A framework for assessing information systems security practices in libraries

Roesnita Ismail[1] and A.N. Zainab[2]
[1]Faculty of Science & Technology, Islamic Science University Malaysia,
Bandar Baru Nilai, 78000 Nilai, Negeri Sembilan, MALAYSIA
[2]Library and Information Unit,
Faculty of Computer Science & Information Technology,
University of Malaya, 50603 Kuala Lumpur, MALAYSIA
e-mail: roesnita@yahoo.com; zainab@um.edu.my

ABSTRACT

Security of information systems is vital in any library regardless of its type and size. If the critical library's resources such as online catalogs, online databases and websites are interrupted and unavailable to its end users, the impact might affect the library's mission as an information provider thus impeding the library and its end users' performance. In order to protect the information systems, many libraries have implemented necessary security control. This paper gives an overview of a suggested framework for assessing information systems security practices in libraries. A brief description of the framework and a more detailed overview on the five steps to be evaluated in the framework are highlighted. An implementation index as well as a scoring tool that may be used to assist the assessment of information systems safeguarding measures in a library are also presented.

Keywords: Information sytems; Information systems security; Security practices; Technological measures; Organisational measures; Countermeasures; Framework; Libraries.

INTRODUCTION

Information systems (IS) are often used to support operations, work, management and services in organisations. IS security is viewed as the need to protect one or more aspects of IS elements such as hardware, software, physical environment, data and people. Thus, a sound IS security practice depends upon effective information security solutions, which encompass the technical and the non-technical safeguards to minimise vulnerabilities associated with a variety of threats (Westby and Allen, 2007; Scarfone, et. al., 2008, and Gupta and Sharman, 2009). This answers why many organisations have invested millions in securing their IT infrastructures in various forms of physical, personnel and administrative defenses to reduce the frequency and severity of computer security-related losses (Guttman and Roback, 1995).

In the current library environment, IS are widely used to provide digitally delivered services and collections to local and remote patrons. Connecting a library to the outside world via the Internet has changed the risks associated and the controls used to secure the IS. Therefore, it is vital to be worried about IS security because much of the value of a library's main business or services is concentrated in the value of its information systems. As highlighted by Newby (2002), information systems are like buildings, simply creating them is not enough; they need consistent maintenance in order to avoid inevitable decay due to interactions with the environment.

However, not much is known on the actual scenario of IS security practices specifically within the library setting. No academic security studies had been conducted specific to this area and similar searches of journals and the Internet substantiated this finding. Thus, one could not assert whether the library sector is lacking or adequate in IS security. As highlighted by Newby (2002), IS security is often under-appreciated in libraries and this is rather surprising since information is the library's main business. Therefore, we attempt to propose a framework for assessing the current IS security practices developed by Malaysian academic libraries in managing their IS security. This framework is designed to be a tool to guide and encourage libraries to adopt the best practices for IS security measures. It represents a roadmap for the implementation, evaluation and improvement of IS security practices for a library to adopt.

THE PROPOSED FRAMEWORK

The proposed components in the assessment of the IS security measures in libraries are pictured in a staircase model (Figure 1.1). The model is adapted from the Organisational Information Security Staircase Model developed by Hagen, Albrechtsen and Hovden (2008). The model shows that the relationship between organisational and technological measures resembles a staircase. This indicates that in order for IS security measures to become effective, security should be built like a staircase combining several measures in order to produce any effect and these measures are mutually dependent on each step (Sundt, 2006; Berghel, 2005). These combined measures are formulated based on Von Solms (2000) suggestion which indicated that "the basis of information security should include organisational aspects, legal aspects, institutionalisation, applications of best practices and security technologies".

The steps in the staircase follow a logical order so as to achieve the three primary goals of a good security system practice, which are to ensure and protect the confidentiality, integrity and availability of a library IS (Eisenberg and Lawthers, 2005). These three objectives have guided the development of security measures to avoid different security threats in libraries. In this context, the library IS security refers to the means and ways a library protects the information processed by an IS and of the IS itself, to only authorised users (confidentiality), protected against unauthorised changes (integrity) and IS are always available and usable (availability) whenever it is needed.

This model consists of five components (Figure 1): the technological security foundation; information security policy; procedures and control; administrative tools and methods; and awareness creation. It highlights that the higher the position on the staircase, the more effective is the state of IS security management in a library (Hagen, Albrechtsen and Hovden, 2008). The first staircase illustrates that in any security environment including a library, the technological foundation must always be in place. Next, the security policies must be the foundation to develop rules, guidelines and plans. The third staircase illustrates that the IS security procedures must be in place to develop appropriate tools and methods. When these formal systems are implemented, the library can deal with the human elements of information security such as the staff and patrons of the libraries who give life to the administrative security routines by applying them in their day to day activity. The final step involves raising awareness and educating everyone who is using the library IS as users and this represent the most important part in any security initiatives. The details of these components are explained in the sections below.

TECHNOLOGICAL MEASURES: STEP 1

Technical security mechanisms are used to guard the library IS integrity, confidentiality, and availability. These include the mechanisms that are put in place to protect, control and monitor information access as well as prevent unauthorised access to data that is transmitted over a library system. This staircase is constructed based on the assumption that a technological foundation must always be in place in any security IS environment and treated as the main defensive system to any organisation especially in a library setting. Even though Hagen, Albrechtsen and Hovden (2008) did not specify any security measures in their model, they strongly argued that without technological security solutions, there would be no need for administrative measures since it is the technological solutions which prevent, detect and react to virus and spam attacks faced by most organisations (Hagen, 2007). Moreover, there is evidence that many research on traditional information security has been dedicated to technological aspects since security technologies form the basis of a security system (Siponen and Oinas-Kukkonen, 2007). Thus, at this level, we have included technological security foundation which a library should have in order to protect its hardware workstations, servers, hardware, software, data, network and its physical facilities and environment (Appendix 1).

a) Hardware Security

A library IS consists of several hardware equipment such as telephone lines, input/output ports, modems, network cablings, scanners, printers and storage media. These equipment need to be secured from any threats including thefts, power faults, equipment incompatibilities and careless damage. In order to prevent these attacks from causing serious damage to the availability, confidentiality and integrity of data, a library should incorporate several basic measures as suggested by Yeh and Chang (2007) and INTOSAI (1995) as shown in Appendix 1.

b) Software Security

Flaws and risks related to the library software are more likely to be found when services such as OPACs, online databases and resources are made accessible via the Internet. The scope of software security in libraries should encompass several ways in protecting the software components from cracks and assuring the library IS confidentiality, availability and integrity as highlighted by Eisenberg and Lawthers (2005), Yeh, and Chang (2007) and Newby (2002) as shown in Appendix 1.

c) Workstation Security

As more libraries make available to their patrons Internet-connected computers, there is a need to create secure public access to each individual computer from any security threats from the Internet as well as threats from the users. The most common security threats from the Internet include virus and worms. Whereas the security threats from dishonest users might include access to child pornography sites, harassment, identity theft and hacking. Eisenberg and Lawthers (2005) and INTOSAI (1995) suggest several security measures in order to create a secure public access workstation in a library as shown in Appendix 1.

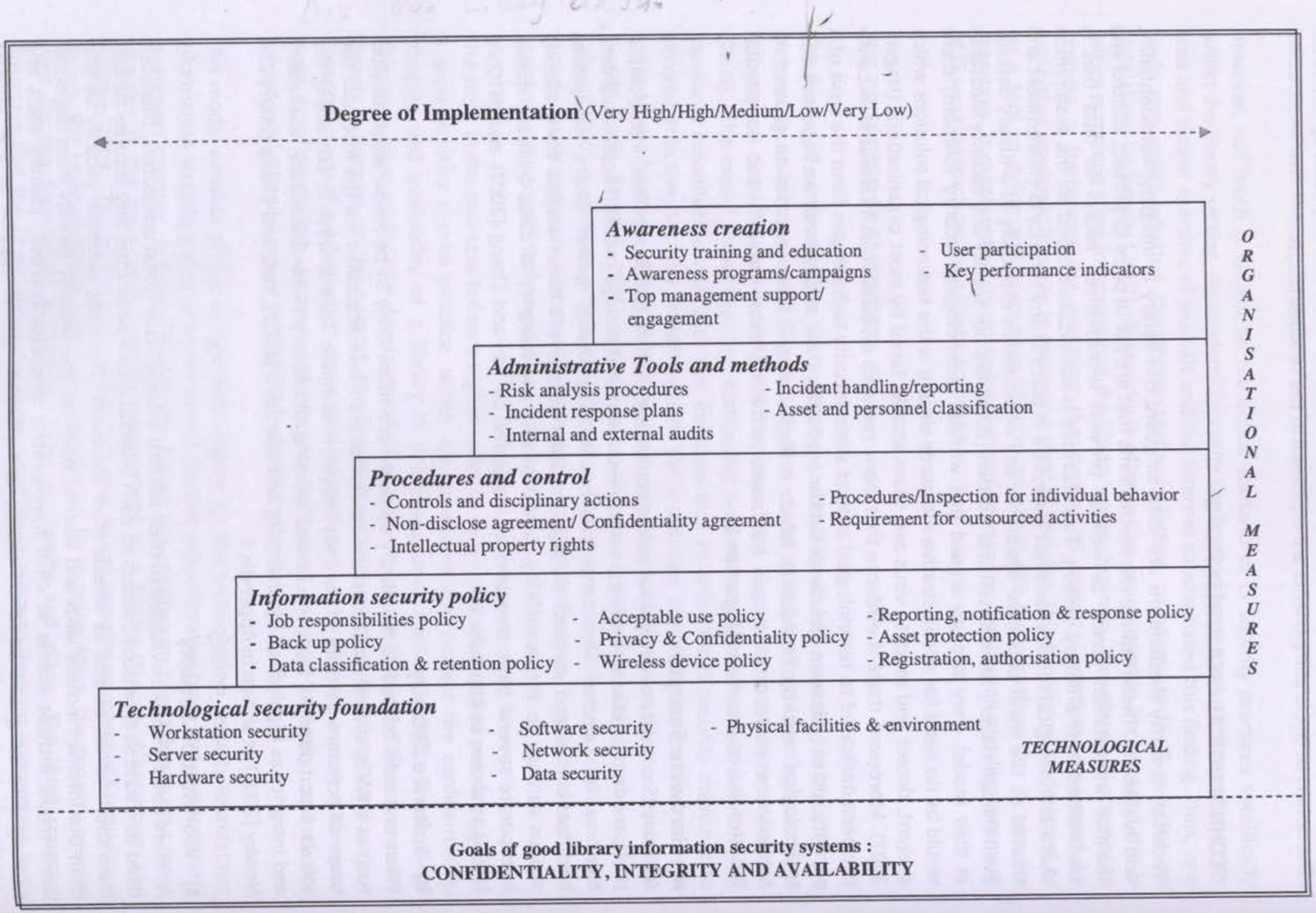
Degree of Implementation (Very High/High/Medium/Low/Very Low)
Awareness creation
- Security training and education
- Awareness programs/campaigns
- Top management support/ engagement
- User participation
- Key performance indicators
Administrative Tools and methods
- Risk analysis procedures
- Incident response plans
- Internal and external audits
- Incident handling/reporting
- Asset and personnel classification
Procedures and control
- Controls and disciplinary actions
- Non-disclose agreement/ Confidentiality agreement
- Intellectual property rights
- Procedures/Inspection for individual behavior
- Requirement for outsourced activities
Information security policy
- Job responsibilities policy
- Back up policy
- Data classification & retention policy
- Acceptable use policy
- Privacy & Confidentiality policy
- Wireless device policy
- Reporting, notification & response policy
- Asset protection policy
- Registration, authorisation policy
Technological security foundation
- Workstation security
- Server security
- Hardware security
- Software security
- Network security
- Data security
- Physical facilities & environment
TECHNOLOGICAL MEASURES
ORGANISATIONAL MEASURES
Goals of good library information security systems :
CONFIDENTIALITY, INTEGRITY AND AVAILABILITY

Figure 1: Organisational Information Security Staircase Model (Adapted from Hagen, Albrechtsen and Hovden, 2008)

d) Network Security

Good network security protects the network in a manner that is consistent with its purpose and secures it from adware, spyware or network intruders. The network security for a library would need to allow access to the IS for authorised remote users, while simultaneously ensuring that full access to the Internet is always available to its internal users. In this model, we included several network security measures as indicated by Eisenberg and Lawthers (2005), and Yeh and Chang, (2007) as shown in Appendix 1.

e) Server Security

In a library's network, servers play a vital role in providing access to key library services such as online databases, online catalogs and circulation systems to internal and remote patrons. The term 'server' often refers to the computer hardware, the operating system and applications loaded on the hardware. Server applications are the software programs loaded over a server's operating system enabling the server to perform specific functions such as acting as a web server or email server (Eisenberg and Lawthers, 2005). The web servers and email servers are complex and are the most appealing targets to attackers. It is therefore important that libraries take steps to secure the email and web server applications from any intrusion, hardware and application failure due to viruses, hackers or natural disasters. The availability, confidentiality and integrity of the library server can be assured via proper implementation of specific counter measures as suggested by Eisenberg and Lawthers (2005) as shown in Appendix 1.

f) Data Security

Since a library stores, processes and provides access to vast amounts of data, it will definitely require a sound data management to assure the security of its data. Data security is about keeping and ensuring data against accidental loss, unauthorised modifications or unauthorised access by taking appropriate measures. Yeh and Chang (2007), Thiagarajan (2003), and Powell and Gillet (1997) listed several physical measures that should be in place in a library so that confidentiality, privacy, availability and integrity of its data could be maintained (Appendix 1).

g) Physical Facilities and Environmental Security

The term physical and environmental security refers to measures taken to protect the library systems, buildings and related supporting infrastructures or resources (including air conditioning, power supply, water supply and lighting) against physical damaged associated with their physical environment such as fire, flood and physical intrusion (INTOSAI, 1995; and Yeh and Chang, 2007) as shown in Appendix 1.

ORGANISATIONAL MEASURES: STEP 2 TO STEP 5

Many propositions have been made about people or human failures as the weakest link for information security and not the technical vulnerabilities (AlAboodi, 2006; Yeh and Chang, 2007; Ernst & Young, 2008). This suggests that investments for information security in any organisations must not be on the technology alone but there must also be a focus on training and awareness programs (Ernst & Young, 2008). This model has included organisational security measure which comprises of four sequential steps; the presence of security policies, procedures and controls, the non-technological tools, and the creation and maintenance of security awareness (Hagen, Albrechtsen and Hovden, 2008).

a) Information Security Policy: Step 2

Information security policy forms the basis of every administrative security regime (Hagen, Albrechtsen and Hovden, 2008). It primarily informs users of the requirements for protecting various assets including people, hardware, software and data. It specifies the strategies behind an organisation's information security approach through a written document directly linked to the overall security strategy of the library (Hone and Elloff, 2002; Doherty and Fulford, 2006). In libraries, the security policy will have some areas of overlap with the acceptable use policy. An acceptable use policy is generally focused on patron use of the library information systems, whereas a security policy is developed as an administrative guide which includes rules and guidelines for all access and use of information systems (Williams, 2001). A security policy is needed in a library because they provide continuity, consistency and a basis for enforcing staff and patron conduct on using the library IS (Williams, 2001). In order to be more practical and implementable, policies must be further defined by standards, guidelines and procedures (Weise and Martin, 2001).

b) Procedures and Controls: Step 3

Administrative procedures and controls are vital in a library IS security practices. Procedures are the step-by-step instructions on how to implement and enforce policies in the organisation (Conklin et. al., 2004). Procedures and controls are directly derived from the security policy through work processes and procedures. They are as equally important as policies since they outline how to protect the resources. For example, a Password Policy would outline password construction rules, rules on how to protect the passwords and how often to exchange them. In contrast, the Password Management Procedures would draft the process to create new passwords, distribute them as well as the process for ensuring the passwords have changed on critical devices (Guel, 2007). Thus, this step consists of documents guiding individuals and organisational behaviour which includes user instructions, security plans, non-disclosure agreements and follow-up activities of the documented systems.

c) Administrative Tools and Methods: Step 4

Administrative tools and methods are both proactive and reactive means in ensuring the security of IS in a library which includes presence of asset classification, risk analysis, audits and incident reporting systems.

d) Awareness Creation: Step 5

Security awareness is the process of making people understand the importance of security, the use of security measures, the implications of security on their ability to perform their jobs and the process of reporting security violations (Pipkin, 2000). Studies and surveys repeatedly show that the human factor is the biggest threat to IS and assets. Ironically, the human factor is also the best way to prevent loss. Therefore, security awareness programs are critical to any security design as lack of awareness can lead to a variety of security issues. This implies that awareness creation can be placed at the top of the staircase.

IMPLEMENTATION INDEX

The sequence of steps proposed in this model illustrates the ideal sequence of combined security measures for the library IS.

Table 1: Level of ISM Implementation Measures
(Source: Information-Technology Promotion Agency. 2008)

Level	Ranking	Description of the attributes of information system security process
1	Not Implemented	No security measure has been established
2	↓	Only some part of security measure has been implemented
3		Implemented but the stage has not been reviewed
4	Fully Implemented	Implemented and the state reviewed on regular basis.
5		Implemented enough to be recognised as good example for others libraries

However, there are possibilities that some measures might be widely implemented than the others. Thus, the implementation index based on the Information Security Measure Benchmark (Information-Technology Promotion Agency, 2008) is used to assess which measures or steps are widely implemented and which measure or step is least implemented in each library. For each measure or variable, the implementation index is measured based on the five levels implementation score (1 = Not Implemented to 5 = Fully Implemented) that reflect the degree of maturity as indicated in Table 1.

ASSESSMENT TOOL AND SCORING TOOL

A scoring tool is designed specifically to determine the overall score for information systems (IS) safeguarding measures in a library as well as total score for each steps or category of measures. This tool is an adaptation from the Information Security Governance (ISG) Assessment Tool for Higher Education (EDUCAUSE/Internet2 Security Task, 2004). As seen in the tool (Appendix A) the total score from each of the five sections below should be entered into the corresponding box on this chart to determine the library's total IS safeguarding measures assessment score. The library's overall IS security protection evaluation rating is determined by factoring together the "Total Score for Presence of Technological Measures" with the "Total Presence of Organisational Measures" to correspond with an overall assessment of poor, needs improvement or good (Table 3).

A library's technological security measures implementation index for its IS security is 'very high' when a library total score for Stage 1 is between 256 to 340 (Table 2). This implies that the library implements the most proper and updated technological countermeasures to protect its security objectives. Based on this score, a library can identify whether its overall organisational security measures are good, needs improvement or poor as shown in Table 3.

terang terangan

diadak kalih
9/15 ?

benang

Table 2: Total Score for Presence of Technological Measures and Organisational Measures

		Low	High	Presence
TOTAL SCORE FOR PRESENCE OF TECHNOLOGICAL MEASURES		0	42	**Very Low**
		43	85	**Low**
		86	170	**Medium**
		171	255	**High**
		256	340	**Very High**
Total Score for Presence of Information Security Policy				
Total Score for Presence of Procedures and Controls				
Total Score for Presence of Administrative tools and Methods				
Total Score for Presence of Awareness Creation				
TOTAL SCORE FOR PRESENCE OF ORGANISATIONAL MEASURES (Presence of IS Policy, Procedures, Administrative tools and Awareness)				

Table 3: Overall Information Systems (Is) Safeguarding Measures Assessment Rating.

Presence of Technological Measures	Total Score for Presence of Organisational Measures		Overall Assessment
Very High	0	90	Poor
	91	130	Needs Improvement
	131	165	Good
High	0	80	Poor
	81	120	Needs Improvement
	121	165	Good
Medium	0	70	Poor
	71	110	Needs Improvement
	111	165	Good
Low	0	60	Poor
	61	100	Needs Improvement
	101	165	Good
Very Low	0	50	Poor
	51	90	Needs Improvement
	91	165	Good

CONCLUSION

In an information-sharing environment, the main concern for a library is to continually provide access to resources and services via a variety of delivery modes including information systems. Simply put, if the critical library IS such as online catalogs, online databases and websites are interrupted and unavailable to its end users, the impact might affect the library's mission as an information provider thus impeding the library and its end users' performance. Therefore, a library's need for effective information security exists regardless of its size since it might face the same security challenges that are keeping intruders away from its private information (Newby, 2002).

This paper attempted to propose a feasible and flexible framework adapted from the Organisational Information Security Staircase Model (Hagen, Albrechtsen and Hovden, 2008) designed to assess the current IS security practices in a library setting. This model encompasses the five steps in the staircase as means and ways for a library to protect the confidentiality, availability and integrity of information processed by an information system and of the information system itself. The first step is concerned with the technological counter measures to protect the workstations, servers, hardware, software, data, network and its physical facilities. The second step can be used to assess the presence of information security policies in a library. The third staircase refines the IS security procedures that should be in place to develop appropriate security tools and methods. The fourth step assesses the presence of administrative security routines in the library's day to day life. The final step evaluates the presence of information security awareness activities in a library so as to strengthen the IS security initiatives among its community.

This paper also presented an assessment tool which was developed to enable a library, regardless of type and size, to use this framework as a self-evaluation to assess regularly the extent or the presence of each IS security measures. Based on the scoring level, a library can evaluate or modify the existing security methods as well as add some new additional security measures at any time based on its security needs and requirements.

REFERENCES

AlAboodi, S.S. 2006. A New Approach for Assessing the Maturity of Information Security. *ISACA: Journal Online*. Available at http://www.itgi.org/Template.cfm?Section=Home&CONTENTID=34805&TEMPLATE=/ContentManagement/ContentDisplay.cfm

Conklin, W.A., White, G.B., Cothren, C., William, D. and Davis, R.L. 2004. *Principles of Computer Security: Security+ and Beyond*. Illinois: McGrawHill Technology Education.

Doherty, N.F. and Fulford, H. 2006. Aligning the information security policy with the strategic information systems plan. *Computers & Security*, Vol.25(1):55-63.

EDUCAUSE/Internet2 Security Task. 2004. The Information Security Governance (ISG) Assessment Tool for Higher Education. Available at http://net.educause.edu/ir/library/pdf/SEC0421.pdf

Eisenberg, J. and Lawthers, C. 2005. Library Computer and Network Security: Library Security Principles. Infopeople Project. Available at http://www.infopeople.org/resources/security/basics/index.html.

Ernst and Young. 2008. *Moving beyond compliance: Ernst & Young's 2008 Global Information Security Survey*. Available at http://www.ey.com/global/Content.nsf/International/Assurance_&_Advisory_-_Technology_and_Security_Risk_-_Global_Information_Security_Survey_2008

Guel, M.D. 2007. *A Short Primer for Developing Security Policies*. Available at http://www.sans.org/resources/policies/Policy_Primer.pdf.

Gupta, M. and Sharman, R. (Eds.). 2008. *Social and Human Elements of Information Security: Emerging Trends and Countermeasures*. Hershey, PA: IGI Global.

Guttman B. and Roback E. 1995. 'An Introduction to Computer Security: The NIST Handbook' U.S. National Institute of Standards and Technology, NIST Special Publication 800-12. Available at http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf.

Hagen, J.M. 2007. Evaluating applied information security measures: an analysis of the data from the Norwegian Computer Crime Survey 2006. *FFI/REPORT-2007/02558*, pp. 35-48. Available at http://rapporter.ffi.no/rapporter/2007/02558.pdf

Hagen, J.M., Albrechtsen, E. and Hovden, J. 2008. Implementation and effectiveness of organisational information security measures. *Information Management & Computer Security,* Vol.16, no.4: 377-397.

Hone, K. and Eloff, J.H.P. 2002. Information security policy – what do international security standards say? *Computers & Security,* Vol.21, no.5: 402-409.

Information-technology Promotion Agency. 2008. *Information Security Management Benchmark (ISM-Benchmark).* Available at http://www.ipa.go.jp/security/english/benchmark/.../Howtouse_ISM_Benchmark.pdf

INTOSAI. 1995. *Information System Security Review Methodology: A Guide for Reviewing Information System Security in Government Organisations.* Available at http://www.issai.org/media(421,1033)/ISSAI_5310_E.pdf

Newby, G. B. 2002. *Information Security for Libraries.* Available at http://www.petascale.org/papers/library-security.pdf

Pipkin, D.L. 2000. *Information Security: Protecting the Global Enterprise.* Upper Saddle River, NJ: Prentice Hall.

Powell, A and Gillet, M. 2007. Controlling Access in the Electronic Library. *Ariadne*, Vol.7. Available at http://www.ariadne.ac.uk/issue7/access- control

Scarfone, K., Souppaya, M., Cody, A. and Orebaugh, A. 2008. *Technical Guide to Information Security Testing and Assessment.* Technical Report Spec. Publ. 800-11, U.S. Department of Commerce. National Institute of Standards and Technology, September 2008. Available at http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

Siponen, M.T. and Oinas-Kukkonen, H. 2007. A review of information security issues and respective research contributions. *The Database for Advances in Information Systems,* Vol.38, no.1: 60-81.

Thiagarajan, V. 2003. Information Security Management BS 7799.2:2002 Audit Check List for SANS. Available at http://www.sans.org/score/checklists/ISO_17799_checklist.pdf

Von Solms, B. (2000), Information security – the third wave?, *Computers & Security*, Vol.19, no.7: 615-620.

Weise, J. and Martin, C. R. (2001). *Sample Data Security Policy and Guidelines Template,* Sun BluePrints OnLine. Available at http://www.sun.com/blueprints/tools/samp_sec_pol.pdf

Westby, J. R. and Allen, J. H. 2007. *Governing for Enterprise Security (GES) Implementation Guide* (CMU/SEI-2007-TN-020). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University. Available at http://www.cert.org/archive/pdf/07tn020.pdf

Williams, R. L. (2001). *Computer and network security in small libraries: A guide for planning.* Texas State Library & Archives Commission. Available at http://www.tsl.state.tx.us/ld/pubs/compsecurity

Yeh, Q. and Chang, A.J. (2007). Threats and countermeasures for information system security: A cross-industry study. *Information & Management,* Vol. 44: 480-491.

Appendix 1

INFORMATION SYSTEMS (IS) SECURITY MEASURES ASSESSMENT TOOL FOR LIBRARY

The following is a list of Information Systems (IS) safeguarding measures.
Please tick **(√)** in the box to indicate the level of implementation in your library based on index below:

1 - Not implemented
2 - Only some part has been implemented
3 - Implemented but has not been reviewed
4 - Implemented and reviewed on regular basis
5 - Fully implemented and recognised as good example for other libraries

1.0	PRESENCE OF TECHNOLOGICAL SECURITY IN MY LIBRARY.	SCORE
a)	**Hardware security**	
1.1	CCTV, visual camera, magnetic detection system and electronic anti-theft system at strategic places, public computer areas and server areas.	
1.2	Emergency power sources and alternative communication lines. (e.g. use of alternative telephone lines or cables and generators)	
1.3	Locks, security cables, locked cable trays, metal cages or anchoring devices to improve the security of hardware equipments.	
1.4	Periodical remote mirroring or file mirroring to back up disk drives.	
	Total Score (a)	
b)	**Software Security**	
1.5	Anti-spyware software to detect and remove any spyware threats.	
1.6	Anti-phishing solutions to prevent phishing attacks.	
1.7	Cleanup software to erase files or settings left behind by a user.	
1.8	Desktop security software at application level and operating level to monitor, restrict usage or disable certain features of the workstations.	
1.9	Distribution agents to automate the process of installing an application or updates to workstations on a network.	
1.10	ID management software to automate administrative tasks such as resetting user passwords and enabling users to reset their own paswords.	
1.11	Menu replacement software to replace the standard windows desktop interfaces and provide control on timeouts, logging and browsing activities.	
1.12	Multi user operating systems and application software to allow concurrent access by multiple users of a computer.	
1.13	Periodical automatic debugging and tests to remove any defects from newly developed software or hardware components.	
1.14	Rollback software to keep track and record of any changes made to the computers and allow the system to be restored to its original starting point from any chosen point in time.	
1.15	Single sign on system for a user authentication and authorisation to access all computers and systems without the need to enter multiple passwords.	
1.16	Spam filtering software to automatically detect unwanted spam emails from getting into a user's inbox.	
1.17	Systems recovery to rebuild and repaire the library computer systems after disaster or crash.	
1.18	Timer software to control the amount of time a patron can use a workstation.	
b)	**Software Security**	
1.19	User entrance log to record and monitor user logs. These logs are regularly analysed by a library staff.	
1.20	Web filtering software to prevent access to inappropriate materials or sites.	

	Total Score (b)	
c)	**Workstation Security**	
1.21	All office productivity software and browsers for the workstations/laptops are configured to receive updates in a timely manner.	
1.22	An application firewall is used for mobile laptops that connect to the library external LANs.	
1.23	The computer's BIOS are secured in order to create a secure public access computer.	
1.24	User identification and authentication are required before logging into the library's workstations, laptops screensavers, library network or campus network.	
1.25	Virus protection programs, configuration settings and security software programs are installed for web browsers and email programs.	
	Total Score (c)	
d)	**Network Security**	
1.26	Antivirus software and desktop security software to receive regular updates to protect the internal network from any security breaches.	
1.27	Digital signatures are used to assure the authenticity of any electronic documents sent via the library's network. (e.g. use of passwords, private key encryption, public key encryption or digital certificates)	
1.28	Firewall to protect the internal network from external threats.	
1.29	Firewall with virtual private network (VPN) capabilities is installed for remote and wireless access connections.	
1.30	Limitation of connection time is performed via configuration routines to control and restrict access for the library's high-risk applications or databases.	
1.31	Public and staff's local area networks (LANs) are physically separated by means of separate cabling for each network to provide alternative circuit.	
1.32	Server segregation/perimeter network (DMZ) by using firewalls and some other network access control devices to separate systems that are at a relatively high risk from unsecured network.	
1.33	The network is segmented with a router to increases the bandwidth available to each user and reduce the congestions or collisions of the library's network.	
1.34	Wireless security products to secure the library wireless network. (e.g. use of default passwords on wireless access points, network ID, wireless intrusion detection systems, wired equivalency protocol (WEP) encryption, MAC address filtering or virtual private networking (VPN))	
	Total Score (d)	
e)	**Server Security**	
1.35	Anti-virus software on servers and anti-virus virus definition files are kept up-to-date.	
1.36	Authentication systems to prevent unauthorised access to the library's server.	
1.37	Fault tolerance is implemented to make sure if one system fails, then there is a backup system that immediately takes over.	
1.38	Firewalls to protect the library network from unwarranted intrusion.	
1.39	Intrusion detection software and host auditing software are installed to monitors the servers or computers for signs of intrusion.	
1.40	Regular backups for the data, hard copy of server hardware specifications, installation information, installation software and passwords are regularly performed and stored at an offsite location.	
e)	**Server Security**	
1.41	Server logs are reviewed periodically by using a log file monitor utility to monitor any signs of intrusion or security violations.	
1.42	The file system in a server is restricted access to the directory structure using file or directory permissions.	
1.43	The library servers' operating systems (OS) and applications are hardened to protect from any vulnerabilities.	
1.44	The server is placed in a secure location, such as in a lockable cage, a locked room and place it with	

	environmental controls.	
	Total Score (e)	
f)	**Data Security**	
1.45	Attributes for each removable media applications in your library are properly recorded and the media are kept from any unauthorised devices from accessing, running or transferring data to your library workstations and network. (e.g. USB thumb drives, tapes, CDs, DVDs, disks, drives, ect.).	
1.46	Combination of authentication systems to restrict access of library data and resources based on a variety of access rights. (e.g. user identification, passwords or biometrics system)	
1.47	Disposable of unused media and sensitive media are properly managed to maintain an audit trail.	
1.48	Enforced path is created between a user terminal and other library services that the user is authorised to reduce the risk of unauthorised access.	
1.49	Event logging or log management software to ensure the library computer security records are stored in sufficient detail for an appropriate period of time. (e.g. records for security incidents, policy violations, fraudulent activities and operational problems)	
1.50	Fraud detection and prevention measures to control fraudulent activity and disclosure of information. (e.g. use of address verification system/AVS, proprietary encryption, internal intrusion detection system, multiple login monitoring, password verification on transactions or data access controls)	
1.51	Public key infrastructure (PKI) to secure the exchange of personal data via the library network and Internet. (e.g. use of public and private cryptography key pair).	
1.52	RFID tags to manage and secure the library collection as well as to track attendance and prevent unauthorised access into the library building.	
1.53	Systematic approaches conducted in house or outsourced to a service provider to address the library vulnerabilities (e.g. managing on vulnerability discovery, prioritisation, remediation, dynamic protection, verification and customisable reporting).	
1.54	Use of cryptography techniques, hardware tokens, software tokens and single sign on systems to control data access for the library internal and remote computer systems.	
1.55	Use of password protection of user accounts, anti virus software, firewalls, wireless network protections, intrusion detection systems and Internet Protocol Virtual Private Networks/IP VPNs to ensure data insert and sent from one end of a transaction arrives unaltered at the other end.	
1.56	Vital library's business information or records are regularly backed up. (e.g. inventory records, patrons' data, library databases, production servers and critical network components and backup media).	
1.57	Web access management systems to manage and validate user access to devices, applications and library systems. (e.g. authentication management, single sign-on convenience, audit or reporting systems).	
f)	**Data Security**	
1.58	Web content filtering/monitoring systems on individual workstations or at a central point on the network to prevent users from viewing inappropriate web sites or content. (e.g. at the proxy server or internet server).	
1.59	Your library network and information systems security services are properly managed in house or outsourced to a service provider. (e.g. Round-the-clock monitoring, management of firewalls and intrusion detection systems, management of patch management and upgrades, performing security assessments, performing security audits and responding to emergencies).	
	Total Score (f)	
g)	**Physical and Environmental Security**	
1.60	Air conditionings to stabilise the air temperature and humidity within the library building.	
1.61	Earthquake early warning system to provide an emergency warning to the library staff and patrons prior to damaging ground shaking.	
1.62	Flood detector to sense the presence of water to provide an early warning of developing floods in a library.	

1.63	Lightning protectors and surge protectors to protect any valuable machines or equipments from lighting strikes, voltage spikes and surges.	
1.64	Security guards to monitor people entering and leaving the library buildings and sites.	
1.65	Use of automatic sprinkler systems, smoke detectors, fire extinguishers and fireproof installations in the library buildings and areas adjacent to library's key assets to detect and prevent fires, toxic chemical spills and explosions.	
1.66	Use of magnetic stripe swipe cards, electronic lock, proximity cards, bar code card or biometrics to secure and control access to restricted library areas.	
1.67	Warning signs, fencing, vehicle height-restrictors, site lightings and trenches around the library areas to provide initial layer of security for a library building.	
1.68	Wireless gates, biometrics or other user identifications and authentication forms at the library main entrances, exists and public access areas to control access into the library building.	
	Total Score (g)	
	TOTAL SCORE FOR TECHNOLOGICAL SECURITY IN MY LIBRARY *(a+ b+ c+ d+ e+ f+ g)*	
2.	**Presence of information security policy in my library**	
2.1	Back ups and off-site storage policies for your library data, media or materials that contain sensitive information.	
2.2	Data classification, retention and destruction policies for your library data, media or materials that contain sensitive information.	
2.3	Identity management policies for library Information Systems user registration and password management.	
2.4	Job responsibility policy for individual employee responsibilities related to the library IS security practices.	
2.5	Policies on access control, authentication and authorisation practices for using the library Information Systems.	
2.6	Policies on protection of library IS assets to protect your library's hardware, software, data and people.	
2.7	Secure disposal policies to dispose library data, media or materials that contain sensitive information.	
2.8	Polices on reporting, notification and response of Information Systems security events to affected parties such as individuals, law enforcement, campus or parent organisations.	
2.9	Policies on acceptable use of wireless devices in your library such as laptops and hand phones.	
2.	**Presence of information security policy in my library**	
2.10	Policies on acceptable use of workstations, e-mails, databases, intranet and Internet in your library.	
2.11	Policies on managing privacy and confidentiality issues, including breaches of personal information.	
2.12	Policies on sharing, storing and transmitting of library data via ISPs, external networks or contractors' systems.	
	Total Score (2)	
3.	**Presence of procedures and controls in my library.**	
3.1	Controls and disciplinary procedures if a library staff or patrons breach the IS security policies or rules. (e.g. verbal warning, written warning, suspension and dismissal).	
3.2	Procedures for handling library sensitive data and personal data of library patrons to prevent errors, unauthorised disclosure or misuse by those who handle it.	
3.3	Procedures for non-disclose agreement or confidentiality agreement to all library staff and patrons to protect any type of confidential and proprietary information.	
3.4	Procedures for update and review existing information security policies.	
3.5	Procedures on the intellectual property rights and copyrights in controlling and protecting any digital works or resources that are stored, transmitted, accessed, copied or downloaded via the library IS.	
3.6	Procedures which list all requirements with regard to outsourcing any library Information Systems service or activities.	

	Total Score (3)	
4.	**Presence of administrative tools and methods in my library.**	
4.1	Procedure for owner accountability to ensure appropriate protection is maintained for each library IS asset. (e.g. information assets, software assets, physical assets and library services).	
4.2	Procedures for the development and implementation of risk analysis to protect your library from all types of threats. (e.g. Performance of assets analysis, threat analysis, annual loss expectancy analysis, identification and evaluation of security measures).	
4.3	Procedures on handling, reporting, notification and response of IS security events to affected parties such as individuals, law enforcement, campus or parent organisation.	
4.4	Procedures related to asset classification in order to organise it according to its importance and sensitivity to loss. (e.g. unclassified, confidential, secret and top secret)	
4.5	Regular internal and external audits programs appropriate for your library's Information Systems size, complexity of activities, scope of operations, risk profile and compliance with the relevant standards.	
	Total Score (4)	
5.	**Presence of awareness creation in my library.**	
5.1	All staff and patrons at various levels are made aware of their responsibilities with regard to protecting the library's Information Systems' security and trained to report any security breach incidences.	
5.2	All staff and patrons at various levels receive appropriate information security trainings and education.	
5.3	All staff and patrons at various levels receive regular updates on your library Information Systems' policies and procedures.	
5.4	Information security awareness trainings have become mandatory to all staff and patrons at various levels.	
5.5	Risk assessment approach exists and follows a defined process that is documented.	
5.6	Staff and patrons at various levels are trained to monitor and handle the library's Information Systems on their own.	
5.	**Presence of awareness creation in my library.**	
5.7	There are balanced set of key performance indicators (KPIs) and metrics used to provide the real insight into the effectiveness of security awareness programs.	
5.8	There are positive supports and commitments from the top management to coordinate the implementation of Information Systems' security controls in your library. (e.g. via allocation of budget, strong interest and active involvements).	
5.9	Threats that could harm and adversely affect critical operations of your library Information Systems' security are identified and up dated regularly.	
5.10	Vulnerabilities in your library information systems and related processes are identified and up dated regularly.	
	Total Score (5)	