regulations discussed in the previous section, indicating their applicability with a cross. An indication is also provided of the critical security and compliance areas identified in the previous section that need to be address in a university. Some examples of the metrics that could be used to measure compliance are presented in the last column.

TABLE I. A FRAMEWORK TO GUIDE COMPLIANCE WITH INFORMATION SECURITY IN UNIVERSITIES

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

A framework to guide information security compliance in Universities										
Security practices needed to comply with regulatory requirements	Regulations complied with by security practices (***indicated by a cross (X)***) 1=ECT Act; 2=Protection of personal info; 3=HIPAA; 4=Protection of Access to info; 5=RICI; 6=King III; 7=FICA; 8 = Common Law; 9=Higher Education Act.									Some examples of compliance measures/Metrics
	1	2	3	4	5	6	7	8	9	
Security planning, responsibilities & monitoring: Planning for security ;risk analysis, periodic reviews; Assignment of security responsibilities; Appointment of protection/compliance officer; Ensuring trustworthy people are appointed to manage security; observing duty of care and responsibility for risk mitigation; IT governance; Tracking of documents; report incidents to authorities; Notification of unauthorised use/disclosure of info.	X	X	X	X	X	X		X		Appropriateness of the approach adopted to ensure security/compliance *- use of inappropriate approaches indicate poor planning;* Frequency of audit/reviews. *- Failure to conduct regular reviews suggest poor monitoring;* % of authorised users / total number of users accessing the system *- indicates how many unauthorised users are on the system;* Existence of up-to-date policies on appointments; *- indicates whether policies are revised*
Management of users and systems personnel: staff & student authorisation done; supervision of IT system users; communication & authentication of users Rights to access information allocated	X			X					X	% of unauthorised access to systems/total access rights granted; % of users identified on the system / number authorised; % of rightful users denied access to information/system.
Management of data security/integrity: Prevention of interception of data, interference with data, fraud (information integrity); Compile a manual detailing the subjects and categories of information held and the procedure to access it.	X	X	X	X	X					% of unauthorised access to information; Existence of procedures to follow when requesting, accessing or disclosing information; % of mobile devices operating in approved area; % of incidents of data interceptions/interference per month.
Contingency planning & maintenance: Existence of a data backup plan, disaster recovery plan; critical analysis of applications and data; maintenance of systems.	X	X	X					X		% of information systems that have conducted annual contingency plan
Security awareness and training: (e.g., Provision of security reminders, training on : malicious software protection, log-in monitoring and password management)			X			X				% IS security personnel trained within the past year / total number of security personnel; % of IT budget devoted to training
Retention of electronic records: Securing proper evidentiary weight of electronic evidence Media protection, sanitize or destroy information system media before disposal	x	X								% of media that passes sanitization procedure testing / total number of media tested
Accuracy of the Website & transaction information: Ensuring accuracy of websites & transactions; certification & accreditation of information	X	X	X				X			% of web pages with false/dated information / total number of pages *- indicates accuracy of information presented on the website*

IV. CONCLUSION

Compliance with information security policies and regulations continue to be a major challenge for universities.

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

This paper examined factors influencing compliance and some of the theoretical foundations that explain this problem. Major influencing factors identified include the nature and tradition of universities, poor planning and implementation of security compliance, lack of security awareness and knowledge of security risks. Compliance can be enhanced through the alignment of regulatory requirements with existing security controls or practices. A framework for such alignment and also to guide compliance behaviours of system users in universities is presented above. Examples of some of the metrics that can be used to measure the extent of compliance are also provided..

V. REFERENCES

[1] P. Alder (2006). A Unified Approach to Information Security Compliance. *EDUCAUSE Review,* 41(5) (September/October 2006): 46–61. [Online]. Available: http://www.educause.edu/EDUCAUSE+Review/EDUCAUSEReviewMagazineVolume41/AUnifiedApproachtoInformationS/158087

[2] C.S. Agee and C. Yang. (2009). Top-Ten IT Issues, EDUCAUSE Review, 44(4) July/August 2009). [Online]. Available: http://www.educause.edu/2009IssuesResources

[3] A. Arko-Cobbah, (2008). The right of Access to Information: opportunities and challenges for civil society and good governance in South Africa. IFLA Journal, [Online]. Available: http://ifl.sagepub.com

[4] A. Bandura (1977). *Social learning theory*. Englewood Cliffs, NJ: Prentice Hall.

[5] M. Chan, M. Woon and A. Kankanhalli (2005). Perceptions of information security at the workplace; linking information security climate to complaint behaviour. Journal of information privacy and security 1(3): 18-41.

[6] Gartner Group (2006) How dragon DSCC Addresses Regulatory Compliance Requirements. Enterasys Networks (2006). [Online]. Available:

www.enterasys.com/company/literature/dragon-compliance-wp.pdf

[7] T. Herath and H. Rao. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness . Decision Support Systems. 47(2): 154-165

[8] H. Jones and J. Soltren. (2005). Facebook: Threats to Privacy. [Online]. Available WWW: http://www.swiss.ai.mit.edu/6095/student-papers/fall05-papers/facebook.pdf.

[9] T. Lane. (2007). Information security management in Australian Universities: An exploratory analysis. [Online]. Available: http://eprints.qut.edu.au/16486/

[10] J. McCoy. (2005). Are we ready for a Chief Information Security Officer? [Online]. Available: http://www.docstoc.com/docs/18364711/Are-We-Ready-for-a-Chief-Information-Security-Officer/

[11] J.R. McFadden and D. Saiki, (2005). *Journal of family and consumer sciences*, American Assoc. of Family & Consumer Sciences, Alexandria, USA, 2005, *97*(*3*), pp.75-77.

[12] L. Michalson, 2009. Protection of Personal Information Bill - the implications for you. Retrieved December, 02, 2009, from http://www.michalsons.com/protection-of-personal-information-bill-the-implications-for-you/3041

[13] L. Michalson and B.Hughes.(2005). Guide to the ECT Act, *Michalsons Attorneys*. [Online]. Available: http://www.michalson.com

[14] K.D. Mitnick and W.L. Simon (2002). The art of deception: Controlling the human element of security. Wiley Publishing, Inc

[15] D.G. Oblinger and B. L. Hawkins (2006). The myth about IT security. *EDUCAUSE Review,* 41(3) (May/June 2006): 14–15. [Online]. Available: http://www.educause.edu/EDUCAUSE+Review/EDUCAUSEReviewMagazineVolume41/TheMythaboutITSecurity/158061

[16] C.L. Rogers (1997). Introduction. In *A field guide for science writers*, edited by D. Blum and M. Knudson,

213-16. New York: Oxford University Press

[17] S.E. Schimkowitsch (2009). Key Components of an Information Security Metric Program Plan. [Online]. Available: http://webcache.googleusercontent.com/search?q=cache%3AJo1zW7IuX3AJ%3Ahttps%3A%2F%2Fscholarsbank.uoregon.edu%2Fxmlui%2Fbitstream%2Fhandle%2F1794%2F9479%2FSchimkowitsch-2009.pdf%3Fsequence%3D1+schimkowitsch%2C+2009%2C+Herrmann%2C+2007%2C+metrics&hl=en&gl=za

[18] G. R. Salancik and J. Pfeffer**.** (1978). "A social information processing approach to job attitudes and task design." Administrative Science Quarterly, 23 (1978):

[19] N. Tribbensee. (2003) Liability for negligent security: Implications for policy and practice. [Online]. Available: http://net.educause.edu/ir/library/pdf/ERM0354.pdf.

[20] R. Schad (2008). How secure is Higher Ed? Campus Technology, Focus. [Online]. Available: http://www.oracle.com/us/industries/045694.pdf

[21] J. Shepherd, (31 October 2008). "Universities review plagiarism policies to catch Facebook cheats", *Guardian.co.uk*.[Online] Available: http://www.guardian.co.uk/education/2008/oct/31/facebook-cheating-plagiarism-cambridge-varsity-wikipedia

[22] S.S. Sizwe. (2009) Cyber crime in South Africa – Hacking, cracking, and other unlawful online activities. Journal of Information, Law and Technology. [Online]. Available: http:www.thefreelibrary.com/cyber+crime+in+South+Africa+hacking,+cracking+and+other+unlawful+…-A0206342917

[23] South African schools Act No. 84, 1996. Government gazette, Vol. 396, No. 18900, 15 May 1998

http://www.polity.org.za/polity/govdocs/notices/1998/not98-0776.html

[24] L. Steinfeld, and K, S. Archuleta. (2006). Privacy Protection and Compliance in Higher Education: The Role of the CPO. *EDUCAUSE Review,* 41(5) (September/October 2006): 62–71

[25] K.Thormson, and R. Von Solms, R. (2002).Corporate governance: Information security the weakest link. Available: sa.cs.up.ac.za/issa/2002/proceedings/A007.pdf

[26] K. Van Tonder, (2005). Securing third party data assets: Organisational liability. Elc 2005, [Online]. Available: http://elc.co.za/article.php?subaction=showfull&id=1052909562&archive=&start_from=&ucat=1&