ASSESSING INFORMATION SECURITY MANAGEMENT IN MALAYSIAN ACADEMIC LIBRARIES

ROESNITA BINTI ISMAIL

THESIS SUBMITTED IN FULFILMENT OF THE
REQUIREMENTS FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

FACULTY OF COMPUTER SCIENCE &
INFORMATION TECHNOLOGY
UNIVERSITY OF MALAYA
KUALA LUMPUR
2012

Abstract

Assessing Information Security Management in Malaysian Academic Libraries

This research aimed to study the perceived threats of information security, their frequency of occurrence and the perceived main source of information security threats in Malaysian academic libraries. Utilising the relevant literature, a possible list of information security threats were listed and investigated. In addition, the researcher also studied the levels of implementation of information security measures in these academic libraries. The information security measures were grouped into five (5) components that represent the proposed library information security assessment model (LISAM). The five (5) components included the technological measures, information security policies, security procedures, security methods and security awareness creation activities. The researcher also studied the differences between the academic libraries in applying information security measures based on the type of university, number of staff, years in ICT adoption, yearly information security budget, availability of information system (IS) security staff and availability of wireless connection. Data used was based on structured questionnaires collected from a total of 39 individuals who were responsible for the information systems (IS) or information technology (IT) in academic libraries in Malaysia. The pilot test and the actual data collection indicated all the five components in the instruments are reliable with cronbach alpha correlation coefficients above $\alpha = 0.60$. Findings revealed that hardware security threats (70.0%), human-related threats (66.0%) and environmental threats (51.0%) were perceived as the most common information security threats in Malaysian academic libraries. However, data security threat was perceived as the least threatening to these academic libraries. There were slightly high frequencies of occurrence of hardware maintenance errors, use of unauthorised hardware and malicious code attacks in these academic libraries. Parallel with the existing research findings, hardware and software failures (56.4%) as well as human-related threats (41.0%) were perceived as the main root causes of information security incidents in these academic libraries. Most of technological measures for hardware, software, workstation, network, server, data and environmental security have been implemented and reviewed on regular basis in these academic libraries. This study found significant differences among academic libraries in Malaysia in applying

technological measures due to yearly information system's security budget and availability of information systems (IS) security staff. However, most of information security procedures, information security administrative tools and information security awareness creation were rated at Level 2 (Only some part of measures have been implemented), these findings were discouraging as rating of Level 4 (Implemented and reviewed on regular basis) and Level 5 (Fully implemented and recognised as good example for other libraries) would be better reflection of a well implemented organisational measures in libraries. This study found significant differences among academic libraries in Malaysia in applying the organisational measures due to number of staff, yearly information system security budget and availability of information system (IS) security staff. With regard to the overall security status of information security management in Malaysian academic libraries based on the proposed information security assessment tool for libraries, findings revealed that half of those academic libraries (55.3%) surveyed have good practice of technological security measures but require improvement on organisational measures. This may be due to the over-emphasis on technology as the sole solution to information security problems in these academic libraries. Therefore, it is necessary to put organisational measures in place as relying on technology alone will not solve the information security problems effectively.

Abstrak

Menilai Pengurusan Keselamatan Maklumat di Perpustakaan-Perpustakaan Akademik di Malaysia

Kajian ini bertujuan untuk mengkaji ancaman-ancaman keselamatan maklumat, kekerapan kejadian dan sumber-sumber utama yang dianggap mengancam keselamatan maklumat di perpustakaan-perpustakaan akademik di Malaysia. Berdasarkan ulasan kesusasteraan, senarai kemungkinan ancaman keselamatan maklumat di perpustakaan telah disenaraikan dan diselidiki. Di samping itu, penyelidik juga mengkaji tahap-tahap pelaksanaan pengawalan keselamatan maklumat di perpustakaan-perpustakaan akademik ini. Untuk mencapai matlamat ini, penyelidik mencadangkan model penilaian keselamatan maklumat di perpustakaan (LISAM) yang mempunyai lima (5) komponen penilaian. Lima (5) komponen tersebut meliputi langkah-langkah teknologi, dasar-dasar keselamatan maklumat, prosedur keselamatan, kaedah keselamatan dan aktiviti membentuk kesedaran keselamatan maklumat. Penyelidik juga mengkaji perbezaan di antara perpustakaan akademik dalam menggunapakai langkah-langkah keselamatan maklumat berdasarkan jenis universiti, bilangan kakitangan, tempoh dalam penggunaan ICT, bajet tahunan untuk keselamatan maklumat, kewujudan kakitangan untuk menjaga keselamatan sistem maklumat dan ketersediaan akses Internet tanpa wayar. Data dalam kajian ini berdasarkan kepada soal selidik berstruktur yang telah diperolehi daripada 39 individu yang bertanggungjawab mengenai sistem maklumat (IS) atau teknologi maklumat (IT) di perpustakaan akademik di Malaysia. Keputusan kajian rintis dan kajian sebenar menunjukkan kebolehpercayaan kelima-lima komponen dalam instrumen mempunyai nilai *cronbach alpha correlation coefficients* lebih daripada α=0.60. Hasil penemuan mendedahkan bahawa ancaman perkakasan (70.0%), ancaman manusia (66.0%) dan ancaman alam sekitar (51.0%) telah dianggap sebagai ancaman keselamatan maklumat yang lazim berlaku di perpustakaan akademik di Malaysia. Walau bagaimanapun, ancaman keselamatan terhadap data telah dilihat sebagai kurang merbahaya bagi perpustakaan-perpustakaan akademik ini. Kesilapan penyelenggaraan perkakasan, penggunaan perkakasan yang tidak dibenarkan dan serangan kod berniat jahat berlaku agak tinggi di perpustakaan-perpustakaan ini. Selari dengan penemuan penyelidikan yang sedia ada, kegagalan perkakasan dan perisian (56,4%) serta ancaman berkaitan dengan manusia (41.0%) telah dianggap sebagai punca utama berlakunya insiden keselamatan maklumat di perpustakaan-perpustakaan akademik ini. Secara keseluruhan, kebanyakkan langkah-langkah teknologi untuk melindungi perkakasan, perisian, stesen kerja, rangkaian, server, data dan keselamatan alam sekitar telah dilaksanakan dan disemak secara tetap di perpustakaan-perpustakaan akademik ini. Kajian ini mendapati perbezaan yang signifikan di kalangan perpustakaan akademik di Malaysia dalam menggunapakai langkah-langkah teknologi yang disebabkan oleh bajet tahunan untuk keselamatan maklumat dan kewujudan kakitangan untuk menjaga keselamatan sistem maklumat. Walau bagaimanapun, kebanyakan prosedur keselamatan maklumat, kaedah keselamatan maklumat dan aktiviti mewujudkan

kesedaran keselamatan maklumat hanya dinilai di Aras 2 (Hanya sebahagian daripada langkah-langkah telah dilaksanakan), penemuan ini tidak memuaskan kerana penarafan Aras 4 (Dilaksanakan dan dikaji semula secara tetap) dan Tahap 5 (Dilaksanakan secara sempurna dan diiktiraf sebagai contoh yang baik kepada perpustakaan lain) adalah gambaran perlaksanaan langkah-langkah keselamatan maklumat yang lebih baik di sesebuah perpustakaan. Kajian ini mendapati perbezaan yang signifikan di kalangan perpustakaan akademik di Malaysia dalam menggunapakai langkah-langkah organisasi yang disebabkan oleh bilangan kakitangan, bajet tahunan untuk sistem keselamatan maklumat dan kewujudan kakitangan untuk menjaga keselamatan sistem maklumat. Berdasarkan alat penilaian keselamatan maklumat untuk perpustakaan yang dicadangkan, penemuan mendedahkan bahawa separuh (55.3%) daripada perpustakaan-perpustakaan akademik yang dikaji di Malaysia, mempunyai amalan langkah-langkah keselamatan teknologi yang baik tetapi memerlukan penambahbaikan bagi langkah-langkah organisasi. Ini mungkin disebabkan oleh penekanan yang berlebihan kepada teknologi sebagai langkah penyelesaian tunggal bagi masalah-masalah keselamatan maklumat di perpustakaan-perpustakaan akademik ini. Maka, adalah perlu untuk melaksanakan langkah-langkah organisasi di perpustakaan-perpustakaan ini kerana pergantungan kepada teknologi sahaja tidak akan dapat menyelesaikan masalah-masalah keselamatan maklumat secara berkesan.

Acknowledgements

The thesis writing journey has been a long road for me. Sometimes, there were days when I thought I would never finish it, but the support of my family, my supervisor and my dear friends gave me the courage to continue. Therefore, I would like to express my sincere gratitude to everyone who has guided me through the process and contributed to the completion of this thesis.

First of all, Alhamdulillah, praise to Allah s.w.t for His blessing and Kindness, for giving me the strength and ability to complete this study.

Secondly, I would like to acknowledge my supervisor Prof. Dr. Zainab Awang Ngah for her continuous support, patience, motivation, enthusiasm and immense knowledge. Her guidance helped me in all the time during my PhD journey. I would also like to thank the rest of faculty members in the Department of Library and Information Science, Faculty of Computer Science and Information Technology, University of Malaya: Dr. Kiran Kaur, Dr. Diljit Singh, Prof. Dr. Gary Eugene Gorman, Assoc. Prof. Dr. Abrizah Abdullah, Dr. Maryam Nazari, Dr. Noor Harun Abdul Karim, Dr. Noorhidawati bte Abdullah (Internal Examiner), Prof. Dr. Chen Kuang Hua (External Examiner) and Assoc. Prof. Dr. Jamshid Baheshti (External Examiner) for their guidance, encouragement, constructive and insightful comments.

I would also like to sincerely acknowledge the Universiti Sains Islam Malaysia (USIM) and the Ministry of Higher Education Malaysia, for providing financial assistance in the form of SLAI/KPT scholarship during my Ph.D. tenure in the University of Malaya. I am also extremely indebted to Prof. Dr. Jalani Sukaimi, Dean, Faculty of Science and Technology, USIM, for his valuable advice, constructive criticism and providing necessary infrastructures to complete my study.

Most importantly, I would like to express my deepest gratitude and appreciation to my parents, my husband, my children, my relatives and my dear friends, for their understanding and support during the best and the worst moments of my doctoral journey. I hope I can return the favor someday!

I humbly acknowledge the assistance of librarians at the University of Malaya Library and Tan Sri Dr. Abdullah Sanusi Digital Library, Open University Malaysia for their outstanding efforts to ensure the quality information and relevant literature easily accessible at my fingertips. On a special note I would like to thank to respondents who have participated in this research, this thesis would not have completed without their participations. May Allah reward everyone who has contributed to the completion of this thesis with *Jannatul Firdaus*, amin.

Roesnita Ismail

Table of Contents

CHAPTER TWO

LITERATURE REVIEW

CHAPTER THREE

RESEARCH FRAMEWORK AND DESIGN

CHAPTER FOUR

POSTURES AND THE PERCEIVED INFORMATION SECURITY THREATS IN MALAYSIAN ACADEMIC LIBRARIES

CHAPTER FIVE

LEVEL OF IMPLEMENTATION OF INFORMATION SECURITY MEASURES AND DIFFERENCES IN APPLYING THESE MEASURES

CHAPTER SIX

DISCUSSION AND CONCLUSION

LIST OF FIGURES

LIST OF TABLES

Chapter One

Introduction

1.0 An Overview

Information security (ISec) is the means and ways of protecting data from unauthorised access, change, misuse, loss and ensures its availability whenever required. At the beginning, ISec was focused mainly on technical issues and the responsibility was left to technical experts (Solms, 2000). This view has changed as there is growing management realisation on the importance of ISec, thus, aspects like policies, procedures and top management involvement are incorporated in managing ISec (Solms, 2000). Subsequently, it was felt there was a need for some form of standardisation, best practices, certification, ISec culture, measurement and monitoring of ISec in an organisation. Finally, views encompass the development of ISec governance as an integral part of corporate governance that consists of the stakeholders' commitment, proper organisational structures for enforcing good ISec, user awareness as well as commitment towards good ISec, the necessary policies, procedures, processes, technologies and compliance enforcement mechanisms (Solms, 2006).

ISec management in the context of library management describes controls that a library needs to implement in order to protect its information assets from all potential threats to ensure the confidentiality, integrity and availability of its information resources. All libraries have information assets that need to be protected. The endless volumes of a library's main resources, services and personal patrons' records such as their names, addresses, e-mail addresses, passwords, loan records and website logs reside in the library's IS and most of these resources can be accessed remotely via the library website. As indicated by Mohammed Imtiaz (2001) "library services need to reach to

the readers with the use of the technology to provide online access to globally generated information and to provide uninterrupted worldwide access to the library resources searchable from anywhere, anytime, by anyone". A library's increased reliance on the Internet for generating, collecting, organising, presenting and disseminating information and services has exposed the library to various threats. Failure to appropriately manage ISec can potentially expose the library to loss of time, money, service delivery and public trust. As highlighted by Zimerman (2010), library computers are physically vulnerable to attacks of malware agents which include Trojans, viruses, worms, adware, spyware, pornware, keystroke loggers, password stealers as well as to theft, damage and destruction. Hackers, viruses, worms and Trojan horses are referred as external threats which libraries should be able to handle (Al-Suqri and Afzal, 2007). Thus, availability, integrity and preservation of data are the core roles of libraries in this digital environment (Brainstorming Report, 2001).

The research described in this thesis is concerned with information security management (ISM) in Malaysian libraries. Many studies have concentrated on the issues of how to protect information system (IS) from cyber threats; mostly from the technical perspective. Some other researchers have directed attention not only to technological but also to organisational dimensions (Calder and Watkins, 2003; Chan et al., 2005; Ma and Pearson, 2005; Mercuri, 2004 and Vaast, 2007). This research, however, was motivated to assess types and statuses of technological and organisational measures that are being adopted by academic libraries in Malaysia. Some attempts have been made to understand the types of computer threats targeted on health and industries, public offices and workplaces in Malaysia. However, the possible types of threats that might breach library ISec remain unclear as very few empirical studies related to ISec threats have been conducted specifically in a library setting. Therefore,

this research aimed to study the perceived threats of ISec, their frequency of occurrence and the perceived main source of ISec threats in Malaysian academic libraries. Through the sample obtained from key players of ISec in Malaysian academic libraries, results of the descriptive analysis also revealed the status of implementation of technological and organisational measures in these libraries as well as the differences between these libraries in implementing technical and organisational measures due to type of universities, years in ICT implementation, yearly ISec budget, availability of IS security staff and availability of wireless connection. The final result also provides empirical proof on the most common types of hardware, software, workstation, data, hardware, software, data, network, physical and human-related threats experienced by Malaysian academic libraries.

1.1 The Problems

1.1.1 Information Security Issues in Libraries

The first important step in ISec planning is to understand which assets the library needs to protect and why the protection is necessary. This requires an awareness of the types of threats and vulnerabilities confronting a library's valuable assets. Security attacks such as hacking, denial of services, worms and viruses often compromise the library IS security (Breeding, 2006). In most cases, the threat's target is the information itself rather than the system that transmits it. However, necessary precautions are needed to protect the overall elements of the library IS including the hardware, software, physical environment, documentation and people related to an IS from any potential of threats. And securing any of those elements in a library must be achieved without any compromise to the public services, user privacy and legal access (Eisenberg and Lawthers, 2005). The possible consequences or impacts might be in terms of loss of confidentiality, integrity and/or availability of the information. For instance, the security weaknesses in any library systems can lead to unauthorised accessed of confidential

information (such as the patrons' personal information and circulation record) or loss of integrity of the data stored. These in turn can have negative effect on the trust of publishers or other content providers, can cause embarrassment or even economic loss to the library, and can even lead to other serious problems if urgently needed information is unavailable (Fox and ElSherbiny, 2011).

Libraries, as a broker between the users and the universe of information resources, serve a diverse clientele and there is increasing pressure for libraries to co-operate in providing access to services to members of other libraries or universities (Ahmed, 2000). Thus, libraries must have effective authentication mechanisms to assure the privacy and confidentiality of information during its collection, storage, processing and dissemination only to those authorised, such as library staff and registered members and to prevent accidental disclosure of sensitive information. There are several security problems often not addressed in libraries related to the confidentiality of information and these include (Newby, 2002 and Cain 2003): 1) privacy offered for data that may be collected from patrons apart from circulation records can be questionable; and 2) risks of penetration of library systems from outside parties who may access circulation or other data from outside the library via an Internet connection and an unattended modem or from staff who abuse their access rights. The impacts of unauthorised, unanticipated or unintentional disclosure of confidential information can range from severe to serious consequences and these include: 1) the jeopardising of library security to disclosure of Privacy Act data; 2) loss of public confidence, embarrassment or legal action against the library; and 3) loss of collection or revenue due to insecure computing environment (Stoneburner, Goguen and Feringa, 2002; and Cain, 2003).

Now days, most library resources and services can be accessible at any time and from anywhere. Providing access to those valuable library resources via the library website may expose the library to a greater risk as they can be accessible to people outside the library as well as those within via the library server (Eisenberg and Lawthers, 2005). Libraries must decide how to ensure that the information stored, processed, transited or accessed via the library systems are protected against viruses and worms to guarantee that information and services are not corrupted, degraded or undergone unauthorised modification because the intruders can be anybody and from anywhere in the world. It was once reported that a hacker had defaced the National Library of Australia's website, leaving a cryptic message on parts of its site. It was believed that the defaced page was posted on a Windows NT platform (McAuliffe, 2000). The presence of contaminated, corrupted and missing data could result in violation of data, fraud and successful attack against system availability and confidentiality's which may reduces the assurance or integrity of a library system (Stoneburner, Goguen and Feringa, 2002). These scenarios have been noted by Breeding (2006) as worrying remarks such as 'libraries are often perceived as "an easy mark" and become a jumping-off point for hackers to other networks or computers in a library'.

It is important that a library must use a reliable network system, provide adequate work stations and flexible access hours from internal or remote areas. Equally important, a library also need to ensure that the data and information are secured for authorised users, protecting them from denial of services (DoS), viruses, worms, and lost of IS capabilities due to the natural disasters or human errors (Eisenberg and Lawthers, 2005). If the critical library IS such as online catalogues, online databases and websites are unavailable to its end-users, the impacts are many and might include: 1) affecting the library's mission as an information provider; 2) losing revenue due to the loss of

system functionality and operational effectiveness of a library IS; and 3) losing productive time, thus impeding the library and its end-users' performance. Obviously, the library ISM must at least ensure the confidentiality, integrity and availability of information processed by an IS and of the IS itself as they are essential to the success of a library administrative activities and services.

1.1.2 Perceptions on Information Security Management from Literature

In the past, literature on ISec is seemingly concentrated on the technical aspects as means in protecting information (such as use of encryption, access control, intrusion detection and firewalls) but overlooking the human component (Daniels and Spafford, 1999). As most researches tended to focus on the technical side, management attention to ISec has been low compared to other ISec issues (Olnes, 1994 and Hong et al., 2003). This is because, organisations tend to believe that for every security problem there is a technological solution. They therefore believe that technical tools will solve all their ISec problems.

This situation has somewhat changed. More recently, researchers have suggested that organisations should adopt a mixed approach encompassing procedural (such as security policies, acceptable usage guidelines, security awareness programmes) as well as technical countermeasures (D'Arcy and Hovav, 2004). This is because ISec is seen holistically, which involves two equally important components, namely the physical security and the non-technological security. Loch and Carr (1991) reported that management's concern with IS security ranks among the ten most important topics in information management. The shift towards people rather than technology alone is due to the fact that all technical security controls are purchased, implemented, managed and used by humans (Hinson, 2003). People are seen as both perpetrators and victims of

security breaches or accidents as they use and manage IS on a day-to-day basis (James, 1996). Many recent studies highlighted people or human failures as the greatest threats of information security, not the technical vulnerabilities (AlAboodi, 2006; Yeh and Chang, 2007; Ernst and Young, 2008). As indicated by Hinson (2003) simple configuration mistakes can leave firewalls vulnerable and systems completely unprotected, thus, human error is far more likely to cause serious security breaches than technical vulnerabilities. This is the reason, why many organisations have invested millions in securing their IT infrastructure in various forms of physical, personnel and administrative defenses to reduce the frequency and severity of computer security-related losses (Guttman and Roback, 1995). Summing up, ISec is both a human and a technological problem. This suggests that building a secure library's ISec is becoming more complicated and IS security can be achieved by applying technical, management and procedural means (AlAboodi, 2006).

1.1.3 Gaps in the Literature

Despite the important investments in technological and non-technological components for ISec in any organisation, not much is known on the actual scenario of IS security, especially in libraries. The few Malaysian-related studies covered mainly information system security in healthcare, IT organisations and government sectors (Al-Salihy, Ann and Sures, 2002; Suhazimah, 2007; Samy, Rabiah and Zuraini, 2009). Literature also reports that different industries tend to have different requirements for their ISec needs (Jung, Han and Lee, 2001; Yeh and Chang, 2007). Similarly, several researchers found that financial organisations undertake more security efforts and have stronger deterrent strategies than other industries (Kankanhalli, Teo, Tan et al., 2003; Davamanirajan, Kauffman, Kriebel et al., 2006).

In general, research that focuses on library aspects of control measures for ISec is sparse. Because of the paucity of the work in this area, there is little general guidance for libraries on these matters. As highlighted by Newby (2002), IS security is often under-appreciated in libraries and this is surprising as information is the library's main business. Therefore, this research is designed to explore the current status of security breach incidents that can potentially jeopardised the library IS security and justify whether or not academic libraries have taken appropriate steps via technical, management or procedural means to safeguard their own IS security.

1.2 The Motivation

Despite acknowledging the important value of information in a library and the vital role played by IS to process the information, empirical research in ISec related to libraries is relatively new and rare. As a result, the motivation of this empirical study is to extend knowledge of ISec in literature by specifically focusing on the types of ISec breaches and the current security controls used in Malaysian academic libraries. This study will be a significant endeavor for the enhancement of ISec strategies used by academic libraries and other libraries in protecting their information and IS. The results of this study may help library management identify the strengths, weaknesses and priorities in managing its ISec so that relevant actions can be applied in a more efficient and effective manner.

This study is also aims to find out and contribute to the existing literature on academic library implementations of technical and organisational countermeasures. Types of technical and organisational countermeasures are listed and examined. Based on findings from this study, the researcher proposes an assessment tool for assessing the status of implementation of ISec measures in Malaysian academic libraries. This study

will be a significant in promoting good ISec practices in libraries and encouraging the cultivation of good security culture among library practitioners.

Study on ISec threats especially in libraries is still very rare and the purpose of this research is to gain a better insight on the current status of ISec threats in Malaysian academic libraries. This research holds significant value in terms of providing a possible list of ISec threat categories in academic libraries and identifying the common threats related to hardware, software, data, network and human-related threats in academic library domains.

1.3 Scope of the Study

The scope of the study is to assess ISec management, specifically on the types and levels of implementation of ISec measure deployed in Malaysian academic libraries. The assessment is focused on the level of implementation of technical and organisational countermeasures. This study also explores the various types of ISec threats in Malaysian academic libraries. The possible type of ISec threats are examined, particularly in terms of common hardware, software, data, network, physical and human-related threats experienced by Malaysian academic libraries in the past six months (between June 2009 until December 2009). In order to guide the reader, the researcher positions two guidance points throughout this thesis. Firstly, the research objective is set out to provide the central direction of the study. The second point is the posing of questions and hypotheses that this study seeks to answer.

1.3.1 Research Purpose and Objectives

The purpose of this research is to conduct an information system (IS) security assessment in Malaysian academic libraries by understanding the current IS security threats and its security practices as well as to propose a model for ISec in the academic libraries. Therefore, this study aims to achieve the following objectives:

1) To explore the general information technology (IT) infrastructures in Malaysian academic libraries in terms of number of personal computer (PC) allocations, availability of wireless connection, type of operating system used, years of information and communications technology (ICT) adoption, percentage of IS security budget and availability of IS security staff.
2) To explore the most common perceived ISec threats and the frequency of their occurrences (in term of hardware, software, data, network, physical and other IS security threats) discovered by these libraries during a period of six months;
3) To find out the most common perceived source of ISec threats in Malaysian academic libraries;
4) To ascertain the extent of technological measures deployed by Malaysian academic libraries. This would include identifying the level of implementation of hardware, software, workstation, network, server, data and physical security measures in these libraries;
5) To investigate the differences between academic libraries in Malaysia in applying the technical measures in terms of type of university, years in ICT implementation, yearly ISec budget, availability of IS security staff and availability of wireless connection.
6) To ascertain the extent of organisational measures deployed by Malaysian academic libraries. This would include identifying the level of implementation of security policy, procedures and controls, tools and methods and awareness activities in these libraries.
7) To investigate the differences between academic libraries in Malaysia in applying organisational measures in terms of type of universities, years in ICT implementation, yearly ISec budget, availability of IS security staff and availability of wireless connection; and

8) To propose a model and an assessment tool to assess the implementation status of ISec in Malaysian academic libraries.

1.3.2 Research Questions

In order to meet the purpose and objectives of the study, the following research questions are asked:

Research Question 1:
What is the general background of information technology (IT) infrastructures in Malaysian academic libraries in terms of number of PC allocations, availability of wireless connection, type of operating system used, years of ICT adoption, percentage of IS security budget and availability of IS security staff?

Research Question 2:
What are the most common perceived IS security threats and the frequency of their occurrence in Malaysian academic libraries in terms of hardware, software, data, network, physical and human- related threats?

Research Question 3:
What is the most common perceived source of IS security threats in Malaysian academic libraries?

Research Question 4:
What is the level of implementation of technological security measures (in terms of hardware security, software security, workstation security, network security, server security, data security and physical security measures) in Malaysian academic libraries?

Research Question 5:
Are there significant differences between academic libraries in Malaysia in applying technological measures based on type of university, number of staff, years in ICT implementation, yearly IS security budget, availability of IS security staff and availability of wireless connection?

Research Question 6:

What is the level of implementation of organisational security measures (in terms of security policy, procedures and controls, tools and methods and awareness activities) in Malaysian academic libraries?

Research Question 7:

Are there significant differences between academic libraries in Malaysia in applying the organisational measures based on type of university, number of staff, years in ICT adoption, yearly Isec budget, availability of IS security staff and availability of wireless connection?

Research Question 8:

What is the overall implementation status of technological security measures and organisational security measures in Malaysian academic libraries based on the proposed assessment tool?

1.3.3 Hypotheses

1.3.3.1 Differences between academic libraries in Malaysia in applying technical measures based on the type of university, number of staff, years in ICT adoption, yearly ISecbudget, availability of IS security staff and availability of wireless connection are suspect. Hence, it is therefore hypothesised that;

Hypothesis 1

There are no significant differences between academic libraries in Malaysia in applying technical measures based on type of university, years in ICT implementation, yearly ISecbudget, availability of IS security staff and availability of wireless connection.

1.3.3.2 Differences between academic libraries in Malaysia in applying organisational measures based on the type of university, number of staff, years in ICT adoption, yearly Isec budget, availability of IS security staff and availability of wireless connection are suspect. Hence, it is therefore hypothesised that;

Hypothesis 2

There are no significant differences between academic libraries in Malaysia in applying organisational measures based on the type of university, years in ICT implementation, yearly ISec budget, availability of IS security staff and availability of wireless connection.

1.4 Assumptions

The assumptions for this study are that the academic libraries have larger collections, larger number of staff and patrons, receive more funds and also have more diverse of services when compared to other types of libraries. The academic libraries selected as samples in this study were based on the assumptions that they have automated library systems, provide Internet and online services to the patrons.

This research was limited to a specific individual within an academic library. This would increase the accuracy and quality of response because the individual was chosen due to the nature of his role and responsibilities that are in the relevant position to provide the desired information on ISec threats and measures. The majority (90%) of respondents were from the management division, which include the librarians or library executives, heads of automation units, IT officers or IS officers, senior librarians, automation librarians and chief librarians or deputy chief librarians. Thus, it is likely that they were all sensitive to ISec concerns. This study is descriptive in nature and findings from this research may not be generalised to all libraries and other industries in Malaysia or in other geographic areas.

1.5 Definition of Terms

Definitions of key terminologies used throughout this thesis are derived from documents and handbooks.

1.5.1 Information Security (ISec)

Information security is referred as 'a combined set of measures at the physical, personnel, administrative, computer and information system levels' (INTOSAI, 1995).

1.5.2 Information Security Management (ISM)

Information security management describes controls that an organisation needs to implement in order to ensure the confidentiality, integrity and availability of its information resources.

1.5.3 Information System (IS)

In this study, the term information system (IS) defined as 'people, technologies and machines used to capture or generate, collect, record, store, retrieve, process, display and transfer or communicate information to multiple users at appropriate levels of an organisation to accomplish the specific set of functions' (Federation of American Scientists, 1998). IS in library refers to online databases, web-based resources, digital library collections and library resources (Kochtanek and Matthews, 2002). Library resources may include bibliographic records and patrons' records. Library uses IS for various reasons including managing the library administration (e.g. managing patron records and bibliographic records), processing of library materials, developing online resources, accessing online resources, developing offline resources, accessing offline resources and providing service to patrons (Akintunde,2004). Therefore, IS are crucial for libraries that were highly information-intensive or relied heavily on IS.

1.5.4 Information System (IS) Security

In this study, the term information system security is referred as 'the protection of IS against unauthorised access to or modification of information, whether in storage, processing, or transit, and against the denial-of service to authorised users or the provision of service to unauthorised users, including those measures necessary to detect, document and counter such threats' (INFOSEC, 1992).

1.5.5 Threats

In this study, threat is describe as any circumstance or event with the potential to adversely impact an IS through unauthorised access, destruction, disclosure, modification of data and /or denial of service (NSTISSC, 2000).

1.5.6 Threat source

Threat source or threat agent specifies the intent and method targeted at the intentional exploitation of vulnerability or a situation and method that may accidentally trigger vulnerability (NIST IR 7298, 2006).

1.5.7 Security practice

Information system security practices depend on effective ISec solutions to minimise vulnerabilities associated with a variety of threats, where the broader sharing of such practices will enhance the overall security of the organisation.

1.5.8 Security safeguards or controls

Protective measures and controls prescribed to meet the security requirements specified for an IS. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas and devices (NSTISSC, 2000). In this

study the safeguards or countermeasures specifies the organisational and technical controls prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information (NIST IR 7298, 2006).

1.5.9 Organisational measures

The organisational measures include the security policy; procedures and control; non-technological tools and methods; and creation of security awareness (Hagen, Albrechtsen and Hovden, 2008).

1.5.10 Technological measures

The technical mechanisms or controls refer to mechanisms use to protect the computer hardware, computer software, workstation, network, server, data and physical facilities.

1.6 Organisation of the Thesis

The thesis is organised into six chapters. This chapter provides the research background, the problem statement, significance of the study, the scope of the study, research questions, research objectives, research hypotheses and the definitions of key terms. Chapter Two elaborates a review of literature that highlights the previous studies related to academic libraries, library needs for IS and ISec, types of ISec threats, sources of ISec threats, ISec measures, security assessment models, criteria and packages, studies on ISec frameworks and empirical studies on ISec. The discussion is comprised of the setting-up of concept, variables, terminology used and findings.

Chapter Three outlines the research design and methodology used in answering the research questions and testing the hypotheses, the research approach, sampling design, questionnaire development, data collection and methods of data analyses. Chapter Four

reports the descriptive statistical profiles of perceived ISec threats, their frequency of occurrences as well as the origin of these security incidents experienced by the participating academic libraries. Chapter Five presents the level of implementation of technological measures, organisational measures, the assessment tool, the overall implementation status and results of hypotheses testing. Chapter Six provides the discussions on the results, limitations, implications, future research directions and conclusion.

1.7 Summary of the Chapter

This chapter mainly provides the background of the subject and states the problem and issues leading this study. A brief review of literature about the problem was covered in order to highlight the deficiencies in current literature and identify the gaps to be addressed by this study. Two gaps were identified. One, limited empirical studies on ISec in libraries were the major motivation of this study. Two, the present challenges faced by Malaysian academic libraries in terms of security threats associated with IS also led to the interest to assess the technical and organisational approaches adopted by these libraries. The study used academic libraries as the object of the study. This study was designed based on the Organisational Information Security Staircase Model (Hagen, Albrechtsen and Hovden, 2008) and proposed additional measures for each step to assess the implementation of technological and organisational ISec measures in the library.

Basically, this study explored the types of Isec threats faced by Malaysian academic libraries as well as assessed the level of implementation of technological and organisational measures deployed by these libraries to ensure the security of their IS. In

addition the study also examined the differences in applying the technical and organisational measures due to the selected academic libraries' demographic profiles.

This chapter also put forward the structure of the whole thesis which features six chapters. The subsequent chapter presents a literature review for the pupose of relating to other ISec related studies and paving the way towards filling in the knowledge gaps and establishing the research framework.

Chapter Two

Literature Review

2.0 Introduction

The review of information security (ISec) literature relevant to this study involved two categories; conceptual papers and research studies. The review in this chapter is derived from documentations and literature from the ISec or ISec practitioners and the scientific community. The subsequent review is an attempt to gain some insights on the threats related to ISec in any organisations and their ISec approaches in order to highlight some gaps in the knowledge. The threats and the types of security countermeasures identified will also be used by the researcher to construct the items for the questionnaire and the assessment instrument.

The literature from the scientific community originated from four branches of knowledge domains, which are the information system or management information system, software engineering, computer science and mathematics (Siponen, 2001). However, engineering knowledge such as the system dynamic is also known to contribute to the progress of ISec (Saunders, 2001). From these five branches of knowledge domain, the practitioners and scientific community alike have produced standards, methodologies, models and theories that are relevant to ISec mainly through five different ISec disciplines. They are the information system (IS) security, computer security, database security, cryptology and management system (Suhazimah, 2007).

A comprehensive literature review reveals that this research is the first of its kind in Malaysia which focuses specifically in the library settings. Even though some attempts have been made to understand the types of computer threats targeted on health industries, banking industries, public governments and in public workplaces. It is unfortunate that there is still (to the authors' knowledge) no research that pays attention to the ISec landscape in the library areas. Realising the lack of research in these areas and with the intention to close the gap between findings from other areas and the library areas, the researcher will conduct an exploratory study enabling the development of a comprehensive view regarding the current status of the ISec threats in Malaysian academic libraries. Furthermore, this research also highlights the types and the status of ISec countermeasures that are being adopted by these libraries.

2.1 Defined Information, Security, Information Security (ISec), Information Security Management (ISM) and Information Systems (IS) Security

2.1.1 Information

Information includes both in electronic and physical forms such as paper, electronic, video, audio, voice or knowledge.

2.1.2 Security

A number of computing researchers and practitioners have attempted to define security in various ways. Here are some definitions that researcher thinks are generic enough to stand the test of time. Security based on computer system security perspective is a

branch of technology known as ISec as applied to computers and networks. It refers to the collective ways and processes by which information, property and services are protected from theft, corruption or natural disaster, while allowing them to remain accessible and productive to its intended users (Wikipedia, 2010). The essence of Volonino and Robinson's (2004) work defines security in the context of IT and electronic commerce as 'the policies, practices and technology that must be place for an organisation to ensure the safety of all online activities, transmissions and storage via its network'. In this study, security is generally referred as any technological and managerial procedures applied to a library to ensure the availability, integrity and confidentiality of information managed by the library IS.

2.1.3 Information Security (ISec)

There are various definitions of ISec in the literature. United States Code (2008) defines ISec as protecting information and IS from unauthorised access, use, disclosure, disruption, modification or destruction in order to provide:

a. integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity;
b. confidentiality, which means preserving unauthorised restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
c. availability, which means ensuring timely and reliable access to and use of information.

Other definitions are linked to the roles of ISec for an organisation which include the following functions (Whiteman and Mattord, 2009):

a. Protect the organisation's ability to function,
b. Enables the safe operation of applications implemented on the organization's IT systems,
c. Protects the data the organisation collects and uses, and
d. Safeguards the technology assets in use at the organisation.

In this study, ISec is referred as 'a combined set of measures at the physical, personnel, administrative, computer and information system levels' (INTOSAI, 1995). This definition highlights that ISec is a good management control and shortcomings at any level can threaten the security at other level as shown in Figure 2.1

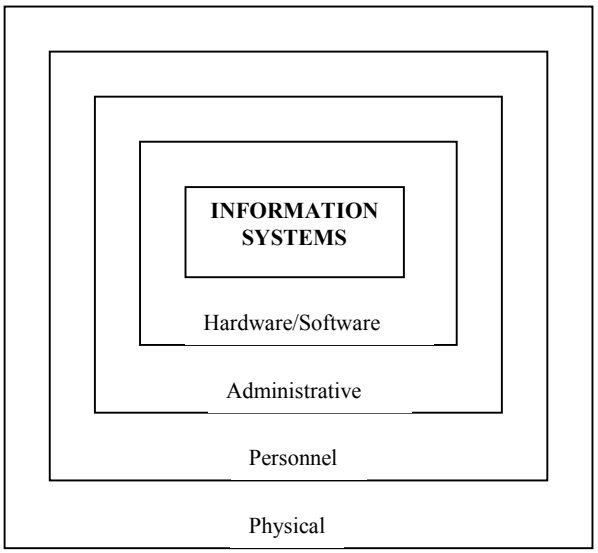


Figure 2.1: Complementary Layers of Information Security (INTOSAI, 1995)

Dlamini, Eloff and Eloff (2009) elaborate in great details the ISec changes started from the era of mainframe computers up to the current state of the complex Internet technology. Based on their article, researcher attempt to summarise the major trends and issues of ISec within the various era and the summary is presented in Table 2.1:

Table 2.1: Information Security (ISec) Trends and Issues

Era	Trends and Issues
• When human beings started learning how to write. • When information began to be transmitted, stored and processed. • 1840s: Invention of telegraph • 1841: Invention of telephone	• Used of a secret code to protect confidentiality of messages sent from a person to another person. • Used of an encryption code to safeguard the secrecy of the transmitted telegrams. • Legislation prohibiting wiretapping via telephone. • Concerned on protecting the secrecy or confidentiality of transmitted data and information.
• 1940s-1950s: existence of the 1s^{t} generation computers. • Existence of the of mainframe computers.	• Only the privileged computer operator (one user one computer) was permitted to use the mainframe computers. • Concerned on protecting the physical computers and the storage media from being stolen or damaged by outsiders.
• The late 1960s-the early 1970s: the beginning of dumb terminals.	• Enabled users (multiple users – one computer) to access and use remote data. • Concerned on protecting the data from unautorised users or outsiders by using security officers, identification and authentication process. • No security policies in place to enforce the use of strong passwords and to prevent password cracking or password sharing. • Guest and anonymous logins were allowed without thorough identification and authentication process but access restricted to only limited resources within the network.
• The era of mini computers. • The beginning of networks, time-sharing and multi-user systems. • The early 1970s: Existence of public key cryptography. • The late 1970s-early 1980s: Existence of digital signatures.	• Used of access controls to prevent users from interfering with one another's workspace. • digital signatures from around the late • Concerned for data integrity

(Source: Dlamini, Eloff and Eloff, 2009)

Table 2.1: Continued.

• 1980s -–introduction of personal computers • The late 1980s- introduction of anti-virus software.	• Companies began to automate their operations. • The rise of computer viruses which spread through the use of diskettes. • The USA government issued the Computer Fraud and Abuse Act of 1984 to prosecute and establish penalties for creators and authors of computer viruses. • The USA government issued the Computer Security Act of 1987 to deal with trainings for security personnel who involved in the processing of sensitive information.
• The 1990s – innovation of open systems and mobile computing. • End of the 1990s- introduction of filtering firewalls.	• More personal computers connected to the Internet. • The rise of computer viruses, worms and script kiddies attacks. • The introduction of distributed denial of services and malicious codes attached to emails and web pages.
• The 21s^{t} century- era of pervasive computing (IT infrastructure became pervasive because everything had gone electronic). • Innovation of computer- like-devices (e.g. Personal Digital Assistants, Smart phones, Laptops, Tables PCs, etc.) • The emerging of mobile computing (Bluetooth and Wi-Fi)	• Attackers become more sophisticated and started hacking for financial gains. • The rise of online payment systems and the usage of credit cards. • The rise of ISec threats like identity theft, social engineering, phishing and etc. • Concerned for non-repudiation issues. • The evolution of spam and phishing to SMS (short message service) and MMS (multimedia message service) technology in mobile phones.

(Source: Dlamini, Eloff and Eloff, 2009)

From the summary it can be concluded that, as the technology evolved and became more advanced, the security landscape also changed and became more complex. Thus, ISec will remain a challenge for all types of organisation including libraries.

2.1.4 Information Systems (IS) Security

The main components of information system (IS) are software, hardware, data (or databases), people (or human resources), procedures and networks (or telecommunication systems) (Encyclopedia Britannica, 2009; Whiteman and Mattord,

2009). Thus, IS can be referred as the entire infrastructure, organisation, personnel and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information (National Security Telecommunications and IS Security Committee, 2000). In this study, IS security refers to any activities that relates to 'the protection of IS against unauthorised access to or modification of information, whether in storage, processing, or transit, and against the denial-of service to unauthorised users or the provision of service to unauthorised users, including those measures necessary to detect, document and counter such threats' (National IS Security, 1992).

2.1.5 Information Security Management (ISM)

Information security management (ISM) in the context of library management describes controls that a library needs to implement to protect its information assets from all potential threats to ensure the confidentiality, integrity and availability of its information resources.

2.2 Academic Libraries

In Malaysia, every university has its own library and this library comes under the jurisdiction of the respective universities (Badilah, Shahar and Chew, 1996). As compared to other types of libraries such as school libraries, special and public libraries, academic libraries in Malaysia have larger collections, larger number of staff and patrons, received more fund and were pioneers in the use of the Internet and web sites (Lee and Tthe 2000). The population of academic libraries at the public universities, private universities and college universities in Malaysia is explained in details in Chapter 3. These academic libraries also have a variety of services when compared to other types of libraries. Especially in today's networked online environment, these libraries exploited all forms of technologies and found new means to provide feasible

form of collections, services and access to library materials (Foo, et al., 2002). As indicated by Rajendran and Rathinasabapathy (2007), academic libraries held collections in the form of physical, electronic and digital to fulfill the knowledge requirements of students, faculty members, research scholars and scientists of the academic institutions. Access to these digital collections should be given through computer networks, local area networks, wide area networks or the Internet. Clifford (2000) highlighted how the advances of IT has profoundly changed and transformed all aspects of higher education, scholarship as well as academic libraries. The summary of the changes that IT played within the various automation phases in academic libraries is displayed in Table 2.2.

Table 2.2: Changes in Academic Libraries due to IT developments

Automation Phases	**Era**	**Changes**
The First Automation Age: Computerising Library Operations	late 1960s or early 1970s	• Automated library processes by locally developed or commercial systems. • Automated circulation system by using minicomputers (stand alone system). • Bar-coded books. • Computer-based ordering systems. • The conversion of automated circulation system from the first system to the second system.
	early 1980s	• Development of shared copy-cataloging systems within the library community by using computers and computer networking. • Retrospective conversion programs for older books and materials.
The Second Automation Age: The Rise of Public Access	1980s-early 1990s	• The library system became reliant on campus networking strategies. • Central databases of collective holdings of the major research libraries. • Machine-readable bibliographic records by individual libraries. • Online public access library catalog as a replacement for the card catalogs. • The growth of library consortia or a group of libraries that wanted to work together. • Development of union catalogs by consortia to promote virtual resource sharing. • The availability of online catalogs, electronic mails as well as abstracting and indexing databases. • The development of computer-assisted interlibrary loan systems that built on the shared national union catalog databases.

(Source: Clifford, 2000)

Table 2.2: Continued.

The Third Automation Age: Print Content Goes Electronic	late 1980s and early 1990s	• The emergence of the Web services. • The library system is critically dependent on both local-area and wide-area networks. • Easier and faster electronic content delivery (e.g. in bitmaps, Adobe PDF, ASCII text and later HTML formats). • Publishers and aggregators began to offer one-stop" databases to libraries. • Proliferation of online journals. • Web-based search engines became very popular among library patrons compared to online library catalogs. • Libraries started to digitise specialised materials (e.g. manuscripts, photographs, maps and other unique works) and made them publicly available on the Web.

(Source: Clifford, 2000)

2.3 Library Needs for Information Systems and Information Security

Library Information System (LIS) encompasses both mature and new developments, including Integrated Library Systems (ILS), online databases, web-based resources, digital library collections and resources (Kochtanek and Matthews, 2002). There are various factors why libraries need IS.

Firstly, the explosive growth of the Internet and its demands for connectivity require the additional external connections which has lead to the creation of a large number of remote users (Pipkin, 2000). These users include employees who need remote access and direct network connections to remote office. Therefore more libraries utilise the IS to assist them in providing digitally delivered services and collections to local and remote patrons. Secondly, to manage a library as an information centre requires a system which can process all forms of information materials in order to provide the right and accurate information to the right patron at the right time. Akintunde (2004), indicated that the library uses information and technology communication (ICT) in several ways including for managing the library administration; processing of library materials; developing and accessing online resources; developing and accessing offline

resources; as well as providing service to patrons. Therefore, IS are crucial for libraries that were highly information-intensive or relied heavily on IS.

However, the increased connectivity of IS to the outside world via the Internet has changed the risks associated especially when they are connected without proper security measures. Jung et al. (2001) observed that the threats associated with the Internet varied among industries according to the needs of the organisation for information availability, confidentiality and integrity. For instance, the libraries need to be concerned with issues related to reliability, durability and accessibility when they are relying heavily on digital content, partnering in distance education, creating in-house databases and addressing technical challenges (Cline, 2000). As highlighted by Bruhn, Gettes and West (2003), key components of a security plan consists of a well managed access to services that protect online resources and user privacy while enabling ease of use. This is because IS and networks are often inherently insecure since they are designed with functionality not security as its primary goal (Gawde, 2004).

Breeding (2003), argued that the only way to guarantee the security of a computer is to keep it unplugged from any network, but this is not a practical option as libraries main role involves providing access to information**.** Even without a direct Internet connection, libraries are still exposed to risks because of the widespread use of laptops and portable storage devices (such as USB drives) by the library staff and patrons. When these devices are plugged into inadequately protected library computers, the data on these unprotected computers can be easily stolen, damaged or changed by the attackers (Ryoo, Girard and Charlotte, 2009).

Other reasons are related to the increasing complexity of security when technology and computer systems are more prone to have security holes. For instance, prior to 1988, criminal activity was mainly centered on unauthorised access to computer systems and

network owned by the telephone companies which provided dial-up access for unauthorised users (Conklin, et al, 2005). In today's highly network world, threats become more widespread and increasingly sophisticated. As a result, libraries are becoming more vulnerable than they were before (Pipkin, 2000). Table 2.3 illustrates the changes in computer systems over time.

Table 2.3: Changes in Computer Systems

Era	System	Risks	Controls
1960s-1970s	Teleprocessing, single central processor with local or remote terminals	• Internal fraud • Tapping of remote • Disaster, manmade or natural	• Hiring practices • Encryption • Fire and flood protection • Off-site data storage
1970s-1980s	Distributed, multiple computers interconnected	Same as above, plus… • External access • File and program corruption • Data theft	Same as above, plus… • Programs and files of record • Audit trails and mirror images • Access and incursion logs
1980s-1990s	Integrated IS, multiple computers with a common operating system and database access	Same as above, plus… • Illegal database access • Incompatibilities • Version differences • Database inconsistencies	Same as above, plus… • Access controls • User authentication • Software and configuration control
1990s-2000s	Client/server computing, multiple computers with local or remote network connections	Same as above, plus… • Hacking • Vandalism • Virus • Denial of service • Data change	Same as above, plus… • Antivirus software • Access control • Firewalls • Public key infrastructure
2000s-2010s	A worldwide system of computer networks (Cloud computing applications) with Virtual Machines (VMs) which users are able to access applications and data from a ``Cloud'' anywhere in the world on demand.	Same as above, plus… • Malware and malicious attacks • Spam and phishing • Data leakage • Identity thefts • Web insecurity	Same as above, plus… • Endpoint security (Combination of antivirus software, antimalware software and a virtual system) • Two-factor authentication • Advanced biometric scanner • Wireless Device Control • Data Recovery Capability • Internet filtering

(Source: Pardoe and Snyder, 2005)

The libraries need for ISec is paralleled with the increased of awareness of the relevance and importance of ISec in an organisation. Loch, Carr and Warkentin (1992) have reported that management's concern with ISec has changed over recent years. They also revealed that the ISec remained high on the list of key issues faced by an organisation although the management believed either that security was less an issue or they had implemented greater control. Besides the above reasons, libraries also need adequate ISec measures in order to protect and minimise the likely consequences of the potential damages due to ISec risks. Williams (2001); Farahmand, F. et al. (2003); Bakari et. al., (2005); and Dlamini, Eloff and Eloff, (2009) have listed various potential damages related to ISec risks such as:

a. Loss of data and library services due to accidental or malicious deletion or alteration of data residing on library network servers;
b. Loss of time reconfiguring workstation settings, recovering from the users' mischief and responding to system resulting from unauthorised use of systems;
c. Loss of funding and need extra costs due to maintain computerised library systems and library networked services;
d. Loss of reputation, credibility, confidence or potential for embarrassment by staff and patrons from the effects of web pages defaced, examination leakages, tampering with examination records or library records;
e. Infringement of privacy or copyrights; and
f. Loss of ability to meet the requirements of regulators.

Unlike almost any other profession, librarians are expected to fulfill their patrons' informational needs without question or bias. This laudable goal makes librarians vulnerable to ISec threats such as social-engineering attacks because the reference inquiries made by a patron about the IS resources available at a library may be used for nefarious purposes (Thompson, 2006). Libraries desperately need to protect their ISec due to limitation of librarians or staff to monitor security as they are often challenged with demands to increase their productivity and improve customer service (Yong, 2008). As reported by Breeding (2003), libraries often do not have full-time systems administrators and security specialists to take charge of IS security. This situation is

worsening when libraries deploy Windows servers without an adequate level of technical administration by competent systems administrator, as these operating systems are more prone to the latest virus and worm attacks (Breeding, 2003). Furthermore, insufficient funding and budget for improving the IS security adding more worries to the libraries' management. This is because much of the value of a library main business or services is concentrated in the value of its IS.

2.4. Types of Information Security Threats

An essential step in security planning is to understand what the organisation needs to protect, before it plans relevant security measures to defend against those threats. That requires an awareness of the possible threats, vulnerabilities and security issues confronting an organisation's hardware, applications, data, computer systems and networks.

In general, security threats refer to any security incidents that can directly or indirectly lead to system vulnerabilities (Baskerville, 1996; Cohen, 1997; Loch et al., 1992). Threats become more specific when discussed in the context of vulnerabilities and attacks (Slade, 2006). Vulnerability refers to weaknesses in hardware, software or people that expose a computer or user to an exploit or a threat (Volonino and Robinson, 2004). Vulnerabilities can be located in hardware, software, infrastructure and processes (Pipkin, 2000). A threat itself does not harm a system, but a successful attack does. An attack is an act that tries to bypass security controls and also known as a realisation of a threat (Slade, 2006). Specifically, an information system (IS) threat refers to a danger posed by an IS vulnerability which can actually lead to undesirable consequences (Neumann, 1995 in Im and Baskerville, 2005). For instance, natural disasters and human errors create vulnerabilities that can be exploited and lead to security problems.

In the early days of computing, security breaches mainly included viruses and worms that would flash a message or advertisement on the screen without causing any serious damage to the information or systems being used (Dlamini, Eloff and Eloff, 2009). Nowadays, attacks are becoming more complex and sophisticated as technologies changed. Following Maiwald's (2004) explanations, Table 2.4 specifies how ISec services are used in an organisation including a library depend upon proper security planning to combat the attacks shown in table below.

Table 2.4: Information Security Services vs. Attacks

Attack	*Security Service*			
	Confidentiality	*Integrity*	*Availability*	*Accountability*
Access	**x**			**x**
Modification		**x**		**x**
Denial of service			**x**	
Repudiation		**x**		**x**

(Source: Maiwald, 2004)

Researchers and authors presented variety of approaches to identify various kinds of security threats. For instance, Loch et al. (1992) carried out a survey to explore the perception of Management IS (MIS) executives regarding the security threats in microcomputer, mainframe computer and network environments. They developed a list of twelve security threats and empirically examined them. The results indicated that natural disasters, employee accidental actions (such as entry of bad data and destruction of data), inadequate control over media and unauthorised access to the accounting IS by hackers had been ranked among the top security threats. Davis (1996) replicated Loch et al.'s study to discover the current status of the security issue in practice among information system auditors. The results revealed that employees' accidental entry of "bad" data, the accidental destruction of data and the introduction of computer viruses were considered as the three top threats in a microcomputer environment. In contrast,

technology advances faster than control practice were said to be the most important threats in network computer environment.

Ryan and Bordoloi (1997) explored how companies moving from a mainframe to a client or server environment evaluated and took security measures to protect against potential security threats. They found several significant security threats such as: a) accidental destruction of data by employees; b) accidental entry of erroneous data by employees; c) intentional destruction of data by employees; d) intentional entry of erroneous data by employees; e) loss due to inadequate backups or log files; and f) natural disaster (fire, flood, loss of power, etc).

Pipkin (2000) identified several forms of threats including human errors, system failures, natural disaster and malicious acts. Centers for Medicare and Medicaid Services (CMS) (2002) has categorised the threat resource for the CMS information systems (IS) into four main groups including; 1) environmental or physical threats; 2) human threats; 3) natural threats; and 4) technical threats. Based on the occurrence and significance in the current CMS environment, they also have divided the threats affecting major applications and other systems into human and technical threats. Whereas, the general support systems are subject to environmental or physical, human, natural and technical threats. Table 2.5 lists the comprehensive index of threats that might occur and the likely effect they could produce to the system confidentiality, integrity and availability. Carelessness, user abuse, theft, sabotage, vandalism or physical intrusions are identified as the major human threats which can jeopardise confidentiality, integrity and availability of IS. Whereas, the major technical threats to information systems' confidentiality, integrity and availability include technical intrusion, unauthorised access to system resources, insertion of malicious code,

database modification, system corruption, system errors, installation errors and misrepresentation of identity.

Table 2.5: Index of Threats to Major Applications, Other Systems and the General Support Systems

a) Threats to Major Applications and Other Systems				
Threat Category	**Threat**	**Threat effect**		
		Confidentiality	**Integrity**	**Availability**
Human	Inadvertent Acts or Carelessness	√	√	√
	User Abuse or Fraud	√	√	√
	Impersonation	√		
	Theft, Sabotage, Vandalism or Physical Intrusions		√	√
	Espionage	√		
	Shoulder Surfing	√		
	Data Entry Errors or Omissions		√	
Technical	Misrepresentation of Identity	√		
	Intrusion or Unauthorised Access to System Resources	√	√	√
	System and Application Errors, Failures and Intrusions not Properly Audited and Logged		√	√
	Data/System Contamination	√		
	Eavesdropping	√		
	Insertion of Malicious Code, Software or Database Modification	√	√	√
	Takeover of Authorised Session	√		
b) Threats to General Support Systems				
Environmental	Environmental Conditions		√	√
	Electromagnetic Interference		√	√
	Hazardous Material Accident			√
	Physical Cable Cuts			√
	Power Fluctuation			√
Natural	Natural Disaster			√
	Secondary Disaster			√
Human	Improper Disposal of Sensitive Media	√		
	Shoulder Surfing	√		
	Inadvertent Acts or Carelessness	√	√	√
	Omissions	√	√	√
	Scavenging	√		
	Theft, Sabotage, Vandalism or Physical Intrusions	√	√	√
	User Abuse	√	√	√
	Espionage	√		√
	Terrorism		√	√
	Arson			√
	Procedural Violation			√
	Riot/Civil Disorder			√

(Source: adapted from CMS Information Systems Threat Identification Resource, 2002)

Table 2.5: Continued.

b) Threats to General Support Systems				
Technical	Data/System Contamination	√	√	√
	Compromising Emanations	√		
	Corruption by System, System Errors or Failures	√	√	√
	Eavesdropping	√		
	Misuse of Known Software Weaknesses	√	√	√
	Insertion of Malicious Code, Software or Database Modification	√	√	√
	Installation Errors	√	√	√
	Intrusion or Unauthorised Access to System Resources	√	√	√
	Misrepresentation of Identity/Impersonation	√	√	√
	Hardware / Equipment Failure		√	√
	Saturation of Communications or Resources		√	√
	Tampering		√	√
	Jamming (telecomm)			√

(Source: adapted from CMS Information Systems Threat Identification Resource, 2002)

Gawde (2004) revealed the danger of using applications such as real-time streaming media players, instant messaging (IM) clients and peer-to-peer (P2P) networks over the Internet by employees to perform online chatting, playing interactive games and surfing non business related sites such as pornography, entertainment and even web based personal email. These activities contribute to productivity drainer as well as lost of confidential information through instant messaging or emails.

Conklin, et al. (2005) outlined three possible ways to break down the various types of threats. Firstly, to categorise based on the internal or external sources of threats in an organisation. Secondly, to categorise based on the various level of sophistication of attacks, from those by “script kiddies” to “elite hackers”. Thirdly, to examine the level of organisation of the various threats, from unstructured threats to highly structured threats.

Bishop (2005) described Shirey's threat classification scheme which divides threats into four broad groups: 1) disclosure (unauthorised access to information); 2) deception (acceptance of false data); 3) disruption (interruption or prevention of correct operation); and 4) usurpation (unauthorised control of some part of a system).

Ahmad (2005) carried out an empirical survey to investigate the significant perceived computerised accounting IS security threats (CAIS) in Saudi environments. Four hundred questionnaires were randomly distributed to different types of Saudi organisations including manufacturing companies, banks, insurance companies, retail merchandising, oil and gas companies, services companies, health care and government units. The respondents were asked to indicate the frequency of occurrence of each security threat based on five available choices (less than once a year, once a year to monthly, once a month to weekly, one a week to daily and more than once a day or more frequently). The findings revealed that a) accidental and intentional entry of bad data; b) accidental destruction of data by employees; c) employees' sharing of passwords; d) introduction of computer viruses to CAIS; e) suppression and destruction of output; f) unauthorised document visibility; and g) directing prints and distributed information to unauthorised users are the most significant perceived security threats to CAIS in Saudi organisations.

Farahmand et al. (2005) designed a comprehensive model for threat classification and control measures to a network system from three points of view, namely the threat agent, threat technique and security measure (Figure 2.2). They conducted case studies and interviewed six ISec experts dealing with security issues. They identified threats to IS of organisations such as theft of proprietary or disclosure of information, virus or worm attacks and denial of service attacks.

Figure 2.2: Combination of agents, techniques, and security measures to a network system (Source: Farahmand et al., 2005).

Similarly, Im and Baskerville (2005) also believed that intentional security threats such as hacking, computer viruses and computer theft are becoming a more severe problem in relation to other security vulnerabilities. In contrast, Olayemi (2005) classified threats to computer and network security into four groups: (a) Physical threats, (b) Accidental error, (c) Unauthorised access and (d) Malicious misuse.

Kimwele, Mwangi and Kimani (2005) reported that 76.2% of respondents had suffered ISec breaches in Kenyan small and medium enterprises (SMEs). The breaches experienced by them included: a) Inadvertent breach (e.g. user accidentally deleted files or changed computer configuration); b) Deliberate attack (e.g. hacker or disgruntled staff gained access, deleting or stealing data); c) Asset theft (e.g. software application misplaced causing re-installation delay); d) Equipment failure (e.g. hard drive crashed causing loss of data and business disruption); e) Back up failure (e.g. system restore failure due to corrupt or inadequate backups); f) Data theft (e.g. espionage which resulted in data loss and possible legal exposure); g) Site disaster (e.g. fire or flood causing damage to systems and business disruption); h) Copyright infringement (e.g.

staff loading pirated software); and i) Compliance (e.g. passing on confidential information).

Unisys (2007) provided insights on the security index among Malaysian community towards different types of security issues. Based on a nationally representative sample of 903 respondents in Peninsular Malaysia aged 18 to 64, the results revealed that 52% of Malaysians or 5.9 million people were very or extremely concerned about computer security in relation to viruses and unsolicited emails. The survey also found that majority of Malaysians (77%) or 8.7 million people were very or extremely concerned about unauthorised access to or misuse of their personal information.

CLUSIF (2008) conducted an in-depth evaluation of Internet users' perception on computer threats and risks in France. Findings revealed that the dominant fears among Internet users were viral infections (86%), spyware (80%), intrusion (71%), spam (67%), phishing (67%), identity theft (65%), WiFi hacking (54%) and equipment breakdown (46%).

Trend Micro White Paper (2009) highlighted the disadvantages of Web 2.0 technologies in providing an additional threat vector to organisations. Web 2.0-based sites, such as Facebook.com, act as a platform for third-party developers to create powerful, scripted applications that can access user account details and execute within a browser window.

Nachtigal (2009) categorised attack categories based on the most widely discussed classes of attack, motives of attackers, attack techniques and consequences of attacks (Table 2.6). She also indicated that attacks are typically not associated with just one threat category but may implement multiple threats.

Table 2.6: Summary of List of Attack Categories

Attack Categories			
a) Classes of attack	b) Motives and objectives of the attackers	c) Attack techniques	d) Consequences of attacks
• Malware (Viruses, worms, Trojans and Spyware • Denial of service • (DoS or DDoS) • Social engineering • Insider attacks • Impersonation attacks • Hacking • Exploitation of implementation errors	• Harassment • Cyber terrorism • Political or industrial net espionage	• Buffer overflow • SQL injection • Spamming • Packet sniffing • Spoofing/masquerade • Abuse of cookies • Routing table poisoning • Phishing • SMiShing • vishing; • DNS (Domain Name System)	• Software corruption/modification; • Hardware malfunction; • Data corruption/modification/exposure/ • theft; • Identity theft; • Intellectual property theft; • Financial loss; • Damage to reputation; • National-level infrastructure disaster.

(Source: Nachtigal, 2009)

Samy, Rabiah and Zuraini (2009) examined the various types of threats that exist in IS in one of government supported hospital in Malaysia. Based on data collected from three different departments using in depth structured interviews, they identified 22 types of threats according to major threat categories based on ISO/IEC 27002 (ISO 27799:2008). They also revealed that power failure, acts of human error, technological obsolescence, hardware failures and software failures as the most critical threats for the Total Hospital Information System (THIS). This research holds significant value in terms of providing a comprehensive list of potential threat categories in IS and subsequently taking the results of this step as input for the risk mitigation strategy (see Table 2.7).

Table 2.7: Threats to a Total Hospital Information System (THIS)

No.	Potential Categories of Threat in THIS	Description
1.	Power failure/loss	• Server down due to power failure • Air-conditioning failure of the server • Interruption by service provider (e.g. electrical department and Internet service provider)
2.	Network Infrastructure failures or errors	• Connection failure • Unsecured wireless network • Network software failure • Network congestion • Switch port problems • Routers or switches hang
3.	Technological Obsolescence	• Outdated hardware • Outdated application software • Outdated system software • Obsolete network equipment
4.	Hardware failures or errors	• Insufficient storage space • Hardware maintenance error
5.	Software failures or errors	• Application software failure • Software maintenance error
6.	Deviations in quality of service	• Minimum technology of transfer (TOT) from contractors and technology vendors
7.	Operational issues	• Lack of training for staff • System documentation not systematically managed • Inadequate knowledge/skill by staff
8.	Malware attacks (Malicious virus, Worm, Trojan horses, Spyware and Adware)	• Embedding of malicious code due to the usage of wireless and mobile technologies • Introduction of damaging or disruptive software
9.	Communications interception	• Spoofing/impersonation due to unsecured network
10.	Masquerading	• Insiders • Service providers • Outsiders
11.	Unauthorised use of a health information application	• Outsiders • Insiders
12.	Repudiation	• Repudiation by staff
13.	Communications infiltration	• Hackers due to unsecured network
14.	Social Engineering attacks	• Gaining access to confidential information through social interaction by outsiders
15.	Technical failure	• Technical failure of the host or storage facility
16.	Deliberate acts of Theft (including theft of equipment or data)	• Deliberate acts of theft by outsiders • Deliberate acts of theft by insiders
17.	Misuse of system resources	• Misuse of confidential information (patients data) by staff • Misuse Internet access by staff

(Source: Samy, Rabiah and Zuraini, 2009)

Table 2.7: Continued.

18.	Acts of human error or failure	• Entry of erroneous data by staff • Accidental deletion or modification of data by staff • Accidental misrouting by staff • Confidential information being sent to the wrong recipient • Storage of data/ classified information in unprotected areas by staff
19.	Staff shortage	• Technical and non-technical staff
20.	Willful damages	• Outsiders • Insiders
21.	Environmental support failure/natural disasters	• Fire at the server • Water damaged at the server • Lightning attacks • Earthquake
22.	Terrorism	• Terrorist attacks

(Source: Samy, Rabiah and Zuraini, 2009)

As numbers and types of IS threats are constantly growing, therefore it is not possible to present a complete list of threats. However, the researcher believes that those available taxonomies and classifications of threats, although have addressed the most important threats for general security or specifically to computer and network security threats, either do not cover all of them in the current library perspectives. Therefore, based on the relevant literature above researcher will attempt to assess the current IS security threats in libraries and present a potential category of the general IS security threats in a library setting.

(a) Hardware Security Threats

Hardware, form as a physical component in an information system is also prone to security attacks. Previous study results (Ke, 1997; Lin and Huang, 1999; and Shen, 1999) revealed several factors that jeopardise hardware security including: a) Natural disasters such as earthquakes, fires, floods and thunder strokes; b) Changes in temperature or humidity; c) Accidents, such as stealing and vandalism; d) Malicious intrusion and destruction; and e) Defects of the hardware itself, such as bugs or errors generated from routers or firewalls; f) Faults in the manufacture of the equipment;

g) Air-conditioning failure; and h) Loss of essential services such as telecommunications or power. Other hardware security threats include electromagnetic interference, failure of communication equipments and services, hardware equipments failure, installation of unauthorised hardware, maintenance errors, physical sabotage or intentional destruction of computing equipments, theft, physical sabotage and vandalism of ICT hardware equipments.

Farahmand, et al. (2003) indicated that hardware attacks can be mounted against hardware for the purpose of using the hardware as a means of denying use of the system. These may include a physical attack against the equipment, a bug implanted within the hardware or an attack against the supporting utilities. Computer hardware infected with malware (i.e. computer viruses, worms and Trojan horses) may suffer some sort of damage such as making it impossible to boot the computer, repeated error messages, hardware malfunctions and lowered the computing speed.

(b) Software Security Threats

In terms of jeopardising software security, the threats can be divided into operating systems and related applications. Security threats associate with operating systems might include the security loopholes due to improper design and improper management. Whereas, software security threats related with applications include stealing or copying software from the Internet which might contain viruses (Shen, 1999). Computer software infected with malware (i.e. computer viruses, worms and Trojan horses) may suffer some sort of damage such as periodically automatic reboots, program crashes or malfunctions, repeated error messages and poorer system performance or unusual behavior.

Other software security threats include corruption by system, system failure, maintenance errors, cyber-terrorism, software piracy, unauthorised access, unauthorised changes to software settings, adware, spyware, hacking, password sniffing, weak passwords and abuse of computer access control. Farahmand, et al. (2003) reported that software attacks can range from discreet alterations to less discreet changes. They indicated that for the discreet alterations, attacks are subtly imposed for the purpose of compromising the system. In contrast, for the less discreet changes, attacks are intended to destruct of data or other important systems features. There are several software security threats that could jeopardise software security such as follows:

i. Abuse of computer access control refers to employees or patrons abusing their access controls rights and privileges for personal reasons or to obtain more data than needed for their jobs;
ii. Adware and Spyware is a type of malware that can be installed on computers to collect information about users without their knowledge. Specifically, adware is used as a marketing tool to monitor people's behaviour on the Internet, to determine which products they are interested in. Whereas, the functions of spyware extend well beyond simple monitoring. Spyware programs can change computer settings, resulting in slow connection speeds and loss of Internet connection or functionality of other programs;
iii. Corruption by system, system errors, or failure of system software. According to Laprie et al. (1992) “a system failure occurs when the delivered service no longer complies with the specifications". Whereas, an error is defined by Laprie et al. (1992) as that part of the system which is liable to lead to subsequent failure, and an error affecting the service is an indication that a failure occurs or has occurred. If the system comprises of multiple components, errors can lead to a component failure. As various components in the system interact, failure of one component might introduce one or more faults in another;
iv. Hacking refers to unauthorised attempts to bypass the security mechanisms of an information system or network either skilled or unskilled persons.
v. Intrusion refers to unauthorised access to system resources such as public access workstations to obtain unauthorised access to resources and can cause damage or loss of data;
vi. Installation or use of unauthorised programmes or software can cause security threat as it associated with the risk of introducing viruses and other unwanted risks into the public-access and administrative library computers. Malicious software can be accidentally or intentionally installed on computers from portable drives, email accounts and web browsing. Allowing these programs to run on workstations presents a serious challenge to the IT administrator’s as

vii. Internet threats such as malicious code, Trojans and spyware could make desktop vulnerable to leakage of important corporate information (Gawde, 2004);

viii. A password is also vulnerable to sniffing or stealing every time it sent across a network such as when users are using remote access to access computers, printers, databases, emails or Internet banking;

ix. The integrity, reliability, confidentiality and availability of the information processed by programme or software could be threatened if errors are made during the programme or software development, maintenance or installation process. For instance, Microsoft has released software which made systems vulnerable to security breaches such as Hotmail, Microsoft Outlook and Outlook Express software. Microsoft Outlook and Outlook Express software had a bug that could allow malicious code to run on a computer without the knowledge of the user and allow the hacker to use the user's access rights to reformat the disk drive, change data or communicate with other external sites;

x. The use of pirated or unauthorised software on the library network is illegal and places the library in danger of legal action by the software supplier. Thus, ensuring that the software on library computer systems is fully licensed is a responsibility of the IT personnel as f libraries are found to be in non-compliance, the consequences can be quite expensive;

xi. Unauthorised changes to software settings or to program code can be used to commit fraud, destroy data or compromise the integrity of a computer system. This would involve a manipulation of settings in the browser such as to delete history files, change security settings or enable private browsing. In order to prevent users from accidentally changing their system settings, a clear separation of functions between software programming staff and operational IT staff who implement all authorised changes should be made clear;

xii. Use of library Internet for illegal or illicit communications or activities such (e.g. porn surfing, e-mail harassment or porn surfing)

xiii. Cyber-terrorism refers to unlawful attacks and threats of attack against computers, networks and the information stored on cyberspace which can cause fear and violence against persons or property (Denning, 2000).

(c) Network Security Threats

Yeh and Chang (2007) reported that networks were rated as contributing the most severe among IS security threats but had the lowest level of protection among Taiwanese enterprises. Williams (2001) listed the most common network security threats in small libraries such as; a) Cracking of passwords; b) Damage to equipment or data due to lightning strike, surges or inadequate power; c) Internet based attacks of internal network resources; d) Local patron tampering workstation desktop and

hardware settings; e) Unauthorised access to workstation file systems, including installation of personal software; f) Unauthorised access to server file systems; g) Tampering local network infrastructure including network devices, network wiring, etc.; h) Defacement of library web pages if hosted on library-based web server; i) Theft of equipment; and j) Inadequate funding to operate, maintain and replace network equipment. Other network security threats that could threaten the network security include such as follows:

i. Denial of service attacks (DoS) prevents legitimate users from making use of a service and it can be very hard to prevent. The DoS attack may typically leads to service downtime and legitimate users losing confidence in the service or organisation;
ii. Eavesdropping or sniffing take places when an attacker uses software to monitors or listens to all traffic activities and interprets all unprotected data such as username password combinations, confidential emails, credit card numbers or reports. This type of software poses significant risk to the network as it can be used to capture the most sensitive network passwords and allow an attacker to do anything on the network (Farahmand, et. al., 2005);
iii. Internet Protocol (IP) spoofing attacks occur when a hacker steals an authorised IP address, which is a unique address for a node on a communication network. Typically, it is done by determining the IP address of a computer and waiting until there is no one using that computer, and then using the temporarily inactive IP address (Farahmand, et. al., 2005);
iv. Malware refers to computer viruses, worms, Trojans and any other kinds of malicious program designed to damage network equipment as well as cause disruption by deleting files or sending emails. Virus code can replicates by attaching itself to existing executables, whereas worms are programs that reproduce by copying themselves through computers on networks. Trojan horse refers to program that performs a desired task but also includes unexpected functionality (Mell, Kent and Nusbaum, 2005);
v. Accidental directing or re-routing of messages to the wrong person can lead to a loss of confidentiality and integrity if these messages are not protected and allowing unauthorised changes to be made prior to delivery to the original addressee;
vi. Password attacks exist when hackers find a user who has system privileges with an easy password to gain unauthorised access to the system (Farahmand, et. al., 2005);
vii. Session hijacking occurs when a hacker taps into a connection between a client and a server, then simulates the connection by using its Internet Protocol (IP) address (Farahmand, et. al., 2005);
viii. Probes and scans refer to unusual attempts to gain access or discover information about remote computers. Probes are sometimes followed by a more serious security event, but they are often the result of curiosity or confusion. Whereas, scans such as a port scan are often a prelude to a more directed attack on

systems that the intruder has found to be vulnerable (Eisenberg and Lawthers, 2005);

ix. Transmission errors may occur due to the failure of any of the network components that are used for the transmission of data. These errors can destroy the integrity and reliability of data and can lead to a loss of availability;

x. Website defacement is an attack usually initiate by a system cracker who breaks into a web server and changes the visual appearance of the website. Penetration and hacking of web sites is increasing due to the growth of virtual private networks and online business.

(d) Data Security Threats

Data security is the practice of protecting and ensuring privacy of personal or corporate data resides in databases, network servers or personal computers from corruption and unauthorised access. The ISO 7498-2:1989 (1989) document considers the threats to data as: 1) Destruction of information and other resources, 2) Corruption or modification of information, 3) Theft, removal or loss of information and other resources, 4) Disclosure of information; and 5) Interruption of services. There are several other threats that could jeopardise data security such as follows: a) Data diddling or changing of data before or during input into a computer system; b) Data loss due to wrong procedures of updating, storage or backup; c) Data manipulation; e) Delay in updating or dissemination; f) Destruction due to natural disaster; g) Exposure of patrons sensitive data through web attack; h) Impersonation or social engineering; i) Loss of patron data or privacy ideas; j) and Malware and Malicious code (e.g. virus, worm, Trojan horse, logic/time bombs and trapdoor); k) Masquerading of user identity; l) Password attacks, sniffing, stealing, phishing or pharming; m) Theft of proprietary data; n) Unauthorised access; o) Unauthorised data copying; p) Unauthorised transfer of data; and q) Unauthorised, accidental disclosure, modifications or alteration of data. Malware refers to computer viruses, worms, Trojans and any other kinds of malicious program designed to damage data by infecting open files and program libraries on an

operating system, deleting data and files in the hard drives, steal information and send it to third parties for illegitimate reasons.

(e) Physical Facilities and Environmental Threats

The most common problem of physical threats that must be factored into a security program includes natural disaster and theft. It has been reported that the relationship between physical threats and virtual threats is most apparent as both physical infrastructure and systems are needed to provide an access point to the virtual world (Lindstrom, 2003). Tittel et al. (2003) listed the most common types of physical threats including: 1) Fire and smoke; 2) Water (rising or falling); 3) Earth movement (earthquakes, landslides or volcanoes); 4) Storms (wind, lightning, rain, snow, sleet or ice); 5) Sabotage or vandalism; 6) Explosion or destruction; 7) Building collapse; 8) Toxic materials; 9) Utility loss (power, heating, cooling, air or water); 10) Equipment failure; and 11) Personnel loss (strikes, illness, access or transport).

Perhaps the most prevalent threat is the natural calamity caused by natural and man-made environmental problems. Computing equipments, physical infrastructure assets and data can be destroyed due to fire, floods, electricity spikes and power outages. Besides that, chemical, radiological and biological hazards can also cause damage to electronic equipments both from intentional attack or accidental discharge in an information system environment (Vacca, 2009). Intrusion or authorised access into library building is seen as another threatening threat which can lead to theft of valuable materials. For instance, stolen computing and network equipment can be resold on the black market for the value of its computing power. In addition, physical attacks can also occur at system consoles through available ethernet ports and in network equipment or wiring closets rooms (Lindstrom, 2003).

(f) Human Related Threats

Prior literature consistently reports that human errors are the most highly ranked security threats (Loch, Carr and Warkentin,1992; Whitman, 2004; Im and Baskerville, 2005). Instances of poor security practices that may put an organisations's IS security at risk caused by human are human errors, poor passwords selection, piggybacking, shoulder surfing, dumpster diving, installing unauthorised hardware and software, access by unauthorised users and social engineering, lack of discipline or knowledge among library staff and patrons (e.g. no data backups) (Pipkin, 2000 and Conklin, et. al., 2005). Dhillon's study (1999) indicated that computer fraud by insiders is recognised as a severe problem which could be difficult to prevent especially when it blends with legitimate transactions.

Human errors including data entry errors or carelessness, though often not considered as threats but they are highly likely to occur. Lindstrom (2003) revealed that erroneous actions by employees or users can threaten the integrity, availability, confidentiality and reliability of data. Examples include: 1) Incorrect set-up of security features could result in loss of confidentiality, integrity and availability of data; 2) Switching off computers when an error is displayed instead of correctly closing all current applications; 3) Deletion of files; 4) Inadequate back-ups; and 5) Processing of incorrect versions of data.

Employee misconducts especially in large corporation may be the most difficult problem to manage, as use of perfect intrusion detection controls become irrelevant when trusted employees either accidentally or unknowingly do something they should not do (Swartz, 2006). Gawde (2004) reported that as much as 80% of the security compromises are due to actions by insiders. The effects of employees' misuses to

organisations include loss of productivity, loss of revenue, legal liabilities and other workplace issues. Therefore, organisations need effective countermeasures such as by enforcing appropriate usage policies to minimise its losses and increase productivity. Similarly, Lindstrom (2003) highlighted the risk of sabotage against sensitive systems by internal employees as they are familiar with the systems. Their knowledge provides them opportunities in sabotaging the organisation's computer systems Common examples of sabotage include: a) Destroying hardware and infrastructure; b) Changing data; c) Entering erroneous data; d) Deleting software; e) Planting logic bombs; f) Deleting data; and g) Planting a virus. Even though, the number of incidents of employee sabotage is believed to be less than for theft and fraud but the individual losses can be high. Despite reports and findings on the seriousness of human errors in threatening IS, these threats have been poorly recognised as important element for IS security (Im and Baskerville, 2005).

2.5 Sources of Information Security Threats

Researchers reported that threats to ISec could derive from variety of sources. For instance, Loch et al. (1992) developed a comprehensive threat model which encompasses sources, perpetrators, intent and consequence. They divided threats' sources into insiders or outsiders with the perpetrators either human or non-human and the actions accidental or intentional with the consequence a disclosure, modification, destruction or denial of service. On the other hand, White et al. (1996) in their study of responses to threats distinguished between internal and external IS security functions, where internal functions focused on technical issues, whereas external functions stressed managerial and operating security, or non-technical issues, on the basis of the US security standard NIST SP800-30.

Bryson (1999) in her handbook on 'Effective Library and Information Center Management indicated that security threats can be found through; 1) Human error or deliberate human intervention (human error, incorrect keying of input data and errors in program development or maintenance); 2) Natural and political disasters (earthquake, flood, fire, industrial sabotage, terrorism and war); and 3) Hardware and software failures (power failure, equipment failure, network failure or system malfunction). Microsoft's white paper on security (2000) divided cause of security threats into human and natural disasters. Human-caused threats include malicious and non-malicious threats (Figure 2.2). The non-malicious threats usually come from employees (e.g. users, data entry clerks, system operators and programmers) who are frequently make unintentional errors (e.g. data entry errors or programming errors) that contribute to security problems directly and indirectly (e.g.: system crashes).

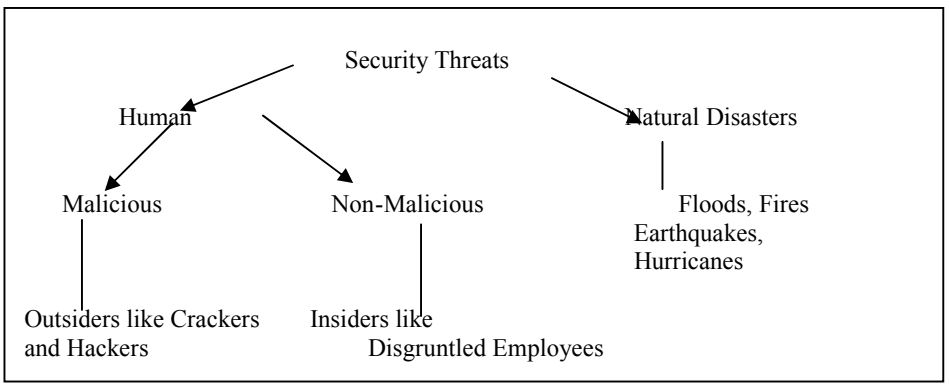


Figure 2.2: Security Threat Classification
(Source: Microsoft White paper on security, 2000)

On the other hand, Volonino and Robinson (2004) categorised origin of the intrusion or threat from external and internal sources. They includes malware, hackers, script kiddies, former employee, espionage, adversaries or terrorists as the external threats to the IS security. Whereas the management, employees, consultants, contract workers, maintenance crew and temporary staff are identified as the internal threats to the IS security. Similarly, Vaast (2007) also reported that IS professionals working in a

hospital believed that most of the external IS security threats came from outside in the form of viruses, ad-ware, intruders and hackers. Whereas internal threats came from employees due to their curiosity, recklessness, lack of time, malevolence and ignorance. Other researchers identified natural environments, infrastructure (like electrical power), hardware malfunction, software misbehavior, communication media failures and human errors as the major causes of security threats (Neumann, 1995; and Im and Baskerville; 2005). On the other hand, Gawde (2004) indicated that the majority of security threats are introduced by employees themselves due to their lack of sense of security, due care and diligence such as: a) accidental errors of attaching wrong files in email attachment and sending email to wrong recipient; b) social engineering attacks; c) sharing folders on a PC; and d) use of weak passwords and sharing passwords.

2.6 Information Security Countermeasures

Countermeasures are controls for vulnerabilities which include deterrent controls, preventive controls, corrective controls, detective controls and recovery controls (Merkow and Breithaupt, 2005). Countermeasures also include action, device, procedure, technique or other measure that reduces the vulnerability of an automated information system (Digital Guards, 2005). In dealing with IS security threats, some researchers have directed attention not only to technological but also to organisational dimensions (Calder and Watkins, 2003; Chan et. al., 2005; Ma and Pearson, 2005; Mercuri, 2004b and Vaast, 2007). As stressed by Tarimo (2006), security program can no longer rely entirely on traditional security controls such as using physical access controls and security guards to ensure the security of an organisation's assets, processes and communications but it must also focus on the human element.

In the literature, there is a rapidly evolving body of knowledge around the principles and practices of cyber security that gives proper attention to the roles of people (i.e. organisational dimensions), process (i.e. policies and procedures dimensions) and technology (i.e. technical dimensions) in order to implement an effective digital security program (Volonino and Robinson, 2004).

For instance, Icove et al. (1999) used a criminology perspective to group security approaches for information system security into seven categories: software, hardware, data, network, physical, personnel and administration (including security regulations and policies). Similarly, Yeh and Cheng (2007) listed 50 fundamental security countermeasures commonly adopted to evaluate the adequacy of IS security in 109 Taiwanese enterprises by using questionnaires. The countermeasures are broadly divided into two main categories that are IT-related countermeasures and non IT-related countermeasures. Each category of countermeasure contained five to eight countermeasures (Table 2.8). Their study revealed that regardless of industry, higher security was applied to software, hardware, data, and physical assets, whereas lower security was apparently required of the network, personnel, and regulation or legality assets. As for overall security, they reported that the banking or finance industry was the most secure (Yeh and Chang, 2007).

Table 2.8: A summary of fundamental security countermeasures

IT-related countermeasures	Non IT-related countermeasures
Software User entrance log System recovery Multi-user system Scanner Automatic debug and test Access control to program source Verification of system modified Covert channels and Trojan code	**Physical facilities and environment** Lightning protector Air conditioner Fireproof installations Waterproof installations Quakeproof installations

(Source; Yeh and Chang, 2007)

Table 2.8: Continued.

IT-related countermeasures	Non IT-related countermeasures
Hardware Remote mirroring Surveillance system use Entrance limitation Emergency power source (UPS) Periodical disk checking	**Personnel** Confidentiality agreement Invalid account removing ISec consultant Security audit irregularly Security education and training Operational procedures training D Incident report procedures
Data Information backup Data access controls, authentication User access rights, authorisation Enforced path Event logging Information handling procedures Management of removable media Disposal of media	**Regulation and legality (including risk transference)** ***Security policy*** ISec policy Security in job responsibilities Business continuity management ***Compliance with legal requirements*** Privacy of personal information Intellectual property rights ***Risk transference*** Security service provider Security outsourcing First party insurance Third party/public liability insurance
Network Anti-virus software Encryption User authentication Instruction detection systems Firewalls Alternative circuit Digital signatures Limitation of connection time	

(Source; Yeh and Chang, 2007)

2.6.1 Technological Measures (Technical dimensions)

Technological controls or logical controls refer to the use of object access restrictions implementation through the use if software or hardware. Moreover, the traditional IS security has emphasised on the security technologies as the basis of a security system (Siponen and Oinas-Kukkonen, 2007). It is undeniably true that some answers to security challenges have been technological (Volonino and Robinson, 2004). Most often the IS professionals have adopted IT tools such as user identification, authentication, encryption, segregated network architecture, firewall, access management and backup systems in order to deal with security challenges (Volonino and Robinson, 2004; Solomon and Chapple, 2005).

(a) Hardware Security Measures

A library IS security consists of several hardware equipments such as telephone lines, input or output ports, modems, network cablings, scanners, printers and storage media. These equipments need to be secured from any threats including thefts, power failures, equipment incompatibilities, careless damage and ensure the availability, confidentiality and integrity of data in a library (Yeh and Chang, 2007; INTOSAI, 1995). For example, Eisenberg and Lawthers (2005) and Rajendran and Rathinasabapathy (2007) encouraged the use of closed circuit television (CCTV), visual camera, magnetic detection system and electronic anti-theft system at strategic places. Besides that, the use of locks, security cables, locked cable trays, metal cages or anchoring devices are advisable for protecting hardware equipments (INTOSAI, 1995; Rajendran and Rathinasabapathy 2007). Telephone lines can be cut or lost and electricity failure might happen, thus a company should set up alternative telephone lines as alternative communication lines and generators as backup power sources (INTOSAI, 1995). Besides that, physical damage to storage media such as hard disks can always happen and might cause some data loss. Consequently, data recovery techniques such as remote mirroring or file mirroring are often employed to save important data. These remote mirror and copy feature are hardware solution that enables the mirroring of data from the local site to a second storage unit at another site or the remote site (Wikipedia Encyclopedia, 2010).

(b) Software Security Measure

Flaws and risks related to the library software are more likely to be found when services such as library systems, OPACs, online databases and resources are made accessible via the Internet. Eisenberg and Lawthers (2005) suggested the use of the following measures for protecting the software security: a) Cleanup software to erase files or settings left behind by a user; b) Desktop security software at application level and

operating level to monitor, restrict usage or disable certain features of the workstations; c) Distribution agents to automate the process of installing an application or updates to workstations on a network; e) Menu replacement software to replace the standard windows desktop interfaces and provide control on timeouts, logging and browsing activities; f) 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; and g) Timer software to control the amount of time a patron can use a workstation.

On the other hand, Yeh, and Chang (2007) listed the following countermeasures in order to secure the software; a) use of multi user operating systems and application software to allow concurrent access by multiple users of a computer; b) use of periodical automatic debugging to remove any defects from newly developed software or hardware components; c) use of systems recovery to rebuild and repair the computer systems after disaster or crash; and regularly analysed the user entrance logs. Yasin (2002) encouraged organisations to use ID management software to automate administrative tasks and the use of single sign on system as a user authentication and authorisation to access all computers and systems. Despite that, organisation should also consider the use of anti-spyware software, spam filtering software and anti-phishing solutions to prevent any spyware, spamming and phishing attacks as well as web filtering software to prevent access to inappropriate materials or sites (Ferrer and Mead, 2003; Ohaya, 2006; Orme, 2001).

Therefore, the scope of software security in libraries should encompass the above components from software security breaches and assure the confidentiality, availability and integrity of the library software.

(c) Workstation Security Measure

As more libraries make available to their patrons Internet-connected computers, there is a need to secure each computer from any security threats from the Internet as well as threats from the users such as viruses and worms, theft and unauthorised access. Creating a secure public access workstation involves many discrete procedures and these steps are interdependent with other security features such as network security, server security and user issues (Eisenberg and Lawthers, 2005). Eisenberg and Lawthers (2005) suggested several considerations in order to create secure public access workstations in libraries such as:

i. Install the special third party lockdown software to customise operating system installations.
ii. Use of operating system hardening. Operating system hardening is the process of modifying and locking down a standard default installation of an operating system on a server or a workstation.
iii. Computers operating systems and applications especially for antivirus should be kept up to date with the latest patches and updates, especially for antivirus.
iv. Secure the computer's BIOS.
v. Install the computer with minimal operating system features
vi. Securely configure applications such as browsers and office productivity.
vii. Educate and constantly remind staff about the need for security
viii. Install desktop security software and personal firewall to restrict user access to a desktop computer's operating system, desktop, printing functions and many applications.
ix. Install rollback software, which resets a public access computer to a previous state every time the computer is rebooted.
x. Install cleanup software which automates the process of deleting temp files and cookies.
xi. Install distribution agent which can automate the process of deploying software to many computers at once.
xii. Require user authentication prior access to workstations.

Gawde (2004), also urged organisations to implement comprehensive desktop security and controls such as implementation of role based access control, host based intrusion detection system, centralised automated antivirus solution, patch and update management system, software metering, monitoring system, personal firewall and

enterprise backup solution that covers the desktops. These initiatives should be pro active rather than reactive with the blend of preventive, detective and corrective in order to mitigate risks due to misuse and in appropriate desktop computers.

(d) Network Security Measure

Good security systems protects the network in a manner that is consistent with its purpose and secures it from adware, spyware or network intruders (Eisenberg and Lawthers, 2005; Yeh and Chang, 2007). The network security for a library would need to be simultaneous to ensure that full access of its bibliographic database to legitimate users on the Internet and in the library as well as disallow access from unauthorised users. Eisenberg and Lawthers (2005) suggested libraries to use firewalls as means to protect their internal network against attackers from the Internet (or outsiders) as well as providing content filtering, web caching and virus protection to the libraries' internal networks. They also urged libraries to consider the use of authentication, anti-virus software, desktop security software and separate cablings for each network or virtual LAN switches to physically separating public and staff local area networks (LANs), in order to protect the internal library networks security breaches by internal patrons or staff. Besides these, libraries should also consider the use of firewall with virtual private network (VPN) capabilities to protect remote access connections especially for wireless network connectivity (Eisenberg and Lawthers, 2005).

(e) Server Security Measure

In a library's network, servers play a vital role in providing access to key library services such as online databases, catalogs and circulation systems to internal and remote patrons (Eisenberg and Lawthers, 2005). The availability, confidentiality and integrity of the library server can be assured via proper implementation of specific

counter measures, because it becomes accessible to those within and outside the library. Thus, libraries need to take steps to secure the e-mail and web server applications from any intrusion and application failure due to viruses, hackers and natural disasters. Eisenberg and Lawthers, (2005) identified several technological security measures in order to protect servers at many different levels such as follows:

i. Install firewall to protect servers from intrusion.
ii. Hardened the server operating systems and the server applications to protect from vulnerabilities.
iii. Employ authentication to ensure that only authorised and valid users can access the system.
iv. Install anti-virus software and keep anti-virus virus definition files up-to-date.
v. Provide physical security for the server such as to place servers in a secure location for instance place it in a lockable cage in a locked room with environmental controls.
vi. Review server logs periodically by using a log file monitor utility which monitors log files for signs of intrusion or security violations.
vii. Protect the file system by restricting access to the directory structure using file or directory permissions.
viii. Make regular backups for the data, installation software, hardware specifications and installation passwords as they are vulnerable to viruses, hackers, fire or flood. The backup media and documentation should be placed at an offsite location.
ix. Implement fault tolerance as backup system if one system such as a hard drive or the computer itself fails.
x. Install intrusion detection software and host auditing software to monitors for signs of intrusion or changes on files and directories of computers or servers.

(f) Data Security Measure

Since a library stores, processes and provides access to vast amounts of data such as the patron records, personnel data, bibliographic records, MARC records, circulation data and so on, it will definitely require a sound data management system to assure the security of its data against accidental loss, unauthorised modifications and access by taking appropriate measures. Ortiz-Caceres (2006) suggested that IT department should block all the physical ports such as the Universal Serial Bus (USB) ports to prevent information theft or data lost in the public domain because of the user's ISec ignorance

or negligence. Yeh and Chang (2007) listed seven countermeasures for protecting the data including use of information backup, authentication for data access controls, authorisation for user access rights, enforced path, event logging, procedures for information handling, management of removable media and disposal of media.

(g) Physical Facilities and Environmental Security Measure

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 damage associated with fire, flood and physical intrusion (INTOSAI, 1995). The use of security personnel to undertake patrol within the library and to enforce appropriate library access at the main lobby has become increasingly common (Rajendran and Rathinasabapathy, 2007). However, they should not necessarily have access rights to IS, sensitive output and secure areas during quiet hours to prevent abuse of privilege (INTOSAI, 1995).

Other use of physical security systems or the non-electronic systems in libraries include: a) inspection of bags and other belongings of library users while entering and leaving the library by security or library staff, b) visual inspection by library staff through floor walks to overcome the unethical practices, and c) the use of window protection with locks, grills, guards, bars, screens and films, door protection, display case protection and dummy security devises to controlled access to the library buildings and library collections.

Rajendran and Rathinasabapathy (2007) also suggest the use of electronic security systems to overcome the security threats in the library by using the following tools: 1) burglar protection to provide alarm notification to the appropriate authorities, 2) Electromagnetic system to combat library material theft, 3) Electronic surveillance

cameras to monitor the library entry control and site surveillance, and 4) Radio Frequency Identification (RFID) system for easy handling and security of the library collection. These electronic security systems are believed to be effective in reducing the levels of theft and unethical practices within the library premises at reasonable cost for many libraries.

Another popular physical security measure in libraries is the use of air conditioner. This is because the computers and their peripherals often have specific environmental requirements. Failing to comply with the environmental conditions specified by the manufacturer may lead to machine failure and disputes over maintenance (INTOSAI, 1995). Beside air conditioners, Yeh and Chang (2007) also encouraged the use of lightning protectors, fireproof installations, waterproof installations and quakeproof installations to protect the IS against physical damage due to natural disasters.

2.6.2 Organisational Measures (Process and Human dimensions)

Most of today's security challenges are related to the human and organisational aspects of security (Anderson, 2007). Often human factor receives less attention in ISec practices as huge amounts of money and time are invested in technical solutions. Technical solutions are necessary to address vulnerabilities such as viruses and denial of service attacks. However, many examples of security issues related to humans such as phishing and social engineering are increasingly exist (Kruger, Drevin and Steyn (2007). Therefore, the relying on the advanced technologies alone will not solve the security problem as technologies are generally served as static barriers and it will become ineffective in an environment where humans exist (Conklin, et al., 2005). Recent research has also recognised the needs to understand the impact of human and organisational factors as well as the technological factors on the effectiveness of ISec

controls (Beznosov and Beznosova 2007; Werlinger, Hawkey and Beznosov, 2009). This is because prevention of the misuse of ISec by employees has direct business value including increased productivity, maximization of corporate assets, compliance with privacy regulations, protection from legal liabilities, preservation of network bandwidth and resources (Gawde, 2004). Thus, organisations should deploy comprehensive countermeasures that include human and organisational security measures to defend against misuse of its resources.

(a) Information Security Policy

Security process comprises administrative safeguards which refer to administrative actions, policies and procedures to manage the selection, development, implementation and maintenance of security measures to protect information as well as to manage the workforce in relation to the protection of that information (Centers for Medicare and Medicaid Services (CMS), 2005). These include hiring practices, usage monitoring and security awareness training (Solomon and Chapple, 2005).

In general, policies are formal and high-level-broad statements which describe required actions the organisation wants to accomplish and why (Guel, 2007). Specifically, security policy is the set of rules and practices that inform and regulate users, staff and managers on how an organisation manages, protects and distributes its key assets including people, hardware and software resources and information (Weise and Martin, 2001). As indicated by Pfleeger and Pfleeger (2003) security policy is a high-level management document that informs all users of the goals and constraints on using a system and must answer three questions, namely *who* can access *which* resources in *what* manner.

The characteristics of good security policies are that they must be implementable through system administration procedures, be enforceable with security tools, clearly define the areas of responsibility for the users and should be documented, distributed and communicated (Weise and Martin, 2001). Weise and Martin (2001) also listed several purposes of a security policy such as; i) to specify the mechanisms through which the security requirements can be met; ii) to provide a baseline from which to acquire, configure and audit computer systems and networks for compliance with the policy; and iii) to allow for the development of operational procedures and the establishment of access control rules for various applications, systems and networks.

There are variety types of security policies in an organisation, but the common types of security policies are acceptable use policy, back up policy, confidentiality policy, data retention policy and wireless device policy (Solomon and Chapple, 2005). Existence of such policies would reflect the top management commitment towards all ICT security aspects and play as a reference framework to all other ICT security sub policies, standards, procedures and countermeasures in an organisation (Bakari et al., 2005). Dimopoulos et al. (2004) suggested that the IT security policies in small medium enterprises (SMEs) should be reflective of the ICT usage. For instance, an IT security policy is not necessary if there is limited or no ICT usage in SMEs, but a detailed policy which addresses all issues about usage of ICT infrastructure is needed for SMEs with sophisticated ICT usage. Gawde (2004) also suggested organisations to develop acceptable use policy for desktop usage that specify on what kind of applications users can run, what kind of data they can store, what can they surf on Internet, what type of activity is strictly forbidden and what consequences will result if the policy is violated. In libraries, the security policy will have some areas of overlap with the acceptable use policy. An acceptable use policy is generally focused at patron use of the library IS, whereas a security policy is developed as an administrative guide, which includes rules

and guidelines for all access and use of IS (Williams, 2001). The security policy is needed in a library as they provide continuity, consistency and a basis for enforcing staff and patron conduct on using the library IS (Williams, 2001).

Literature reveals various benefits of adopting an IT security policy. An international accepted standard ISO 17799, indicates that a security policy is essential foundation for successful security strategy, as it defines issues such as the IT security goals of the organisation, what specifications and guidelines need to be followed and what is acceptable and not acceptable. Dimopoulos et al. (2004) indicated other benefits of creating IT security policy such as follows:

i) ISec policies help clearly defined responsibilities involved in protecting your information such as (reviewing firewall logs and conducting backups) thereby ensuring that necessary tasks are actually carried out.
ii) ISec policies help the organisation understand what tools and hardware are required for protecting their information and ensure that the organisation actual security measures are at an acceptable level.
iii) ISec policies help protect the organisation's investment in IT by defining what must be done to ensure all IT assets are adequately protected against damage.
iv) The practice of developing ISec policies is considered a source of competitive advantage amongst security conscious practitioners.

(b) Information Security Procedures and Controls

In order for ISec policies to be practical and implementable, they must be further defined by standards, guidelines and procedures (Weise and Martin, 2001). As indicated by Pfleeger and Pfleeger (2003) procedure or guideline documents are created to define how the security policy translates into specific actions and controls.

Procedures are the step by step instructions on how to implement and enforce policies in the organisation (Conklin, et. al., 2005). They are equally important as policies as 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).

The importance of creating the policies, guidelines and procedures in an organisation is seen as one of the best tools in defending against human-created security problems as well as establish details on the roles and responsibilities for security administrators and users to maintain the security of the systems and networks (Dhillon, 2001 and Conklin, et al., 2005). As stressed by Breeding (2003) having all the best equipments and software in place will be in vain unless the individuals in the organisation follow the right procedures.

(c) Administrative Tools and Methods

Administrative tools and methods are both proactive and reactive means in ensuring the security of IS in a library which includes asset classification, risk analysis, audits and incident reporting systems. As indicated by Hagen (2008), a technical administrative system must be in place before a system of training and education is adopted, because the formal system provides a framework for the content of the training program.

(d) Information Security Awareness

Awareness programs explain the employee's role in the area of information security. The aim of a security awareness effort is participation. Technology alone cannot solve a problem that is controlled by individuals (Hight, 2005). ISec depends not only on

technology, but also on the awareness, knowledge and intentions of the users of IS. It has been reported that ISec awareness programs have emerged as an important aspect of information security. This is because people are the weakest link in any security-related process, thus organisation is suggested to focus on educating personnel through a security program which address user education, awareness and training on policies and procedures that affect them (Merkow and Breithaupt, 2005). Also, top management is expected to take an active approach to the security of their organisation by supporting and following the policy themselves. Nothing can undermine a security education and awareness effort faster than lack of support from the management of an organisation (Hight, 2005). Moreover, not all employees know their roles and responsibilities in relation to IT security, therefore management should make sure that employees are aware of their roles and if possible stipulate these roles and responsibilities in their job descriptions (Kimwele, Mwangi and Kimani, 2005).

Dlamini, Eloff and Eloff (2009) highlighted the importance of well designed and periodic ISec awareness campaigns in educating the users on the emerging threats and ways in reporting the security incidents when the new threats and countermeasures are introduced. The importance of security awareness programs is further emphasised in the BS7799:1 where the objective of user training is given as 'to ensure that all users are aware of ISec threats and concerns, and are equipped to support organisational security policy in the course of their normal work'. Owners, providers, users and other parties of IS should readily be able to maintain security by gaining appropriate knowledge and be informed about the existence and general extent of IS security measures within an organisation (Zoughbi, 2009).

Im and Baskerville (2005) had recommended a topic on mechanisms for avoidance of human error to be included in any security training and awareness programs. According to them, such training can help individuals update their skill and knowledge and educate the users of their systems. So that, they become more attentive in solving the security problems and making less security errors.

Despite the ISec awareness campaigns, Vaast (2007) on the other hand, stressed the vital of well designed and periodical updates of ISec awareness policies within an organisation in order to make the end-users aware of IS security issues including the potential breaches to security and of the risks associated with these breaches. These policies thus rely on the implicit assumption that if the end-users were sufficiently informed, they would develop the same awareness of security issues. This is because effective communication of a security policy to all employees is critically important for it to be enforceable (Casmir, 2005).

Research also has listed several benefits of providing ISec awareness programs in organisations. For instance, Chan, Woon and Kankanhalli (2005) studied the impact of security related factors on the user's perception of usefulness of secured Knowledge Management Systems (KMS). Their finding suggests that for effective protection of KMS, people should fully understand the purpose of security and their own roles in securing the KMS. They also suggested that organisations should provide training and awareness programs to promote an individual's understanding and awareness.

Kahan (2004) revealed that the aware employees may support the ISec efforts and can create as 'human firewall' (much like a firewall) to prevent and deter threats to a company's critical information assets. This 'human firewall' can be more powerful than

properly configured firewalls and Intrusion Detection Systems. Similarly, Schwartz (2006) also indicated that educating the employees on network security is a key point in preventing security breaches. Of the companies surveyed 84% with security awareness programs credit it with reducing breaches.

2.7 Security Assessment Models, Criteria, Packages and ISO Standards

There are a number of assessments models, criteria, schemes and standards that are related to information security. Kwok (1997) stressed that the Bell-Lapadula Model and the Clark-Wilson Model address only on ways to maintain a secure environment by controlling the flows of information within protection systems and access to controlled data items. Chao (2005) also indicated that these two models are inadequate in reflecting the current position of ISec in an organisation. The following is the comparison of several traditional assessment models which related to ISec of an organisation (Table 2.9).

Table 2.9: Comparison of Security Assessment Models

Model	Description	Research
Bell-Lapadula Model	Provides a theoretical basis for authorisation in traditional computer systems.	Bell and Lapadula, 1975; Lin, 1992; Sandhu, 1993; Waldhart, 1990.
Clark-Wilson Model	Deal with integrity of information in business environment through separation of duty and proper transaction mechanisms to ensure data validity.	Smith-Thomas and Wang, 1995; Zviran and Glezer, 2000.
Risk Data Repository Model	Assess risks based on assets, systems and environments. Uses the threats and countermeasures diagram to identify the security architecture, its countermeasures and threats.	Kwok and Longley, 1996; Kwok, 1997.

(Source: Adapted from Chao, 2005)

Besides the security models, there are several security assessment criteria which are commonly used in organisations. The security assessment criteria such as ISO17799, Best Practice and NIST Security Self Assessment Guide consider security issues more than products or systems by incorporating security issues such as policies, training and awareness (Table 2.10).

Table 2.10: Comparison of Security Assessment Criteria

Security Assessment Criteria	Description	Research
BS7799/ISO17799	It defines Code of Practices and a specification of ISec management system as reference for identifying the required ISec controls where IS are used in industry and commerce.	NIST, 2002; Tong, et al. 2003.
Best Practice Working Group	It addresses the ISec issues such as security policy, processes, people issues and technology adoption in any organisation.	ISAlliance, 2002
NIST Security Self Assessment Guide for IT Systems	It is a guide for information system security administrators to identify the security status of security program in government agents or general organisations. It evaluates management controls, operational controls and technical controls based on five level of effectiveness by using questionnaire approach.	Swanson, 2001

(Source: Adapted from Chao, 2005)

A standard is a document that provides requirements, specifications, guidelines or characteristics that can be used consistently to ensure that materials, products, processes and services are fit for their purpose. There is a need for a set of benchmarks or standards to help ensure that an adequate level of security is attained, resources are used efficiently, and the best security practices are adopted (Hong Kong Special Administrative Region, 2008). There are various standards and regulations that are available for information security such as the ISO standards and some non-ISO standards (Anday, et al, 2012).

Table 2.11: Comparison of ISO Standards

ISO Standards	Description	Research
ISO/IEC 27002:2005 (developed from BS7799) (Code of Practice for Information Security Management)	This standard contains guidelines and best practices recommendations for these 10 security domains: security policy; organisation of information security; asset management; human resources security; physical and environmental security; communications and operations management; access control; information systems acquisition, development and maintenance; information security incident management; business continuity management; and compliance .	Hong Kong Special Administrative Region, 2008.
ISO/IEC 27001:2005 (Information Security Management System - Requirements)	It specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System (ISMS) within an organisation	Ozkan and Karabacak, 2010.

(Source: Adapted from Anday, et al, 2012)

There are some other commonly used information security standards, which are not under the ISO body of standards (Table 2.12).

Table 2.12: Comparison of Non-ISO Standards

Non-ISO Standards	Description
Organization for Economic Cooperation and Development (OECD)	Guidelines for the Security of Information Systems and Networks.
Generally Accepted Information Security Practices (GAISP)	A comprehensive guide to security standards and practices. The first two levels are the Pervasive Principles, which target top executive leadership of organizations, and Broad Functional Principles, which targets IT management. The third level, Detailed Principles, is intended to address the day-to-day security measures needed to fulfill the other two levels.
Payment Card Industry Data Security Standard (PCID)	An information security standard for organizations that handle cardholder information to reduce credit card fraud via its exposure.
Control Objectives for Information and related Technology (COBIT)	It is a framework created by ISACA for information technology (IT) management and IT governance. It defines 34 generic processes to manage IT. Each process is defined together with process inputs and outputs, key process activities, process objectives, performance measures and an elementary maturity model.

(Source: Adapted from Anday, et al, 2012)

There are also a number of ISec assessment packages in the market (Table 2.13). The ISec assessment helps organisation understand the weaknesses and strengths of their security programs as well as ensure the effectiveness of the programs. These security assessment packages target different audiences but they can be apply to the general ISec programs as they shared common ISec objectives and use checklist to assess the ISec programs (Chao, 2005).

Table 2.13: Comparison of Security Assessment Packages

Security Assessment Package	Targeted Audience	Assessment Component and Percent of Coverage
American Institute of Certified Public Accountants (AICPA): 'Security Principle and Criteria' (AIG, 2003).	Accountants in the information assurance field.	Access control: 50.01% Confidentiality/Integrity Control: 5.88% Audit: 5.88% Incident Handling/Disaster Discovery: 11.76% People Issue: 11.76% Management issue: 14.71%
American Insurance Group's (AIG): 'Information Security Self Assessment' (AIG, 2003)	Cyber insurance clients/applicants	Access control: 32.30% Confidentiality/Integrity Control: 3.2% Audit: 9.67% Incident Handling/Disaster Discovery: 9.68% People Issue: 12.90% Management issue: 32.25%
Arizona Cyber Security Alliance's (ACSA) : 'Arizona Cyber Alliance Self Assessment Questionnaire' (ACSA, 2004)	IT professionals and executives of small business and nonprofit organisations in Arizona	Access control: 33.30% Confidentiality/Integrity Control: 0.0% Audit: 16.67% Incident Handling/Disaster Discovery: 25.00% People Issue: 16.67% Management issue: 8.33%
Computer Security Insitute's (CSI) : 'Information Protection Assessment Kit (IPAK)' (CSI, 2002)	IT professionals, Information security managers and system administrators.	Access control: 24.5% Confidentiality/Integrity Control: 10.00% Audit: 5.91% Incident Handling/Disaster Discovery: 14.08% People Issue: 20.90% Management issue: 24.99%
Georgia State University's (GSU) : 'Security Assessment Questionnaire' (Georgia State University, 2003)	University community	Access control: 37.80% Confidentiality/Integrity Control: 0.0% Audit: 6.67% Incident Handling/Disaster Discovery: 22.22% People Issue: 4.44% Management issue: 28.89%

(Source: Adapted from Chao, 2005)

Table 2.13: Continued.

Security Assessment Package	Targeted Audience	Assessment Component and Percent of Coverage
IBM's: 'Security Self Assessment Survey' (IBM, 2003)	IT professionals, Information Security managers and system administrators.	Access control: 17.90% Confidentiality/Integrity Control: 4.47% Audit: 5.96% Incident Handling/Disaster Discovery: 14.94% People Issue: 21.66% Management issue: 35.14%
INSUREtrust.com's (INS): 'Security Assessment Questionnaire' (INSUREtrust, 2000)	Cyber insurance clients/applicants.	Access control: 15.20% Confidentiality/Integrity Control: 2.20% Audit: 21.70% Incident Handling/Disaster Discovery: 10.87% People Issue: 26.14% Management issue: 23.89%
Internet Security Alliance's (ISA): Common Sense Guide For Senior Managers Top Ten Recommended Information Security Practices' (ISAlliance, 2002)	IT professionals, Information Security managers and system administrators.	Access control: 11.70% Confidentiality/Integrity Control: 3.33% Audit: 21.67% Incident Handling/Disaster Discovery: 21.66% People Issue: 5.01% Management issue: 36.60%
Maryland Health Care Commission's (MHCC): 'HIPPA Security Assessment Guide' (MHCC, 2002)	Health care providers and organisations in Maryland.	Access control: 18.70% Confidentiality/Integrity Control: 18.75% Audit: 18.75% Incident Handling/Disaster Discovery: 6.25% People Issue: 31.25% Management issue: 6.25%
NIST 's: 'Security Self Assessment Guide for IT Systems' (NIST, 2000)	Government agencies.	Access control: 22.70% Confidentiality/Integrity Control: 9.33% Audit: 10.22% Incident Handling/Disaster Discovery: 19.11% People Issue: 9.78% Management issue: 30.66%

(Source: Adapted from Chao, 2005)

It is believed that the following criteria based on the security assessment criteria, ISO standards, Non-ISO Standards and security assessment packages are difficult to realise into the organisation's need due to lack of educated and skilled IT staff in an organisation (Chao, 2005).

2.8 Studies on Information Security Frameworks

Kim (1992) has compared five IS security models from the literature and the summarised the frameworks in Table 2.14. Based on the summary, he concluded that the effectiveness of ISec is largely determined by: a) organisational factors such as industry susceptibility, b) managerial factors such as security policies and procedures, and c) user factors such as user's system usage and security awareness (Table 2.14).

Table 2.14: Summary of Security Frameworks

Framework	Dependent Factor	Independent Factor
Managerial Control Model (Madnick, 1978)	Effectiveness of computer security	• Operational considerations • Organisational impact • Economics • Objective and accountability
User's security concern (Goodhue and Straub, 1991)	User's security concern	• Industry risk • Company action • Individual factors
Security Impact Model (Straub, 1990)	Computer abuse	• Deterrent factor • Rival explanations factor
PC Security Behavior Framework (Frank, Shamir, and Briggs. 1991)	Security-related behavior of personal computer user	• Motivation • Role clarity • Ability
Model of Organisational Factors on Personal Computing Problems (Guimaraes and Ramanujam, 1986)	Incidence and intensity of personal computing problems, such as: - Integration - Costs - MIS-User relations - Data integrity and security	• Level of personal computing usage • Level of control • Level of support

(Source: Kim, 1992)

Kim (1992) also proposed a new security framework of IS environmental factors which influence an organisation's effort to reduce security risks based on the relevant IS security literature. The framework consists of five IS environmental factors such as organisational context, risk assessment by management, organisational impact, organisational use of IS and system characteristics which might influence the effectiveness of security efforts by an organisation in reducing the potential IS security risks.

Loukis and Spinellis (2001) assessed IS security in the Greek public sectors based on implemented organisational measures, technical measures and human resources measures. This study adopted the framework for IS development risks assessment, proposed by Willcocks and Margetts (1994) to determine the organisational and technological context factors which affect the application of the ISS measures, and to find contexts favoring their application. Based on the framework, they classified the risk factors into four categories: internal context risk factors, external context risk factors, process risk factors and content risk factors.

Chao (2005) developed an ISec assessment model to evaluate the security level of an ISec system in higher education institutions around the world. The assessment model consisted of a two-layer structure: the security controls and the sub-security controls which are formed based on literature reviews, ISec standards, best practices and ISec assessment guides. The main security controls include authentication, authorisation, access control, confidentiality/integrity control, audit, incident handling or disaster discovery, people issue and management issue. This model is used to verify the varying importance levels of security controls and sub-security controls among different types and different sizes of institutions and organisations. This model is contributes in improving security evaluation metric over extant methods and provides a potential baseline for the standard of ISec metric.

Dhillon and Torkzadeh (2006) performed a qualitative IS security assessment based on the value-focused thinking approach to identify fundamental objectives for IS security and means of achieving them in an organisation. Based on in-depth interviews with 103 managers about their values in managing IS security revealed 86 sub objectives, grouped into nine fundamental and 16 means categories that are essential in managing

IS security. The nine fundamental objectives related to IS security include: 1) enhance management development practices; 2) provide adequate human resource management practices; 3) develop and sustain an ethical environment; 4) maximise access control; 5) promote individual work ethic; 6) maximise data integrity; 7) enhance integrity of business processes; 8) maximising privacy; and 9) maximise organisational integrity. Their findings suggested that for maintaining IS security in organisations, it is necessary to go beyond technical means and adopt socio-organisationally grounded principles and values.

Suhazimah (2007) used Integrated System Social-Technical Theory as the basis of the research framework to identify the underlying dimensions of ISec management system, explore the relationship between these dimensions and test their impact as the antecedents of ISec maturity of the organisation in the Malaysian Public Service. The research framework consists of four independent variables representing the technical factors (formal coping mechanism) and social factors (organisational structure, organisational ISec culture and individual ISec key players' perception). Based on the findings, she had proposed the newly Integrated System Social-Technical Theory which consisted of risk management mechanism and six social factors namely organisational structure, awareness and training culture, individual perception on information security, social barriers and technical barriers as answer on underlying dimensions of ISec management approach in the Malaysian

Hagen, Albrechtsen and Hovden (2008) studied the implementation of organisational ISec measures and assessed the effectiveness of such measures among ISec managers in selected Norwegian organisations. Based on a web-based survey, the results revealed the companies participating in the study have emphasised developing and applying

formal systems, like security policies, procedures and controls, while awareness activities are less applied in the organisations. The study also highlighted that there was a deviation between measures the respondents used and how they assessed the effectiveness of the security measures. They reported that that measures that are not implemented were assessed to be more effective than implemented measures. This inverse relationship was interpreted as a metaphorical staircase of four steps of security policy, procedures and control, tools and methods, and awareness creation.

Schuessler (2009) assessed IS security effectiveness in large and small organisations by using general deterrence theory (GDT). This research model consists of four primary constructs: organisational factors (size and industry affiliation), threats, GDT's components and IS security effectiveness. The GDT's deterrence, prevention, detection and remedy constructs are used as a baseline to assess the countermeasures in eliminating a threat or at least mitigate some of the risk. This theory is used to examine the effects of organisational size, industry affiliation and threats faced by an organisation on the organisation's use of countermeasures as well as the impacts on an organisation's IS security effectiveness.

The IBM Security Framework provides organisations with a baseline to assess their security posture holistically that addresses technical, behavioral and managerial issues related to ISec (Buecker, et al., 2010). The model consists of six domains including: a) People and identity cover aspects on how to assure that the right people have access to the right assets at the right time; b) Data and information cover aspects on how to protect critical data in transit or at rest across the organisation; c) Application and process cover aspects on how to ensure application and business services security; d) Network, server and endpoint (IT infrastructure; e) cover aspects on how to stay ahead

of emerging threats across IT system components; and f) Physical infrastructure cover aspects on how to leverage the capability for digital controls to secure events, people or things.

Haniza (2009) carried out a study to gauge the level of enforcement and effectiveness of ISec policy from the users' perspective at a public university in Malaysia. This study proposed a theoretical framework for the effectiveness of institution's ISec policy, which consists of enforcement, users' awareness, users' understanding and users' acceptance as independent variables, whereas an effectiveness of ISec policy identified as dependant variable.

Based on the existing ISec frameworks described above, it can be concluded that assessing ISec in any organisation should incorporated the technical issues as well as management and people issues. As any organisation including a library comprised of people, therefore if an organisational factor is an issue in information security, there may be a reason to study the human element as well. This study used the idea of the metaphorical staircase of four steps of security policy, procedures and control, tools and methods, and awareness creation (Hagen, Albrechtsen and Hovden, 2008) but details it by proposing additional factors for each steps to assess the implementation of technological and organisational ISec measures in the library.

2.9 Empirical Studies on Information Security

Post and Kievit (1991) argued that research in the ISec largely falls under three major categories, which related to technical aspects of system security, management-oriented approaches and causes of computer security breaches. Kim (1992) reviewed 12 major empirical studies related to IS security (Table 2.15) and concluded that the success of

security depends on many factors but users' awareness of system security is identified as one of the most prominent factors.

Table 2.15. Summary of Empirical Studies

Author	Research Questions	Findings/Conclusion
Loch, et al. (1992)	Senior IS managers perception on computer security risks	• Greater risk in the microcomputer environment than in the mainframe environment. • The most serious threats are natural disasters and employee accidental actions. • Management needs to be more informed potential risks in the mainframe and network environment.
Goodhue and Straub (1991)	Factors influencing system's user security concern	• Negative relationship between firm's security action and user's concern. • Transportation industry is in the highest risk. • No significant relationship between user awareness and sensitivity to risk and company actions.
Post and Kievit (1991)	System users' demand on security	• Increased demand for more complex security as the number and diversity of users increase. • The most critical factor of successful security is users' awareness. • Users do not satisfy with existing security system.
Frank, Shamir, and Briggs (1991)	Factors influencing PC's users security-related behavior	• PC user's knowledge and informal norms are the most significant. • The existence of formal policies is not significant.
Bradbard, et at. (1990)	Computer security in small business firms	• When there is a high level of security, it tends to be comprehensive. • Firms need more adequate disaster recovery plans.

(Source: Adapted from Kim, 1992)

Table 2.15. Continued

Author	Research Questions	Findings/Conclusion
Hoffer and Straub (1994)	Profile of computer abuse incidents	• Large organisations experience more significant and frequent computer abuse than small organisations. • Educational institutions, wholesale and retail trade and utilities are more vulnerable to computer abuse than other industries. • No significant relationship between users' system privileges and their propensity to computer abuse.
Gupta et al. (1989)	Impact of organisational factors in problem related to personal computing.	• The level of PC usage and the level of support significantly influence the intensity of PC problems.
Richards (1986)	Profile of computer-related crime	• Financial service industry is in the highest risk. • Significant portion of the crime is committed by insiders. • Significant portion of the crime is not discovered by control procedures.

(Source: Adapted from Kim, 1992)

Hermanson et al. (2000) conducted an exploratory survey using questionnaires to understand how organisations address their IT risks and to examine evaluations of IT risks performed by internal auditors in their organisations. The results of the study revealed that internal auditors focus primarily on traditional IT risks and controls, such as IT asset safeguarding, application processing, and data integrity, privacy and security.

White and Pearson (2001) surveyed over two hundred USA companies to investigate the security controls of personal use of computers, controlling e-mail accounts and securing company data. The results of the study reinforced the need for better security control in the majority of surveyed companies. The results also revealed that many

corporations began to use computer technology before implementing appropriate safeguards and the majority of the company's safeguards continue to be lacking.

Loukis and Spinellis (2001) studied a representative sample of 90 public sector organisations to determine the organisational and technological context factors which affect the application of organisational measures, technical measures and human resources measures and to find contexts favoring their application. Analysis of data collected via structured questionnaires revealed that Greek public sector organisations have only a basic level of information system security awareness and adopted mostly basic IS security measures, such as back-up copies, recovery procedures, security zones and firewall. Only a small percentage has developed a systematic, complete and integrated approach towards the security of their information system, including IS security plans, IS security policies and internal audit procedures. Results also found that the investigated public sector organisations were more concerned about digital data confidentiality, probably because the IS security of many public sector organisations contain personal and sensitive data. Cluster analysis revealed that critical public enterprises such as banks, hospitals, social security organisations had applied most of the outlined IS security measures, including the written and approved IS security plan, written and approved ISS policy with specific roles and procedures and full-time IS security officer. As comparison, the central and local government organisations had applied only some basic IS security measures. However, the application of basic IS security measures varied significantly among the investigated public sector organisations, affected by the extent of usage of IT in the organisation (the number of IS users and the number of the functions supported by the IS) and the size (from the staff number viewpoint) of the IS organisational unit responsible to design and apply IS security measures.

Warren (2002) investigated the IS security practices in three countries: Australia, UK and USA. The survey reported that security practices in the USA seemed to be more effective than those of Australia or the UK. The results of the survey revealed that Australian organisations have poor levels of computer security due to poor implementation of security procedures and lack of budget for computer security. In UK, 42% of organisations did not have ISec policy and 49% of the organisations listed budget constraints as an issue in implementing computer security. In USA, theft of information and financial fraud caused great financial damage to organisations.

Chao (2005) utilised web survey to study the different importance levels of security controls and sub-security controls in universities. Based on analysed responses from 159 Information System administrators in IT centers of universities around the world, she found that authentication was the most important security control in small and medium-sized organisations. However, confidentiality or integrity was viewed the most important security control in large size organisations. Apparent results revealed that people issue was the least important security control in most of the organisations regardless of size. This study also revealed that the importance of management support increases parallel with the size of an organisation. In comparison, security awareness training was rated important only to large size organisations but small organisations viewed encryption technology as extremely important.

Suhazimah (2007) analysed 210 questionnaires from chief information officers, ICT managers and ICT officers to identify the antecedents of ISec maturity in organisations of Malaysian Public Service (MPS). Her analysis revealed that 60% of MPS organisations' ISec maturity was at Level 3 of maturity level signifying that awareness about ISec exists and that respondents believed the ISec management practices were

documented and have been communicated throughout their organisations. Results also reported that the most common attacks were spamming and malicious codes attacks but there were low occurrence of website defacement and distributed denial-of-service (DDos) attacks. This study also found that the antecedents of ISec maturity are risk management mechanism, organisation structure, technical barriers and awareness and training culture.

Haniza (2009) studied the level of enforcement and effectiveness of ISec policy from the users' perspective at a public university in Malaysia. This study involved three phases of data collection: a) a preliminary study to explore the IT arrangement and organisational structural practices in the university; b) interview with an IT-expert to understand the establishment of the ISec in the university; and c) survey questionnaire to gauge the level of users' perception on the institution's security policy. The study found that nearly half of the respondents perceived that they are aware, understand and accept the university's policy, whereas more than half of them agreed that the university's policy is effective.

Schuessler (2009) surveyed 1000 professional of the Association of IT Professionals (AITP) members by using online survey to assess the IS security effectiveness in large and small organisations. Results indicated that industry affiliation was found to be related to prevention efforts but not the deterrence, detection and remedy efforts. Both deterrence and prevention efforts were found to be positively related to the IS security effectiveness and the application of countermeasures in an organisation has changed the effectiveness of the threats faced. However, organisational size was not found to be positively related to ISS effectiveness as was industry affiliation. The results also indicated that certain industries are more effective at securing IS than others.

Dionysiou, Kokkinaki and Magirou (2010) presented the preliminary results on ICT security practices in 33 Cyprus private and public sectors based on a nationwide survey initiated by the University of Nicosia Research Foundation (UNRF) and the Cyprus Academic Research Institute (CARI). The survey used questionnaire which was drafted based on the IT Security Guidelines promoted by the national security agency of the German federal government. The questionnaire consisted of simple checklists that addressed all factors related to security policies and procedures, ICT Security Management, ICT Security measures, networking and Internet connection. The preliminary results indicated that the majority of organisations in the sample have made provisions for security mechanisms and its management.

Findings from the previous research have revealed that there are various types of ISec controls deployed in various organisations. However, the level of implementation of these security measures in many industries was still lacking as they tend to focus primarily on technical measures. Studies also found that the application of ISec measures in organisations was affected by several factors such as the organisation size and lack of budget for computer security. The review has highlighted the need to assess the actual status or the level of implementation of the different types of ISec controls in Malaysian academic libraries as well as the identification of the possible factors which might affect the level of implementation of the security measures in these libraries.

2.10 Chapter Summary

The first section reviewed on definitions of the key terms such as information, security, ISec and IS security. The next section provides brief overview on characteristic and roles of an academic library as well as its changes within the five automation phases. The third section highlights on the various issues and factors why a library needs for

IS and IS security. The fourth section reviews the sources and the possible types of threats, vulnerabilities and security issues related to the organisation's hardware, software, data, network, people and its physical facilities which are relevant to the study.

Main focus of this chapter was the review relating to the common types of information system security controls use in organisations. The countermeasures are reviewed from two different approaches; IT-related countermeasures and the non-IT related countermeasures. The IT-related countermeasures which also known as traditional approaches emphasised on the use of security technologies. Under the technical dimensions, the review covers the use of IT security tools for protecting the hardware, software, workstation, network, server, data and physical facilities. Whereas, the non-IT related countermeasures or also known as the 'soft approach' focused on the process, organisational and human aspects of security. Under the non-technical dimensions, the review covers on the use of ISec policy, ISec procedures, administrative tools and ISec awareness initiatives.

Chapter Three

RESEARCH FRAMEWORK AND DESIGN

3.0 Introduction

Information security management (ISM) describes controls that need to be implemented by a library in order to ensure the confidentiality, integrity and availability of its information resources. As libraries are increasingly reliant on computer technology and the Internet, there is no doubt that security becomes an important component of their technological infrastructures (Williams, 2001). However, not much is known about the actual implementation level of ISec in the library area. No academic library security study has been conducted specific to this area, and searches of journals and the Internet substantiated this finding. Thus, one could not make an assertion 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 surprising as information is the library's main business. Therefore, this research aims to assess the current practices of Malaysian libraries in managing their information security. This chapter outlines the research methods used in answering the research questions. It describes the research framework, review of research methodology related to information security, development of the instrument, as well as an assessment of the reliability and validity of the instrument, the way data was collected and analysed.

3.1 Research Purpose, Research Questions and Hypotheses

Most of the empirical evidence on ISec and its determinants are confined to the use of data from Western countries. Evidence from other environments, where the social, economic and cultural characteristics are different, is needed before any generalisation

can be made (Seliem, et al., 2003). Thus, the purpose of this research is to get a clear picture of ISec threats and security practices in libraries. This study would be a significant analysis of ISec threats and ISec management in a library environment, which is lacking in published literature. The results of this study may help the management of academic libraries identify their strengths, weaknesses and priorities in managing their ISec so that relevant actions can be applied in a more organised manner.

3.1.1 Research Purpose

This study aims to achieve the following objectives:

1) To explore the general IT infrastructures in Malaysian academic libraries in terms of number of personal computer (PC) allocations, availability of wireless connection, type of operating system used, years of ICT adoption, percentage of IS security budget and availability of IS security staff.
2) To explore the most common perceived ISec threats and the frequency of their occurrence (in term of hardware, software, data, network, physical and other IS security threats) discovered by these libraries during a period of six months;
3) To find out the most common perceived source of ISec threats in Malaysian academic libraries;
4) To ascertain the extent of technological measures deployed by Malaysian academic libraries. This would include identifying the level of implementation of hardware, software, workstation, network, server, data and physical security measures in these libraries;
5) To investigate the differences between academic libraries in Malaysia in applying technical measures based on type of university, years in ICT implementation, yearly ISec budget, availability of IS security staff and availability of wireless connection;
6) To ascertain the extent of organisational measures deployed by Malaysian academic libraries. This would include identifying the level of implementation of security policy, procedures and controls, tools and methods and awareness activities in these libraries;
7) To investigate the differences between academic libraries in Malaysia in applying organisational measures based on type of university, years in ICT implementation, yearly ISec budget, availability of IS security staff and availability of wireless connection; and
8) To propose a model and an assessment tool to assess the implementation status of ISec in Malaysian academic libraries.

3.1.2 Research Questions

In order to meet the purpose and objectives of the study, the following research questions are asked:

Research Question 1:
What is the general background of IT infrastructures in Malaysian academic libraries in terms of number of PC allocations, availability of wireless connection, type of operating system used, years of ICT adoption, percentage of IS security budget and availability of IS security staff?

Research Question 2:
What are the most common perceived IS security threats and the frequency of their occurrence in Malaysian academic libraries in terms of hardware, software, data, network, physical and human- related threats?

Research Question 3:
What is the most common perceived source of IS security threats in Malaysian academic libraries?

Research Question 4:
What is the level of implementation of technological security measures (in terms of hardware security, software security, workstation security, network security, server security, data security and physical security measures) in Malaysian academic libraries?

Research Question 5:
Are there significant differences between academic libraries in Malaysia in applying technological measures based on the type of university, number of staff, years in ICT implementation, yearly information system security budget, availability of IS security staff and availability of wireless connection?

Research Question 6:
What is the level of implementation of organisational security measures (in terms of security policy, procedures and controls, tools and methods and awareness activities) in Malaysian academic libraries?

Research Question 7:

Are there significant differences between academic libraries in Malaysia in applying the organisational measures based on type of university, number of staff, years in ICT adoption, yearly ISec budget, availability of IS security staff and availability of wireless connection?

Research Question 8:

What is the overall implementation status of technological security measures and organisational security measures in Malaysian academic libraries based on the proposed assessment tool?

3.1.3 Hypotheses

3.1.3.1 Differences between academic libraries in Malaysia in applying technical measures based on type of university, number of staff, years in ICT adoption, yearly ISec budget, availability of IS security staff and availability of wireless connection are suspect. Hence, it is therefore hypothesised that;

Hypothesis 1

There are no significant differences between academic libraries in Malaysia in applying technical measures based on type of university, years in ICT implementation, yearly ISec budget, availability of IS security staff and availability of wireless connection.

3.1.3.2 Differences between academic libraries in Malaysia in applying organisational measures based on type of university, number of staff, years in ICT adoption, yearly ISec budget, availability of IS security staff and availability of wireless connection are suspect. Hence, it is therefore hypothesised that;

Hypothesis 2

There are no significant differences between academic libraries in Malaysia in applying the organisational measures based on type of university, years in ICT implementation, yearly ISec budget, availability of IS security staff and availability of wireless connection.

3.4 The Research Framework

The framework in this research is adapted from the Organisational Information Security Staircase Model developed by Hagen, Albrechtsen and Hovden (2008). The original model (Figure 3.1) is constructed to show the degree of implementation and the subjective assessment of its effectiveness. The original model specifies 16 items on organisational measures that are grouped into four: policy; procedures and control; tools and methods and awareness creation. Hagen, Albrechtsen and Hovden (2008) reported that technical-administrative security measures, such as security policies, procedures and methods are the most commonly implemented organisational ISec measures in a sample of Norwegian organisations. The awareness-creating activities are applied by these organisations to a considerably lesser extent, but are assessed as being more effective organisational measures than the technical-administrative measures. This inverse relationship is interpreted as a metaphorical staircase of four steps: (1) security policy; (2) procedures and control; (3) tools and methods; and (4) awareness creation.

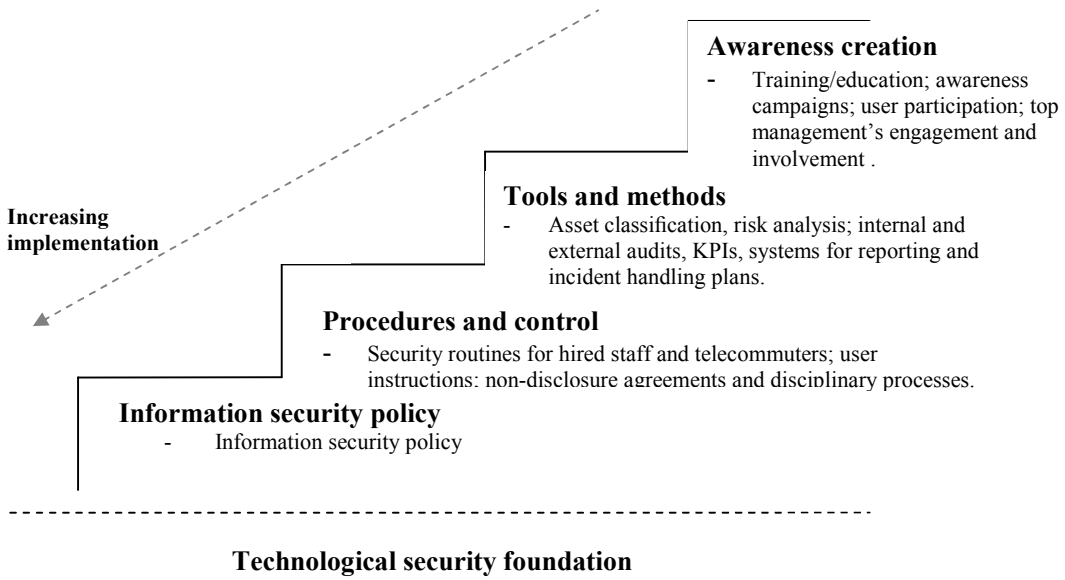


Figure 3.1. Organisational Information Security Staircase Model (Hagen, Albrechtsen and Hovden, 2008).

The basic premise of adapting the Organisational Information Security Staircase Model by Hagen, Albrechtsen and Hovden (2008) as the research framework is that the model is built around particular view of the technical-administrative measures in managing information security management such as technological measures, security policies, procedures and controls and awareness creation. The model provides a solid framework for incorporating the human part of information security measures. This is particularly mandatory in the adoption of effective information security measures since in most cases human is the key component in managing ISec in an organization. The model is chosen as it is considered generic and has enough flexibility to allow for planning for expandability by altering the variables or security elements measured. For instance, the model does not specify and assess on the implementation of technological solutions, thus, the revised model in this study is designed to simplify and make clear the different features of technological measures and organisational measures. The data used in the model is also flexible where it can be used for a large and a small sample size. This allows for flexibility to include more or less data elements in certain areas.

This study proposes a library Information Security assessment model (LISAM) which is derived by mapping the insights obtained from literature with the four steps of the Organisational Information Security Staircase Model to define and list the essential areas of ISM for libraries (Figure 3.2). This study proposes additional variables for each step to assess the implementation of technological and organisational ISec measures in the library. Also, the assessment instrument that aligns with the LISAM is proposed to provide more detailed guidance on how the LISAM can be used in assisting a library to assess the degree of implementation of technological measures and organisational measures as well as its overall ISec level.

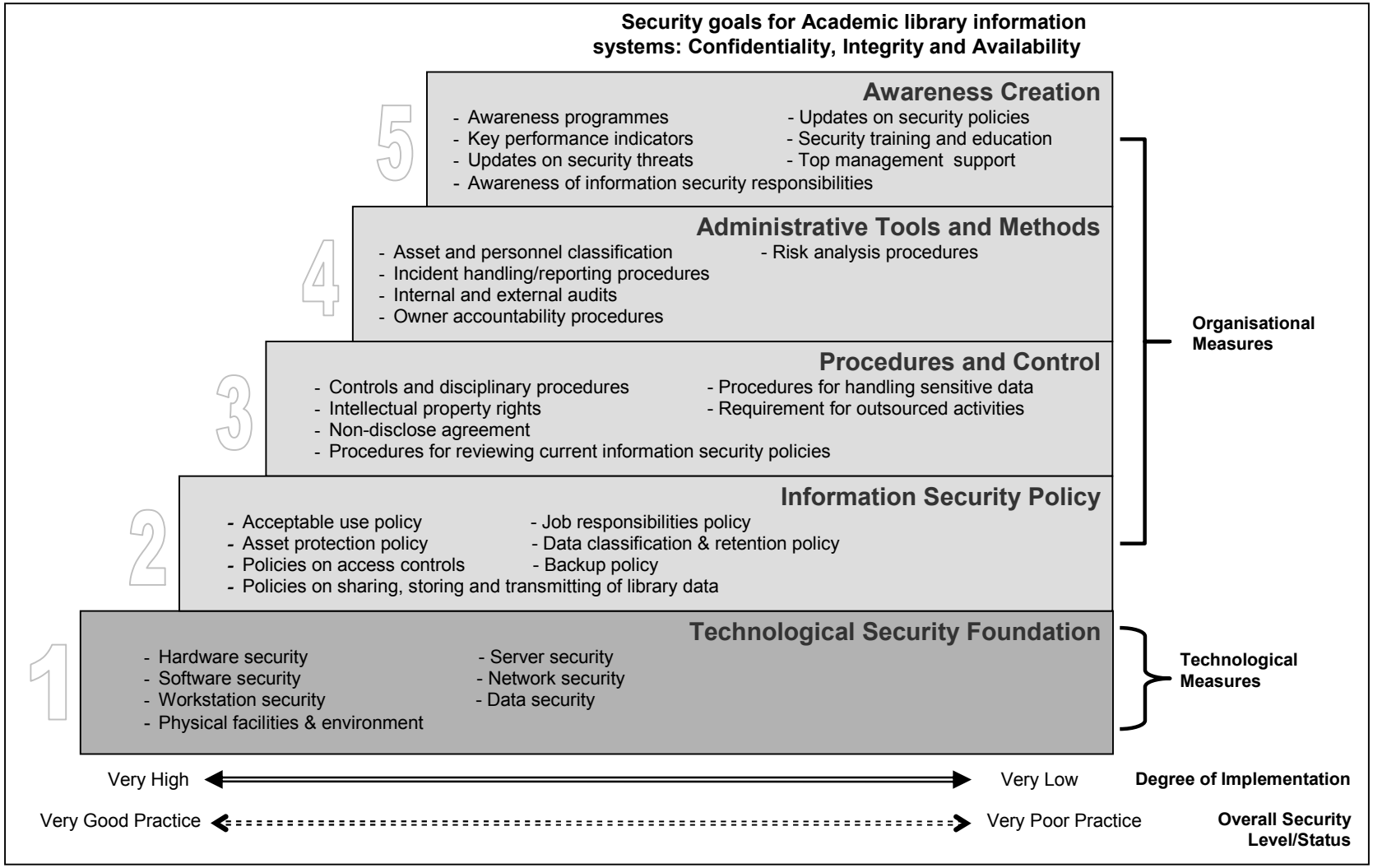


Figure 3.2. Library Information Security Assessment Model (LISAM)

The proposed components in the assessment of the ISec measures in libraries are pictured in a staircase model in Figure 3.2. The model is formulated on the basis that ISec includes organisational aspects, legal aspects, institutionalisation and applications of best practices in addition to security technologies (Von Solms, 2000). The relationship between the groups of organisational measures and technological measures metaphorically looks like a staircase. The model illustrates that in order for ISec measures to become effective, security should be built like a staircase of combined measures. To produce any effect, security measures are mutually dependent on each step (Sundt, 2006; Berghel, 2005). The steps in the staircase follow a logical order to achieve the three primary goals of a good security system practice, which are to ensure and protect the confidentiality, integrity and availability of an IS (Eisenberg and Lawthers, 2005). These three objectives guide the development of security measures to avoid different security threats in libraries. In this context, library IS security refers to means and ways that a library protects the confidentiality, integrity and availability of information processed by an IS and of the IS itself.

a) Protecting confidentiality means the privacy of information assets, such as the library's financial information, patrons' circulation information, applications and passwords to access library systems. These must be kept private and cannot be accessible or revealed to unauthorised people. Protecting confidentiality also means that the library should always follow the principle of least privilege, which states that the patrons are given only the privileges that they need to perform their jobs or tasks. For instance, if a user only needs to check or print out their emails using a library's Internet connection, they should have no ability to access the operating system files of that print server.
b) Protecting data integrity means a library has to make sure that data made available via the library IS is accurate, complete and is not inappropriately changed or deleted by unauthorised persons. Therefore, the library needs to implement appropriate security measures so that the library can recognise, protect and recover the systems from any breaches of integrity such as viruses,

worms and Trojan horses. It also means that the library should allow only appropriate access to the library computers, websites, databases and servers.

c) Ensuring data availability means a library should be able to recognise and defend against denial-of-service attacks and viruses by implementing a good backup policy and recovery procedures. This also implies that the library has to make sure that library services are available and not interrupted during routine hardware and software maintenance. This means that the data can be accessed whenever it is needed and that data can be restored quickly during downtime.

The model also highlights that the higher the position on the staircase, the more complex is the state of IS security management in a library. The first staircase illustrates that in any security environments, 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. These 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 element of ISec as the staff and patrons in libraries must abide by administrative security routines by applying them in their day-to-day activities.

3.2.1 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 and prevent unauthorised access to data that is transmitted over a library system. The staircase is constructed based on the assumption that a technological foundation must always be in place in any security IS environment as the main defensive system to any organisation; especially in a library setting. It is argued that without technological security solutions, there would be no need to have administrative measures (Hagen, Albrechtsen and Hovden, 2008). This is because it is technological solutions that prevent, detect and react to virus and spam attacks faced by most organisations (Hagen, 2008). Moreover, there is obvious evidence

that many research on ISec has traditionally been dedicated to technological aspects, as security technologies form the basis of a security system (Siponen and Oinas-Kukkonen, 2007). Thus, level one comprises technological security foundation, which a library should have to protect its workstations, servers, hardware, software, data, network, physical facilities and environment.

i) Hardware Security

A library IS consists of several hardware equipments such as telephone lines, input/output ports, modems, network cablings, scanners, printers and storage media. These equipments need to be secure from any threats including thefts, power failures, equipment incompatibilities, careless damage and ensure the availability, confidentiality and integrity of data in a library (Yeh and Chang, 2007; INTOSAI, 1995).

ii) Software Security

Flaws and risks related to the library software are more likely to be found when services such as library systems, OPACs, online databases and resources are made accessible via the Internet. The scope of software security in libraries therefore encompass protecting the software components from breaches and assure the confidentiality, availability and integrity of the library software (Eisenberg and Lawthers, 2005; Yeh, and Chang, 2007; Newby, 2002).

iii) Workstation Security

As more libraries make available to their patrons Internet-connected computers, there is a need to secure each computer from any security threats from the Internet as well as threats from the users (Eisenberg and Lawthers, 2005; INTOSAI, 1995). The most

common library's workstation security threats come from the Internet. Those from the users include viruses and worms, theft and unauthorised access.

iv) Network Security

Good security systems protect the network in a manner that is consistent with its purpose and secures it from adware, spyware or network intruders (Eisenberg and Lawthers, 2005; Yeh and Chang, 2007). The network security for a library would need to disallow access to the IS from unauthorised users, while simultaneously ensuring full access to legitimate users.

v) Server Security

In a library's network, servers play a vital role in providing access to key library services such as online databases and catalogues, circulation systems to internal and remote patrons, computer hardware, the operating systems, application programmes loaded on the hardware to perform specific functions, such as a web server or email server (Eisenberg and Lawthers, 2005). Libraries need to take steps to secure the email and web server applications from any intrusion, hardware or application failure due to viruses, hackers and natural disasters. The availability, confidentiality and integrity of the library server can be assured via proper implementation of specific countermeasures.

vi) Data Security

Since a library stores, processes and provides access to vast amounts of data, it will definitely require a sound data management system to assure the security of its data against accidental loss, unauthorised modifications and access by taking appropriate measures (Yeh and Chang, 2007, Thiagarajan, 2003, Powell and Gillet, 1997).

vii) 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 damage associated with fire, flood and physical intrusion (INTOSAI, 1995; and Yeh and Chang, 2007).

3.2.2 Information Security Policy: Step 2

Information Security (ISec) policy forms the basis of every administrative security regime (Hagen, Albrechtsen and Hovden, 2008). It refers to protecting various assets including hardware, software, data and people. This is laid out in the form of written documents 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 generally focuses on patron use of the library IS, whereas a security policy is a guide that includes rules and guidelines for access and use of IS. A security policy is needed in a library as it provides continuity, consistency and a basis for enforcing staff and patron conduct when using the library IS (Williams, 2001).

3.2.3 Procedures and Controls: Step 3

Procedures are step-by-step instructions on how to implement and enforce policies in the organisation (Conklin et al., 2005). Procedures and controls are implemented through work processes and procedures, which outline how resources are protected. For example, a password policy would outline password construction rules, rules on how to protect the passwords and how often to change 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 are changed on critical devices (Guel, 2007). This step consists of documents guiding individuals and organisations through user instructions, security plans, non-disclosure agreements and follow-up activities of the documented systems.

3.2.4 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 asset classification, risk analysis, audits and incident reporting systems.

3.2.5 Awareness Creation: Step 5

This step refers to the process of making people understand and aware of 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). The human factor is the biggest threat to IS and assets and ironically, is also the best way to prevent loss. This implies that lack of awareness can lead to a variety of security issues.

3.2.6 Implementation Index

The sequence of steps shown in the model illustrates the ideal sequence of combined security measures for library ISec. However, there is a possibility that some measures were more fully implemented than the others. The implementation index based on the Information Security Measure Benchmark (Information-Technology Promotion Agency, 2008) was applied to the model to create an instrument that can be used to assess the level of implementation of ISec measures in a library. At each level, the variables are measured based on five status of implementation scores (1 = Not

Implemented to 5 = Fully Implemented) that reflect the attributes of implementation (Table 3.1).

Table 3.1: Levels of Implementation of Information Security Measures in Libraries

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

(Source: Information-Technology Promotion Agency. 2008)

3.5 Research Methodology Related To Information Security Management

Review of previous work relating to research approaches used in the area of ISec indicates that surveys and case studies are the most popular methods used in ISec research. Bolan and Mende (2004) identified that the most popular approaches used by researchers in three computer security journals and articles published in 2000 until 2004 included subjective/argumentative, case studies, surveys, action research, experiments, grounded theory, ethnography, theorem proof, simulation and forecasting.

Review of literature related to ISec threats and countermeasures indicated that surveys and questionnaires are the most popular research method and data gathering technique utilised by researchers. For instance, Loch and Carr (1991) adopted a survey to examine the organisation's view on ISec threats in Atlanta based on questionnaires sent to the Directors of Management of IS (MIS) or MIS security in various organisations in Atlanta, Georgia. Loukis and Spinellis (2001) investigated ISec measures and its associations with the context factors (number of IS users, number of IS staff, connection

to Internet and etc.) in the Greek public sectors by means of a structured questionnaire. May and Lane (2006) examined the current status and key issues of ISM in tertiary environment using the survey instrument administered to all Australian Vice Chancellor-listed universities. Yeh and Chang (2007) identified the threats and countermeasures for IS security in Taiwanese enterprises using mail questionnaires. Hagen, Albrechtsen and Hovden (2008) in their survey explored the relationship between implementation and effectiveness of security measures through a web-based questionnaire among ISec managers in a selection of Norwegian organisations.

Galliers (1991) presented a taxonomy of IS research approaches based on suitability of different research methods in the context of: 1) research objects (having an impact on society, an organisation or group, or an individual); 2) whether the concentration is on technological or methodological factors; and 3) the process of theory building, testing or extension (Table 3.2). Thus, this research adopted a survey method to obtain a snapshot of ISec threats and security practices at a particular point in time, which is deemed appropriate for a project impacting Malaysian academic libraries (organisations), and also where the concentration is on process (methodology) rather than technology itself.

Table 3.2. Information System Research Approaches: A Revised Taxonomy (Galliers, 1991, p.168)

OBJECT	Modes for traditional empirical approaches (observation) (interpretations) →					Modes for newer approaches →			
	Theorem Proof	Laboratory Experiment	Field Experiment	Case Study	**Survey**	Forecasting and Future Research	Simulation and Game or Role Playing	Subjective or Argumentative	Descriptive or Review
Society	No	No	Possibly	Possibly	**Yes**	Yes	Possibly	Yes	Yes
Organisation or Group	No	Possibly	Yes	Yes	**Yes**	Yes	Yes	Yes	Yes
Individual	No	Yes	Yes	Possibly	**Possibly**	Possibly	Yes	Yes	Yes
Technology	Yes	Yes	Yes	No	**Possibly**	Yes	Yes	Possibly	Possibly
Methodology	No	No	Yes	Yes	**Yes**	No	Yes	Yes	Yes
Theory Building	No	No	No	Yes	**Yes**	Yes	Yes	Yes	Yes
Theory Testing	Yes	Yes	Yes	Possibly	**Possibly**	No	Possibly	No	Possibly
Theory Extension	Possibly	Possibly	Possibly	Possibly	**Possibly**	No	No	No	Possibly

3.6 Population and Sample

There are two important considerations when embarking on research in the ISec field: 1) the research should addresses an area of importance to the organisation, and 2) the information gained from the research can be applied in practice within the organisation (Suhazimah, 2007). Many factors influence the implementation of ISec measures in a library; hence it is necessary to examine the libraries in their natural setting. The population in this study is libraries in Malaysia. Malaysia has several types of libraries, including the National Library, academic libraries, special libraries, public libraries and school libraries. Based on purposeful sampling, the targeted sample chosen for the context of actual study are academic libraries because of the higher level of ICT implementation compared to other types of libraries. Since the population of all academic libraries at public universities, private universities and college universities in Malaysia is small (57), all academic libraries at these three types of universities were chosen for study, excluding the small academic libraries at private colleges. It was recognised that this may create disproportionate numbers of small libraries, but if

stratified sampling was done, the sample population would have been too small to provide meaningful results.

Another issue that rose in ISec literature is the sensitive nature of surveys that ask questions about ISec practices. Previous research reported that many companies are reluctant to provide hard data regarding computer abuse or security practices because of the extremely sensitive nature of the topic (Kotulic and Clark, 2004; Straub and Welke, 1998). Based on the lessons offered in the literature and due to the sensitive nature of the topic, researchers investigating ISec practices should proceed with caution, and as an alternative, should opt to use professional subjective judgment to questions posed. Thus, the unit analysis in this study is the individual designated to be responsible for the security of IS or IT in an academic library.

This study seeks to capture the ISec threats and practices of academic libraries, therefore the target individuals are the middle and top management group that are the custodian and implementers of ICT related to library functions and services. Only one individual may be sampled from each academic library, which depends on the designated Head of ICT Department, ICT Librarian, ICT Manager, ICT Officers or ICT Executive responsible for the System or IT Division/Unit/Department in an academic library. The common characteristic of these people is that all of them are either directly or indirectly responsible for the safeguarding or protection of the library's information system assets.

3.4.1 Unit of Analysis

The unit of analysis for this study was academic library. The questionnaire enquired individuals about their perception regarding the security postures with respect to threats and countermeasures within the context of their academic libraries. The goal of using the academic library as the unit of analysis was to provide findings that were useful to academic libraries in assessing their current state of IS security threats and practices, as well as to provide a metric with which to compare academic libraries of similar characteristics and types.

The scope of targeted libraries covers all the academic libraries in Peninsular Malaysia, and also Sabah and Sarawak in East Malaysia. The total number of academic libraries in Malaysia is based on the total number of public universities and private universities in Malaysia (see Table 3.3 and Table 3.4).

Table 3.3. List of Public Universities and Year of Establishment

No.	Public Universities	Year of Establishment
1	University of Malaya (UM)	1962
2	Science University of Malaysia (USM)	1969
3	National University of Malaysia (UKM)	1970
4	Putra University Malaysia (UPM)	1971
5	University of Technology Malaysia (UTM)	1975
6	International Islamic University Malaysia (IIUM)	1983
7	Northern University Malaysia (UUM)	1984
8	University of Malaysia, Sarawak (UNIMAS)	1992
9	University of Malaysia, Sabah (UMS)	1994
10	Sultan Idris University of Education (UPSI)	1997
11	MARA University of Technology (UiTM)	1999
12	Universiti Sultan Zainal Abidin (UNISZA)	2005
13	Islamic Science University of Malaysia (USIM)	1998 (2006)
14	University of Malaysia Terengganu (UMT)	1999 (2006)
15	Tun Hussein Onn University of Malaysia (UTHM)	2000 (2006)
16	University of Technical Malaysia Melaka (UTeM)	2000 (2006)
17	University of Malaysia Pahang (UMP)	2001 (2006)
18	University of Malaysia Perlis (UNIMAP)	2001 (2006)
19	University of Malaysia, Kelantan (UMK)	2006
20	National Defence University of Malaysia (UPNM)	2006

* Year in bracket indicates the year upgraded to University status)
(Source: IPTA Management Sector, Ministry of Higher Education Malaysia, 2010)

Table 3.4: List of Private Universities and Year of Establishment

No.	Private Universities	Year of Establishment
1	Universiti Tenaga Nasional (UNITEN)	1999
2	Universiti Tun Abdul Razak (UNIRAZAK)	2000
3	Multimedia University (MMU)	1999
4	Universiti Teknologi Petronas (UTP)	2000
5	Malaysia University of Science and Technology (MUST)	2000
6	University of Nottingham Malaysia Campus (UNMC)	2000
7	Monash University Malaysia (MUM)	2000
8	Curtin University of Technology Sarawak, Campus Lutong (CUTS)	2000
9	Industrial University of Selangor (UNISEL)	2001
10	International Medical University (IMU)	2001
11	AIMST University (AIMST)	2001
12	Open University Malaysia (OUM)	2001
13	Universiti Tunku Abdul Rahman (UTAR)	2002
14	Universiti Kuala Lumpur (UniKL)	2002
15	Management and Science University (MSU)	2002
16	Kuala Lumpur Infrastructure University College (KLIUC)	2003
17	Limkokwing University	2003
18	UCSI University	2003
19	Twintech International University College Of Technology (TWINTECH)	2003
20	Sunway University	2010
21	Asia Pacific University College of Technology and Innovation (UCTI)	2004
22	Kolej Universiti Islam Antarabangsa Selangor (KUIS)	2004
23	HELP University College (HUC)	2004
24	Binary University College of Management & Entrepreneurship (BUCME)	2004
25	Swinburne University of Technology, Campus Sarawak (SUT)	2004
26	Cyberjaya University College of Medical Sciences (CUCMS)	2005
27	INTI International University (INTI IU)	2010
28	Kuala Lumpur Metropolitan University College (METROPOLITAN)	2006
29	Kolej Universiti Insaniah (KUIN)	2006
30	TAYLOR's University	2010
31	Al-Madinah International University (MEDIU)	2007
32	International Centre for Education in Islamic Finance (INCEIF)	2007
33	Asia e University (AeU)	2007
34	Nilai University College	2007
35	TATI University College (TATIUC)	2007
36	Wawasan Open University (WOU)	2007
37	Albukhary International University	2007

(Source: IPTS Management Sector, Ministry of Higher Education Malaysia, 2010)

All academic libraries in Malaysia as listed by the Ministry of Higher Education Malaysia (2010) were selected to produce a representative sample and to reduce sampling errors (Table 3.5). These academic libraries were selected based on the assumption that they have automated library systems and provide Internet access and online services to their patrons. A total of 57 questionnaires were distributed at each

respective academic library either by hand, post or e-mail depending on their locations. The researcher aimed to collect 51 questionnaires with 10% allowance for non-return rate and spoilt questionnaires. Targeting a specific individual within an academic library would increase the accuracy and quality of response because the individual chosen, due to the nature of his role and responsibilities, is in the most relevant position to provide the desired information.

Table 3.5: Number of Academic Libraries in Malaysia as at 2008

Academic libraries	N	% of total population (N)	Estimate response
Public universities	20	35%	20
Private universities	22	39%	22
University Colleges	15	26%	15
Total	57	100%	57

(Source: Ministry of Higher Education Malaysia, 2009)

3.5 Research Instruments

The instrument used to collect data for this study is a structured questionnaire. The survey research is believed to be well understood and applied by management IS scholars. It has been applied for several years and it has precise procedures that, when followed closely, yield valid and easily interpretable data (Pinsonneault and Kraemer, 1993). Surveys are useful in describing the characteristics of a large population, whereas no other method of observation can provide this general capability. Fowler (1984) indicates that there are several elements in the conduct of surveys that can be used to assess the quality of survey research. These elements include: (a) research design, (b) sampling procedures and (c) data collection methods. These elements and their related dimensions constitute the framework used to assess survey research methodology in management of IS.

The design of the survey instrument was completed following a comprehensive literature review, which directly affected the design of the questions. The sections of the survey that were designed each deal with a specific section of the research: a) Part A deals with questions related to demographic profiles of academic libraries and demographic profiles of respondents; Part B deals with questions related to the most common ISec incidences, frequency of ISec incidence occurrences and the most common perceived source of ISec threats experienced by academic libraries, and b) Part C deals with questions pertaining to the level of implementation of technological and organisational measures in academic libraries. Questions related to academic libraries' profile, respondents' profile and the source of ISec threats were assessed based on multiple choices. These scales consist of a few possible responses from which respondents may select either one or more responses. The indicator for occurrence of ISec threats experienced by academic libraries requires responses to a Likert-scale to measure the frequency of the threats. In contrast, the indicator level of implementation of technological and organisational measures in academic libraries were assessed based on the five status of implementation scores (1 = Not Implemented to 5 = Fully Implemented) that reflect the attributes of implementation (Table 3.1). A complete questionnaire with its cover letter can be referred in Appendix A.

3.5.1 Validity of the Measurement

Content validity can be identified via three sources, including literature, representativeness of the relevant population and experts (Burns and Grove, 2004). The instrument for this study was developed through several stages, as follows: First, a sample of items for relevant ISec threats and countermeasures was identified by employing an exhaustive review of literature generally on ISec and IS security threats and safeguarding measures. In order to better understand the current security threats in

academic libraries, this study categorised each threat based on hardware threats, software threats, network threats, data threats, physical threats and human-related threats. The list of threats under each category was based on the index or list of threats developed by Centers for Medicare and Medicaid Services (2005), Farahmand, et al. (2003), Yeh and Chang (2007), Samy, Rabiah and Zuraini (2009) and other researchers (Table 3.6).

Table 3.6. Types of Information Security Threats

Threats	Descriptions	Representative References
Hardware security threats	Threats of physical damage to physical components in an information system.	Farahmand, et al. (2003); Samy, Rabiah and Zuraini, (2009).
Software security threats	Threats that jeopardise the operating systems and related applications.	Farahmand, et al. (2003); Gawde, (2004); Samy, Rabiah and Zuraini (2009).
Network security threats	Threats related to the network such as virus and hackers	Williams (2001); Farahmand, et. al. (2005b); Eisenberg and Lawthers (2005); Mell, Kent and Nusbaum (2005); Yeh and Chang (2007); Samy, Rabiah and Zuraini (2009).
Data security threats	Threats related to data, such as unauthorised access.	Adam (1992).
Physical and environmental security threats	Threats due to interference of natural disasters such as fires and flooding.	Lindstrom (2003); Tittel et al. (2003); Samy, Rabiah and Zuraini (2009); Vacca (2009).
Human-related threats (Other security threats)	Threats from humans or users such as human errors.	Pipkin (2000); Centers for Medicare and Medicaid Services (2005); Lindstrom (2003); Conklin, et al. (2005); Samy, Rabiah and Zuraini (2009).

Similarly, the relevant security countermeasures listed in this study were those identified by Eisenberg and Lawthers (2005), Rajendran and Rathinasabapathy (2007), Yeh and Chang (2007) as well as by other relevant researchers (Table 3.7). The identified security countermeasures were each classified into the respective dimensions of LISAM.

Table 3.7: Types of Information Security Controls or Security Measures

Security Control	Descriptions	Representative References
Technological security	The technical mechanisms or controls that are put in place to protect hardware, software, workstation, network, server, data and physical facilities security.	INTOSAI (1995); Bryson (1997); Ormes (2001); Thiagarajan (2003), Yasin (2002); Banerjee (2003); Ferrer and Mead (2003); Oder (2004); Shahid (2005); Eisenberg and Lawthers (2005); Ohaya (2006); Ortiz-Caceres (2006a); Rajendran and Rathinasabapathy (2007); Yeh and Chang (2007).
Information Security policy	Policies that state job responsibilities, acceptable use of library IS, backup policy, privacy and confidential policy, asset protection policy, data classification policy, wireless device policy and authorisation policy.	Weise and Martin (2001); Thiagarajan (2003); EDUCAUSE/Internet2 Security Task (2004); Eisenberg and Lawthers (2005); Breeding (2006); Yeh and Chang (2007).
Procedures and controls	Any documented procedures and formal practices to manage the selection and execution of IS security policies including disciplinary controls, confidentiality agreement, requirement for outsourced activities and intellectual property rights.	Thiagarajan (2003); Adomi and Eruvwe (2004); Yeh and Chang, (2007).
Administrative tools and methods	Any proactive and reactive means in assuring security of IS such as asset classification, risk analysis, audits and incident reporting systems.	Thiagarajan (2003); Yeh and Chang, (2007).
Awareness creation	The existence and maintenance of ISec awareness initiatives via security trainings, active user participation, awareness programmes and the top management support.	Pethia (2003); Thiagarajan (2003); Hight (2005); Im and Baskerville (2005); Kimwele, Mwangi and Kimani (2005); Merkow and Breithaupt (2005); Vaast (2007); Yeh and Chang (2007); Zoughbi (2009); Dlamini, Eloff and Eloff (2009).

3.5.1.1 **Pre-Testing the Instrument for Content Validity**

Content validity refers to the extent to which the items, questions and measures reflect or represent the specific or the real construct domain and eliminates undesirable items to a particular construct. Although content validity is a highly desirable and

recommended practice in order to ensure rigour in any empirical research, its application is limited in ISec research (Straub, Boudreau, and Gefen, 2004). This study involves designing and building a new survey instrument, thus pre-testing the instrument is undeniably essential to examine the questionnaire for any ambiguity, misleading or unclear terminology. As asserted by Boudreau, Gefen and Straub (2001), every instrument should be pretested as a preliminary step to ensure that there are no unanticipated difficulties. The literature suggested a range of 2 to 20 content experts to be selected to review relevant and clarity of research instrument (Malmgreen, et al. 2009). However, in this study a total of five individuals were involved in the pre-testing exercise. They include two IS librarians, one IS executive and two academicians. The objectives of this pre-testing approach were to obtain feedback for improvement before finalising the questionnaire and to identify relevant items that adequately cover relevant dimensions on ISec threats and safeguarding measurements in a library setting.

A copy of the drafted instrument along with an introductory letter that explains the research objectives, instructions and definitions of key terminologies was sent to each of these individuals by hand or e-mail depending on their locations. These individuals were asked to respond in three ways based on D'Arcy's approach (2005): (1) to indicate whether they felt that the individual items and the scenarios serve to answer the larger research-guiding questions; (2) to recommend other items that they felt would be useful for the survey, and (3) to comment on content and structure of the instrument as a whole. The feedback focused mostly on suggestions to improve the instrument for readability, clarity and usefulness for gathering the required data. Major changes resulted from this feedback, including revision to the wording of some threats questions to eliminate ambiguities and make the statements for security countermeasures more concise. For instance, question 17.1 in the Hardware Security was reworded greater

concision: “Surveillance systems at strategic places, public computer areas and server areas (e.g. use of CCTV, visual camera, magnetic detection system and electronic anti theft system)” was changed to “CCTV, visual camera, magnetic detection system and electronic anti theft system at strategic places, public computer areas and server areas”. Minor changes also resulted from this feedback, including the omission of question 23.7 in Part C (Presence of Hardware Security Threat), the question 23.7 “Physical sabotage or intentional destruction of computing equipments” was replaced with question 23.8 “Theft, physical sabotage, vandalism of ICT hardware equipments”, which carries a similar meaning. Additional items were also suggested for the ‘Presence of ISec Policy’ and ‘Presence of Awareness Creation’ sections. Thus, the results of the pretest suggested that the instrument possessed adequate content validity.

3.5.1.2 Pilot Study

The corrected version of the instrument was finally adopted and piloted in order to determine approximate length of the survey in terms of time as well as to further refine the instrument. As indicated by Phelps (2005), the pilot test of the instrument included opportunities for comments relating to the clarity and content of the instrument. The proposed questionnaire was piloted based on the convenience sample of 110 public and special libraries in Malaysia between the months of September 2009 and November 2009. When choosing the public and special libraries, the same criteria are applied as for the academic libraries, i.e. that the libraries have automated library systems as well as provided Internet and online services.

The questionnaires were distributed to the individual responsible for ISec or IT in the public or special library, either by post, hand or e-mail attachment depending on locations of the libraries. Each questionnaire booklet or email attachment was attached

with an introductory letter that explains the research objectives, instructions and definitions of key terminologies together with self-addressed and stamped envelope. Some follow-up telephones calls and reminders via e-mails were made to encourage respondents to answer and return the questionnaires. A total of 110 questionnaires were distributed and a total of 50 (constituting 45%) useable questionnaires were collected at the time of data collection (Table 3.8).. Minor changes resulted from this feedback, including a modification to choice of answers for question five, i.e. 'Numbers of PC/workstation with Internet connection for patrons in your library' in the Library Profile section to conform more directly to the actual scenarios. Also, in the initial sections, Part B (a list of the most common ISec incidents experienced by organisations) and Part C (a list of ISec safeguarding measures) were exchanged in order to encourage a higher response rate, as the researcher believed that the questions listed in Part C were more difficult to answer than questions listed in the Part B.

Table 3.8. Breakdown of Questionnaire Distribution for Pilot Test

Type of Libraries	N*	Distributed	% of Distributed	Response Obtained	% of Returned
Public libraries	15	15	100%	10	66.7%
Special libraries (Public)	497	55	11.0%	30	54.5%
Special libraries (Private)	93	40	43.0%	10	25.0%
Total	**605**	**110**	**18.2%**	**50**	**45.5%**

(* Source: National Library of Malaysia, 2008)

3.5.2 Reliability of the Measurement

A research instrument must be evaluated in terms of reliability and validity (Kerlinger, 1986). Reliability refers to the extent to which the measures give consistent results and can be improved via a pretest or a pilot test. Cronbach's alpha was used to evaluate the consistency of the responses for each item within the instrument. Cronbach's alpha is an index of reliability associated with the variation accounted for by the true score of the underlying construct. The construct is a hypothetical variable that is being measured (Hatcher, 1994). Alpha coefficient value from 0 to 1 and may be used to describe

internal consistency, the reliability of factors extracted from dichotomous (i.e. questions with two possible answers) and multi-point formatted questionnaires or scales (e.g. with a rating scale: 1 = poor, 5 = excellent). A commonly-accepted rule of thumb is that an Alpha (α) of 0.7 indicates acceptable reliability, and 0.8 or higher indicates good reliability. The goal in designing a reliable instrument is for scores on similar items to be related (internally consistent), but for each to contribute some unique information as well (Nunnally, 1978; Akuezuilo and Agu, 2002; and Vaus, 2004).

Cronbach alpha values for the various items of the instrument used in this research are shown in Table 3.9. The five components for ISec safeguarding measures in libraries used in this research have Cronbach alpha values in the .70 to .80 range. ISec policy is shown to have the highest reliability as alpha is .844, whereas procedures and controls is shown to have the lowest reliability as alpha at .689. This reliability value provide statistically sound justification for continuing to use all the research items for the real sample, as reliability coefficient of .70 or higher is considered acceptable in most social science research situations (Nunnally, 1978; Akuezuilo and Agu, 2002; and Vaus, 2004).

Table 3.9: Cronbach's Alpha Scores for the Various Items in the Survey Instrument.

Section	Themes of Items on Survey	Cronbach's Alpha (Pilot Test)
1	Type of ISec incidents experienced by my academic library in the last six months	.940
2a	Presence of technological countermeasures in my academic library	.699
2b	Presence of ISec policies in my academic library	.844
2c	Presence of ISec procedures and controls in my academic library	.689
2d	Presence of ISec administrative tools and methods in my academic library	.705
2e	Presence of ISec awareness creation in my academic library	.755

3.6 Data Collection

In this research, survey is adopted for data collection procedure due to economy of design and the rapid turn-around in data collection. Judging from the relatively new issues of ISec management in libraries, many librarians may have difficulty in articulating their own responses. As indicated by Suhazimah (2007), asking respondents to give their response about scenarios or statements, based on their individual, attitude and the practices in an organisation will invite higher and better quality response. Following Suhazimah's (2007) approaches, the statements in the questionnaire were grouped into themes and assessed based on multiple choices and Likert-scale so that the respondent is prepared to answer with the appropriate mainframe. Since this study was aimed to answer provide empirical data from natural settings, a self-administrated survey design was deemed appropriate as it allows the respondents to answer with no interference from the researcher as well as allowing anonymity, thus encouraging forthrightness and honesty due to the highly sensitive information involved.

A questionnaire was sent to the individual responsible for the information system, IT or Information Communication and Technology Division/Unit/Department in an academic library, such as the Head of ICT Department, ICT Librarian, ICT Manager, ICT Officer or ICT assistant. The time scope for information pertaining to security incidents and trainings are limited to the respondents' experience of the last six months. However, there is no timeframe reference for other aspects of the study. The respondents only needed to draw answers from their own beliefs, perceptions and knowledge regarding prevalent IS security practices of their library.

However, this method of data collection has the risk of a low response rate and no assurance that the questions were understood. In order to address the risk of incomprehensible questions, a pre-test of the questionnaire with an enclosed booklet that provides a list of definitions of key terms became the mitigating measure. As for the issue of low response rate, the researcher adopted the strategy of having personal contact in advance with some respondents and enclosing each questionnaire booklet with a self-addressed, stamped envelope and a cover letter explaining the purpose of the study along with the requisite statements that participation was voluntary and that no personally identifiable information was being gathered.

3.6.1 Data Collection Process

The whole administration of the questionnaire took about four months to complete (January 2010 until April 2010). The questionnaires were distributed to the targeted respondents from all academic libraries in Malaysia either by post, hand or e-mail depending on their locations. The respondents were expected to return the questionnaires within one to two weeks. Approximately a week after the questionnaires were sent, some follow-up telephone calls were made and e-mail reminders were sent to encourage respondents to return the survey questionnaires. Approximately three weeks after the initial follow-up telephone calls and e-mail reminders were sent, follow-up emails were sent again thanking those who had already responded and encouraged those who had not. The bulk of responses were received after three to four weeks of the questionnaire distribution.

Finally, upon completion of the data collection, Cronbach's alpha was calculated to ensure internal consistency within the six sections of the survey instrument, those involving separate questions to determine the overall score within that section based on

a summation of the individual questions. The five constructs for IS safeguarding measures in libraries used in the actual research have Cronbach's alphas in the .80 to .90 range, which is considered acceptable (Table 3.10). This reliability values provide statistically sound justification to use all the research items for the different samples i.e. for academic libraries, as reliability coefficient of .70 or higher is considered acceptable in most social science research situations (Nunnally, 1978; Akuezuilo and Agu, 2002; and Vaus, 2004).

Table 3.10: Cronbach's Alpha Scores for the Various Items in the Survey Instrument.

Section	Themes of Items on Survey	Cronbach's Alpha (Actual Study)
1	Type of ISec incidents experienced by my academic library in the last six months	.958
2a	Presence of technological countermeasures in my academic library	.949
2b	Presence of ISec policies in my academic library	.867
2c	Presence of ISec procedures and controls in my academic library	.921
2d	Presence of ISec administrative tools and methods in my academic library	.898
2e	Presence of ISec awareness creation in my academic library	.930

3.7 Response Bias

Before proceeding to data analysis, absence of response bias was established. Response bias is the effect of non-responses on survey estimates (Fowler, 1984). This procedure examines the scenario that if the non-respondents had responded, their responses would have substantially changed the overall results of the survey (Suhazimah, 2007). The non-response analysis may be performed to identify characteristics that may differ between respondents and non-respondents in order to potentially clear out any bias that may exist within a dataset. While directly inquiring non-respondents as to the reasons for not participating in the study would be ideal, it would be unlikely that such non-participants would respond to further inquiries given their lack of participation in the

initial inquiry. Another method of assessing non-response bias is to compare early responders and late responders to the survey. Table 3.11 below displays a means comparison between the early and late responders. An independent sample t-test was performed against responses to ten demographic variables. The table illustrates that there are no significant differences at the .05 level of significance between early and late respondents.

Table 3.11: T- Test for Non Response Bias

Demographics	Early respondents (n=15)	Late respondents (n=15)	t-value	p-value
Total Number of Staff	2.4000	2.8000	-.972	.348
Number of Staff PCs	2.5333	2.7333	-.400	.695
Types of Operating Systems	4.7333	3.8667	.638	.534
Percentage of IS Security Budget	2.4000	2.0000	.802	.443
Availability of IS Security Staff	.8000	1.2000	-1.000	.334
Years in ICT Implementation	2.2667	2.8000	-1.372	.192
Academic Qualification	3.4000	2.9333	1.974	.068
Numbers of IS Conferences/Workshops/Trainings Attended	.8667	.5333	-.972	.348
Types of Ownerships	2.0000	1.9333	.193	.849
Types of Universities	1.9333	1.6667	.845	.413

p> .05. 100%

3.8 Data Analysis Strategy

The information from the questionnaire was coded and compiled using Statistical Package for Social Sciences (SPSS) for Windows Version 17.0 for statistical computation and evaluation. A range of statistical analysis techniques were used to capture the descriptive profile of academic libraries, respondents, ISec threats and ISec practices of the academic libraries. The level of measurement for the quantitative data is in nominal, ordinal and interval values. The data was analysed using descriptive statistics (Table 3.12). Descriptive statistics was used to show the distribution process including frequency, percentage, mean and standard deviations. The descriptive data was used to present the profile of academic libraries and respondents (individuals

responsible for IS and IT in the library). Other descriptive statistics included the ISec breaches, sources of ISec breaches, types of safeguard technological and organisational measures deployed the libraries. All these present the IS security threats and practices of Malaysian academic libraries.

Table 3.12: Data Analysis Strategy: Approaches for Solving the Research Questions.

No.	*Research Questions*	*Approaches*
1.	What is the IT infrastructures in Malaysian academic libraries in terms of number of PC allocations, availability of wireless connection, type of operating system used, years of ICT adoption, percentage of IS security budget and availability of IS security staff?	Descriptive analysis of number of PCs allocations for patrons and staff, availability of wireless connection, type of operating system used, years of ICT adoption, percentage of IS security budget and availability of IS security staff.
2.	What are the most common perceived IS security threats and frequency of their occurrence in terms of hardware, software, data, network and human-related threats in these academic libraries?	Descriptive analysis of hardware threats, software threats, data threats, network threats, physical and human-related threats. Descriptive analysis of frequency of occurrence of hardware security threats, software security threats, data security threats, network security threats, physical security threats and human-related threats.
3.	What is the most common perceived source of ISS threats in Malaysian academic libraries?	Descriptive analysis of the most common perceived source of ISec threats.
4.	What is the level of implementation of technological measures (in terms of hardware security, software security, workstation security, network security, server security, data security and physical security measures) in Malaysian academic libraries?	Descriptive analysis of types and level of implementation of hardware security, software security, workstation security, network security, server security, data security and physical security measures in Malaysian academic libraries.
5.	Are there significant differences between academic libraries in Malaysia in applying the technological measures based on type of universities, number of staff, years in ICT adoption, yearly ISec budget, availability of IS security staff and availability of wireless connection?	Kruskal-Wallis test and Mann-Whitney U Test for testing the differences between Malaysian academic libraries in applying technical measures. The hypothesis was separated into six sub-hypotheses and every sub-hypothesis is tested separately.

Table 3.12: Continued

No.	*Research Questions*	*Approaches*
6.	What is the level of implementation of organisational measures (in terms of hardware security, software security, workstation security, network security, server security, data security and physical security measures) in Malaysian academic libraries?	Descriptive analysis of types and levels of implementation of security policies, procedures and controls, tools and methods and awareness activities in Malaysian academic libraries.
7.	Are there significant differences between academic libraries in Malaysia in applying organisational measures based on universities, number of staff, years in ICT adoption, yearly ISec budget, availability of IS security staff and availability of wireless connection?	Kruskal-Wallis test and Mann-Whitney U Test for testing the differences between Malaysian academic libraries in applying organisational measures. The hypothesis was separated into six sub-hypotheses and every sub-hypothesis is tested separately.
8.	What is the overall implementation status of technological security measures and organisational security measures in Malaysian academic libraries?	Descriptive analysis of overall status of technological measures and organisational measures based on the proposed library ISec measures assessment tool for library.

3.9 Instrument to Assess Status of Implementation

Not much is known about the actual scenario of ISec practices specifically in the library setting. Thus, one cannot assert whether the library sector is lacking or adequate in information security. As highlighted by Newby (2002), ISec is often under-appreciated in libraries and this is surprisingly as information is the library's main business. Therefore, we attempt to propose an assessment tool for assessing the current ISec practices deployed by Malaysian libraries in managing their information security. This assessment tool is designed based on the proposed Library Information Security Assessment Model (LISAM) to encourage academic libraries to adopt best practices for ISec measures. It represents a roadmap for the implementation, evaluation and improvement of IS security practices for a library that adopts it.

3.9.1 Assessment Tool and Scoring Tool

A scoring tool is designed specifically to determine the overall score for ISec safeguarding measures in a library as well as a total score for each component of ISec measures. This tool is an adaptation from the Information Security Governance (ISG) Assessment Tool for Higher Education. The ISG assessment tool was developed by the Security Risk Assessment Working Group of the EDUCAUSE/Internet2 Computer and Network Security Task Force (EDUCAUSE/Internet2 Security Task, 2004).

Tthe ISG assessment tool is meant to be used in higher education context and it can also be used with the LISAM model. The ISG Assessment Tool for Higher Education was designed to support the ISG framework recommended by the Corporate Governance Task Force and has been modified and can be used by institutions of varying sizes and types to gain a better understanding at a level of the role information security governance has in their organisations and how it can best be structured. The first section of the original assessment tool is used to assess an institution of higher education (HIE) reliance on information technology. The remaining sections are intended to help HIE determine the maturity of information security governance at a strategic level. The overall rating (good, needs improvement and poor) is depend on the raw score and an institution's reliance on information technology. In contrast, the proposed assessment tool in this study is created to evaluate the technological and administrative or organisational components of information security management in an academic library. This tool is intended for use by an academic library as a whole, although a unit within an academic library may also use it to help determine the maturity of its individual information security program.

(a) Assessing the Overall Implementation Status of Technological Measures

The library's overall implementation status of technological measures is evaluated by summing up all the seven sections of the technological components (sections i + ii+ iii + iv + v + vi + vii), and the summed score should be entered into the corresponding box (A) on this chart to determine the overall status of technological measures in a library (Table 3.13).

Table 3.13 Total Score for Technological Measures

TECHNOLOGICAL MEASURES		Low	High	Presence
Total Score for Presence of Hardware Security	i	0	2	Very Low
		3	5	Low
		6	10	Medium
		11	15	High
		16	20	Very High
Total Score for Presence of Software Security	ii	0	10	Very Low
		11	20	Low
		21	40	Medium
		41	60	High
		61	80	Very High
Total Score for Presence of Workstation Security	iii	0	2	Very Low
		3	6	Low
		7	12	Medium
		13	18	High
		19	25	Very High
Total Score for Presence of Network Security	iv	0	5	Very Low
		6	11	Low
		12	22	Medium
		23	33	High
		34	45	Very High
Total Score for Presence of Server Security	v	0	6	Very Low
		7	12	Low
		13	25	Medium
		26	37	High
		38	50	Very High
Total Score for Presence of Data Security	vi	0	9	Very Low
		10	18	Low
		19	37	Medium
		38	55	High
		56	75	Very High
Total Score for Presence of Physical Security	vii	0	5	Very Low
		6	11	Low
		12	22	Medium
		23	33	High
		34	45	Very High
TOTAL SCORE FOR PRESENCE OF TECHNOLOGICAL MEASURES (Presence of Hardware, Software, Workstation, Network, Server, Data and Physical Security) (i+ii+iii+iv+v+vi+vii= A)	A	0	42	Very Low
		43	85	Low
		86	170	Medium
		171	255	High
		256	340	Very High

The ISec measures assessment tool proposes a way to assess the status of technological measures in a library as illustrated in Table 3.14. The total score for presence of technological measures **(A)** is where **n** is the highest score for the total items in the technological component (68 items) with each question giving a maximum 5 points. In this case, the highest score **(n)** is 340, indicating the presence of technological measure in a library is very high. The presence of technological measures in a library is considered high **(e_2)** if the library's total scores for technological measures is at 75% of the full scale score **(n)**. The medium rate **(b_2)** should be very close to exactly half (50%) of the full scale score **(n).** The presence of technological measures in a library is considered low **(c_2)** if the library's total scores for the technological measures is at 25% of the full scale score **(n)**. The very low rate **(d_2)** should be very close to exactly half of **c_2,** or at 12%-13% of the full scale score **(n)**. The same formula is applied to assess the presence of each component in the technological measures such as the presence of hardware, software, workstation, network, server, data and physical security (section i, ii, iii, iv, v, vi and vii).

Table 3.14. The Proposed Scale for Assessing the Overall Implementation Status of Technological Measures

Example	Low	High	Presence
Total score for presence of technological measures	**d_1**= d_2x0 [0%]	**d_2**= c_2/2 [12%]	Very Low
	c_1= d_2+1 [13%]	**c_2**= b_2/2 [25%]	Low
	b_1= c_2+1 [25%]	**b_2**= n/2 [50%]	Medium
	e_1= b_2+1 [51%]	**e_2**= b_2+c_2 [75%]	High
	a_1= e_2+1 [76%]	**a_2**= **n** [100%]	Very High

(b) Assessing the Overall Implementation Status of Organisational Measures

Table 3.15 illustrates that a library's overall implementation status of organisational measures is evaluated by summing up all the four sections of the organisational components (section 1 + 2 + 3 + 4= B), and the summed score should be entered into the corresponding box **(B)** on this chart to determine the overall status of organisational measures in a library.

Table 3.15 Total Score for Presence of Organisational Measures

ORGANISATIONAL MEASURES		Low	High	Presence
Total Score for Presence of Information Security Policy	1	0	7	Very Low
		8	15	Low
		16	30	Medium
		31	45	High
		46	60	Very High
Total Score for Presence of Procedures and Controls	2	0	4	Very Low
		5	8	Low
		9	15	Medium
		16	22	High
		23	30	Very High
Total Score for Presence of Administrative Tools and Methods	3	0	2	Very Low
		3	6	Low
		7	12	Medium
		13	18	High
		19	25	Very High
Total Score for Presence of Awareness Creation	4	0	6	Very Low
		7	13	Low
		14	25	Medium
		26	37	High
		38	50	Very High
TOTAL SCORE FOR PRESENCE OF ORGANISATIONAL MEASURES (Presence of Information Security Policy, Procedures, Administrative tools and Awareness creation)	B	(1+2+3+4 =B)		

The same formula for assessing the overall implementation status of technological measures is applied to assess the presence of each component in the organisational measures (i.e. section 1, 2, 3 and 4) (Table 3.16). For example, the total score for the presence of ISec policy in a library **(1)** is where **n** is the highest score for the total items in the ISec policy component (12 items) with each question giving a maximum 5 points. In this case, the highest score **(n)** is 60, indicating the presence of ISec policy in a

library is very high. The presence of ISec policy in a library is considered high **(e_2)** if the library total scores for the technological measures is at 75% of the full scale score (n). The medium rate **(b_2)** should be very close to exactly half (50%) of the full scale score **(n).** The presence of ISec policy in a library is considered low **(c_2)** if the library's total scores for the ISec policy is at 25% of the full scale score **(n)**. Lastly, the very low rate **(d_2)** should be very close to exactly half of **c_2,** or at 12%-13% of the full scale score **(n)**.

Table 3.16. The Proposed Scale for Assessing the Total Score for Each Organisational Component

Example	Low	High	Presence
Total score for presence of ISec policy	**d_1**= d_2x0 [0%]	**d_2**= c_2/2 [12%]	Very Low
	c_1= d_2+1 [13%]	**c_2**= b_2/2 [25%]	Low
	b_1= c_2+1 [26%]	**b_2**= n/2 [50%]	Medium
	e_1= b_2+1 [51%]	**e_2**= b_2+c_2 [75%]	High
	a_1= e_2+1 [76%]	**a_2**= **n** [100%]	Very High

ISec measures assessment tool proposes a way to assess the status of organisational measures in a library as illustrated in Table 3.17. The status of organisational measures in a library is divided into poor, needs improvement and good implementation of organisational measures. These three levels of implementation status are further mapped according to the five different levels of implementation status for the technological measures. This implies that the actual overall status for organisational measures in a library is assessed based on the overall status of technological measures.

Table 3.17 Total Score for Organisational Measures

Status of Implementation of Technological Measures	Total Score for Presence of Organisational Measures		Status of Implementation of Organisational Measures
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

For instance, if a library has a very high implementation score for technological measures, the implementation status of the organisational measures in a library is considered good if the library's total score for the presence of organisational measures is between 131 to 165. However, a library's overall implementation of organisational measure is also considered good, if that library's total score for the presence of organisational measures is between 101 and 165, as the library has a low score for technological measures. The total score for the presence of organisational measures **(B)** is where **N** is the highest score for the total items in the organisational component (33 items) with each question giving a maximum of 5 points. In this case, the highest score **(N)** is 165. This N score is further prorated into three levels which are poor, needs improvement and good (see Table 3.18). A higher level of the implementation status of organisational measures (good) requires a higher total score for the presence of organisational measures.

Table 3.18 The Proposed Scale for Assessing the Overall Implementation Status of Organisational Measures

Status of Implementation of Technological Measures	Total Score for Presence of Organisational Measures		Status of Implementation of Organisational Measures
Very High	$v_1=0$	v_2= N-75	Poor
	$v_3= v_2+1$	v_4= N-35	Needs Improvement
	$V_5= v_4+1$	N	Good
High	$h_1=0$	h_2= N-85	Poor
	$h_3= v_2+1$	h_4= N-45	Needs Improvement
	$h_5= v_4+1$	N	Good
Medium	$m_1=0$	m_2= N-90	Poor
	$m_3= m_2+1$	m_4= N-55	Needs Improvement
	$m_5= m_4+1$	N	Good
Low	$l_1=0$	l_2= N-105	Poor
	$l_3= l_2+1$	l_4=N-65	Needs Improvement
	$l_5= l_4+1$	N	Good
Very Low	$w_1=0$	w_2= N-115	Poor
	$w_3= w_2+1$	w_4= N-75	Needs Improvement
	$w_5= w_4+1$	N	Good

(e) Assessing the Implementation Status of Information Security Measures

Based on this score, the academic library can identify whether its overall organisational security measures are good, needs improvement or poor as shown in Table 3.19. Later, from the overall scoring level, an academic 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.

Table 3.19. Overall Information Systems Safeguarding Measures Assessment Rating

Presence of Technological Measures	Total Score for Presence of Organisational Measures		Presence of Organisational Measures	Overall Assessment
Very High	0	90	Poor	Poor practices, organisational measures need immediate attention
	91	130	Needs Improvement	Good practice, but organisational measures need improvement
	131	165	Good	Very good practice
High	0	80	Poor	Poor practices, organisational measures need immediate attention
	81	120	Needs Improvement	Good practice, but organisational measures need improvement
	121	165	Good	Very good practice
Medium	0	70	Poor	Poor practices, technological measures need improvement and organisational measures need immediate attention
	71	110	Needs Improvement	Average practice, but organisational measures need improvement
	111	165	Good	Good practice, but technological measures need improvement
Low	0	60	Poor	Very poor practices, technological measures and organisational measures need urgent attention
	61	100	Needs Improvement	Poor practices, technological measures and organisational measures need immediate attention
	101	165	Good	Poor practices, technological measures need immediate attention
Very Low	0	50	Poor	Very poor practices, technological measures and organisational measures need urgent attention
	51	90	Needs Improvement	Poor practices, technological measures and organisational measures need immediate attention
	91	165	Good	Poor practices, technological measures need immediate attention

(n=1)

3.10 Chapter Summary

The chapter discusses the methodology that was used as the determining approaches toward meeting the research purpose and answering the research questions. Firstly, the research purposes, research questions and research hypotheses were listed, and then the framework of the study was proposed. The research model presented was the reference point of the research method and design adopted in the study. Research design chosen, methods and techniques used were then explained. Based on the literature, the type of IS security threats and countermeasures were listed and an instrument for assessing the

countermeasures was developed. Consequently, in the process, the instrument of the study was developed and later pre-tested and piloted. In order to make the instrument of this research correct and reliable, the researcher checked and confirmed the reliability and validity of the instrument based on the results of the pilot survey and actual survey. Finally, the strategy for data collection was discussed, whereby a self-administrated mail survey was to be deployed. Analysis of the data would include using statistical analysis software package SPSS Version 17.0. Descriptive analysis would be used to answer the research questions. The next two chapters are the highlight of the research where findings and analyses of the empirical evidences would be presented and discussed.

Chapter Four

Postures and the Perceived Information Security Threats in Malaysian Academic Libraries

5.0 Introduction

The focus of this chapter is the presentation of descriptive findings of an ISec survey conducted at Malaysian academic libraries. It explains the perceived ISec threats and the ISec practices generally adopted in these libraries. This chapter will answer Research Questions 1, 2 and 3 as articulated in the Chapter One.

At first, general information about survey distribution information and subsequent data collection results are presented. Section 4.2 then describes the demographic profiles of the respondents and the academic libraries they represent. Section 4.3 presents the ISec landscape of Malaysian academic libraries. It includes descriptive statistics profiles of perceived ISec threats, their frequency of occurrences as well as the origin of these security incidents experienced by these participating academic libraries.

4.4 Description of Survey and Data Collection Results

Academic libraries in Malaysia are generally referred to as a library that is attached to academic institutions, such as public universities, private universities and university colleges. Public universities in Malaysia are fully-funded by the Government and are governed as self-managed institutions. Private universities include locally established universities and branches campuses of foreign universities. The private universities and university colleges are mostly run by the private sector to provide tertiary education to school-leavers.

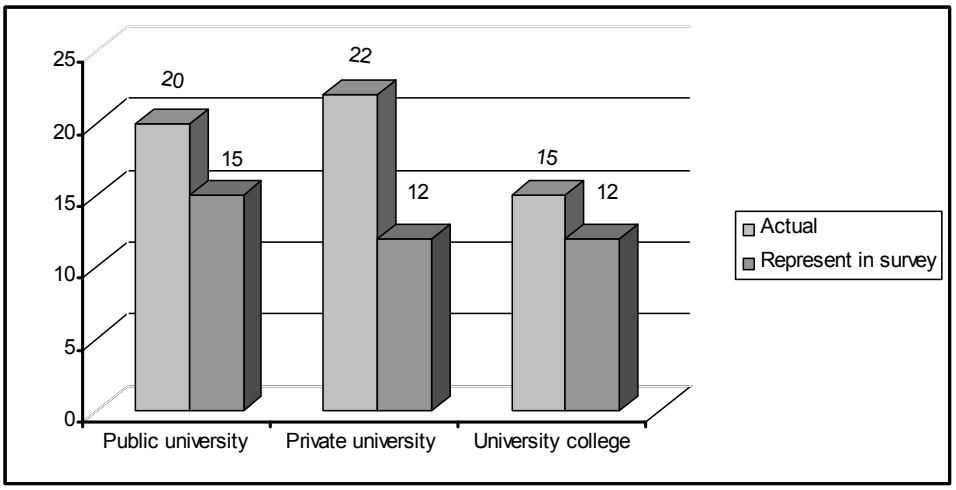
In this study, a total of 57 sets of printed questionnaires were distributed via post to all 57 academic libraries in Malaysia. Participants from these academic libraries represented locations across Peninsular Malaysia (West Malaysia) and extends to another region, Sabah and Sarawak (East Malaysia). A total of 39 participants completed the survey during the four months of data collection (Jan 2010 until April 2010), for a response rate of 68.4% (Table 4.1).

Table 4.1 Breakdown of Questionnaire Distributions and Response Obtained

Type of Academic Libraries	N	Distributed	Response Obtained	% of Returned
Public University	20	20	15	75.0
Private University	22	22	12	54.5
College University	15	15	12	80.0
TOTAL	**57**	**57**	**39**	**68.4**

These 57 survey invitations incorporated the academic libraries in Malaysia at three different types of universities, including 20 public universities, 22 private universities and 15 university colleges (Figure 4.1).

Figure 4.1. Comparison between Actual and Representation in the Survey



4.5 Descriptive Profiles of the Respondents

The heading "Profiles of Respondents" covers the outcomes of information related to the background of respondents, comprising: 1) the highest academic qualification of the

respondents; 2) the respondents' current position in the academic library; 3) the respondents' responsibility for ISec and IS security; 4) the number of IS formal training attended by the respondents; and 5) the respondents' perception towards role of IS in academic libraries.

Table 4.2 summarises the demographic characteristics of respondents. Respondents' highest academic status ranged from Master's degree to diploma. Most of the respondents had Bachelor's degrees (64.1%) and none of them had Doctorate degrees. This table also reveals that forty percent of respondents with Master's degrees worked in academic libraries in public universities. These findings may illustrate the growing need and supports for continuing education for librarians in public universities as compared with other academic libraries.

Table 4.2. Information Systems Staff Profile by Type of Academic Libraries

Characteristics		**Type of Academic Library at**			**n (%)**
		Public university	Private university	University college	
Highest academic qualification	Diploma	2 (13.3)	2 (16.7)	1 (8.3)	5 (12.8)
	Bachelor's degree	7 (46.7)	9 (75.0)	9 (75.0)	25 (64.1)
	Master's degree	6 (40.0)	1 (8.3)	2 (16.7)	9 (23.1)
Current position in academic library	IT Assistant	1 (6.7)	2 (16.7)	1 (8.3)	4 (10.3)
	IT Officer/Info Systems Officer	3 (20.0)	1 (8.3)	1 (8.3)	5 (12.8)
	Librarian/Library Executive	6 (40.0)	5 (41.7)	6 (50.0)	17 (43.6)
	Automation librarian	0 (.0%)	1 (8.3)	1 (8.3)	2 (5.1)
	Senior librarian	1 (6.7)	1 (8.3)	1 (8.3)	3 (7.7)
	Head of Automation Department	3 (20.0)	2 (16.7)	2 (16.7)	7 (17.9)
	Chief librarian/Deputy Chief Librarian	1 (6.7)	0 (.0%)	0 (.0%)	1 (2.6)

Table 4.2. Continued.

Characteristics		Type of Academic Library at			n (%)
		Public university	Private university	University college	
Responsibility for ISec and IS security	No	2 (13.3)	4 (33.3)	7 (58.3)	13 (33.3)
	Yes	13 (86.7)	8 (66.7)	5 (41.7)	26 (66.7)
Number of ISec Formal Training Attended	None	7 (46.7)	6 (50.0)	9 (75.0)	22 (56.4)
	1	4 (26.7)	4 (33.3)	2 (16.7)	10 (25.6)
	2	3 (20.0)	1 (8.3)	1 (8.3)	5 (12.8)
	3	1 (6.7)	0 (.0%)	0 (.0%)	1 (2.6)
	4 or more	0 (.0%)	1 (8.3)	0 (.0%)	1 (2.6)
Perception towards Role of IS in Academic Libraries	IS serve an important role, but are not critical to our library	4 (26.7)	3 (25.0)	3 (25.0)	10 (25.6)
	IS are critical to our library	11 (73.3)	9 (75.0)	9 (75.0)	29 (74.4)

The targeted respondents represent individuals who are responsible for ISec in their respective libraries, at the senior management, middle management or the operational level positions. Figure 4.2 shows the distribution of the respondents by their positions in academic libraries. The majority (90%) was from the management division, which include the Librarians or Library Executives (43.6%), Heads of Automation Unit (17.9%), IT Officers or IS Officers (12.8%), Senior Librarians (7.7%), Automation Librarians (5.1%) and Chief Librarians or Deputy Chief Librarians (2.6%). The remaining ten percent of the respondents were operational staffs (i.e. IT assistants). This breakdown implies that the results from the survey captured perception and knowledge from various key individuals in the academic libraries.

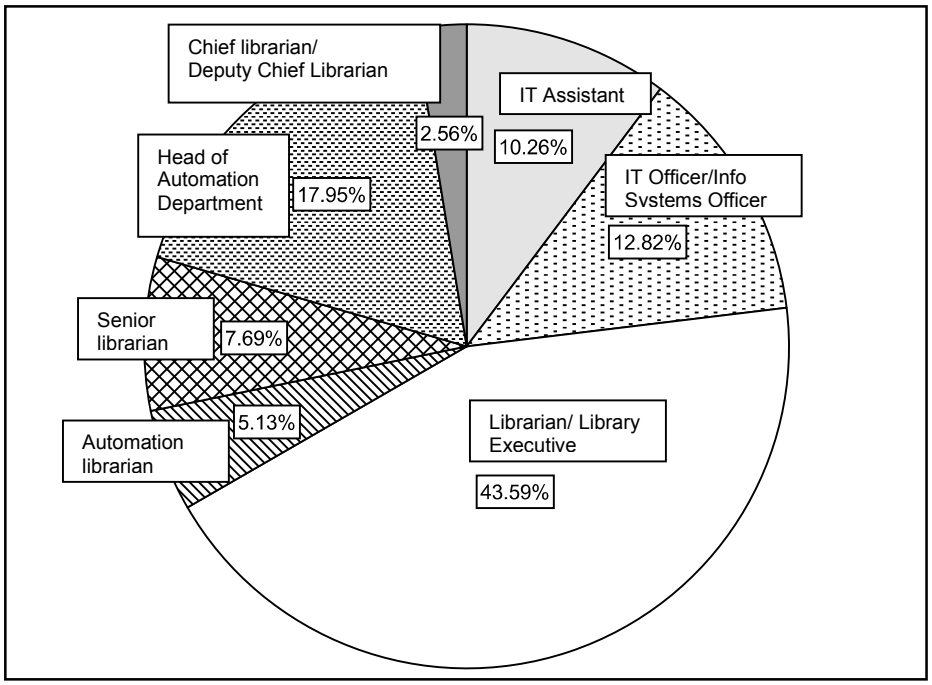


Figure 4.2 Distributions of Respondents by Positions in Academic Libraries

In term of responsibility for ISec and IS security, a majority of respondents (66.7%) indicated that they were responsible for ensuring security of information and IS in their respective academic libraries (Table 4.3). This finding again enhances credibility of the responses given on the perception and knowledge about the various type of IS security threats as well as the extent of IS security measures being adopted in their libraries. The results show that libraries in public and private universities have more librarians to oversee their ISec and IS security than libraries in university colleges. The smaller figure for university colleges may be due to the smaller library collection and thus. The libraries need only a small number of librarians or staff.

Table 4.3 highlights the proportion of respondents who are responsible for ISec and IS security, indicating that they are librarians or library executives, Head of Automation Department, IT Officer or IS Officers, Automation librarians, Senior Librarians as well as IT Assistants. This situation demonstrated how the responsibility for ISec and IS

security was placed on the shoulders of staff within a library regardless of position as people are the key to a secure organisation. As frequently quoted in the literature, "ISec is not the sole responsibility of just one ISec Officer but it is the responsibility of everyone in an organisation" (Qayoumi and Woody, 2005). In some academic libraries, the responsibility for ISec and IS security was given to fellow staff within IT departments or units in their respective universities.

Table 4.3. Information Security and IS Security Responsibilities in Academic Libraries

Responsible for info security and info systems security		Current position in library							Total
		IT Assistant	IT Officer/ Info Systems Officer	Librarian/ Library Executive	Automation librarian	Senior librarian	Head of Automation Department	Chief librarian/ Deputy Chief Librarian	
No	Count	2	1	5	0	2	2	1	13
	% within Current position	50.0%	20.0%	29.4%	.0%	66.7%	28.6%	100.0%	33.3%
Yes	Count	2	4	12	2	1	5	0	26
	% within Current position	50.0%	80.0%	70.6%	100.0%	33.3%	71.4%	.0%	66.7%
Total	Count	4	5	17	2	3	7	1	39
	% within Current position	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

Table 4.2 testifies that half of the respondents (56.4%) have not received any formal trainings and only less than five percent of them revealed that they have attended four or more formal training sessions in ISec and IS security in the last two years. It is apparent that these individuals did not receive adequate training to assist them in their roles as individuals who are responsible for ISec and IS security. Staff awareness and training are often considered key to successful IS security processes which are to impart the knowledge and skills needed to defend their systems (Smith and Jamieson, 2005).

4.5.1 Academic Libraries' Profiles

This section discusses the background information of participating academic libraries such as; 1) the academic libraries' ownerships; 2) the numbers of staff in academic libraries; 3) the number of patrons in academic libraries; 4) the availability of IS security staff in academic libraries; 5) the IT infrastructures in academic libraries; and. 6) the percentage of IS security budget in academic libraries.

There are almost equal representation of libraries from public universities (38.5%), private universities (30.8%) and university colleges (30.8%) in this survey. As highlighted in Table 4.4, all academic libraries in public universities in Malaysia in this study are owned by the government, whereas ninety-two percent of academic libraries in private universities and eighty-three percent of academic libraries in university colleges, respectively, are owned by private organisations.

Table 4.4 Profile of Academic Libraries

Characteristics		**Type of Academic Library**			**n (%)**
		Public university	Private university	University college	
Library Ownership	Government	15 (100.0)	0 (.0%)	2 (16.7)	17 (43.6)
	Private	0 (.0%)	11 (91.7)	10 (83.3)	21 (53.8)
	Non-profit	0 (.0%)	1 (8.3)	0 (.0%)	1 (2.6)
Number of Staff	‹10	0 (.0%)	2 (16.7)	6 (50.0)	8 (20.5)
	10 - 50	3 (20.0)	7 (58.3)	5 (41.7)	15 (38.5)
	51- 100	5 (33.3)	2 (16.7)	1 (8.3)	8 (20.5)
	101 - 190	4 (26.7)	0 (.0%)	0 (.0%)	4 (10.3)
	› 191	2 (20.0)	1 (8.3)	0 (.0%)	3 (7.8)
Estimate Number of Patrons	‹ 500	0 (.0%)	3 (25.0)	4 (33.3)	7 (17.9)
	500- 1000	0 (.0%)	1 (8.3)	1 (8.3)	2 (5.1)
	1001 -5 000	3 (20.0)	2 (16.7)	4 (33.3)	9 (23.1)
	› 5 000	12 (80.0)	6 (50.0)	3 (25.0)	21 (53.8)
Availability of IS Security Staff	No	5 (33.3)	7 (58.3)	5 (41.7)	17 (43.6)
	Yes	10 (66.7)	5 (41.7)	7 (58.3)	22 (56.4)

It is apparent that academic libraries in public universities have more staff than academic libraries in university colleges. However, there was no significant difference between the type of academic libraries and the number of patrons, as many academic libraries both in public and private universities reported to have over 5,000 patrons. One factor could be due to the fact that academic libraries serve both internal as well as remote patrons, including their faculty members, staff, undergraduate students, postgraduate students, alumni, private individuals or members of other academic institutions and unaffiliated users.

More than half (56.4%) of academic libraries answered that they have dedicated staff assigned for IS security-related jobs. These findings demonstrate some positive progress and concerns regarding security of IS in these academic libraries, even though some academic libraries are still lagging in terms of assigning dedicated staff for ISec roles.

(a) The Information Technology Infrastructures in Academic Libraries

General background on IT infrastructures at Malaysian academic libraries are derived through five questions regarding the number of staff's personal computers (PCs), number of patrons' PCs, availability of wireless connection, type of operating system used and years of ICT implementation in these libraries. As can be seen from the table 4.5, a majority of academic libraries (41.0%) provide adequate PCs for their staff and the ratio is one PC for every single library staff (Table 4.5). As compared to academic libraries in university colleges, academic libraries in public universities provide more computers to their staff.

Table 4.5 shows that majority of the academic libraries (59.0%) provide less than 100 PCs for their patrons. These may be due to the fact that patrons are allowed to use their own laptops inside the library building and connect their laptops to the Internet using the free wireless connections.

Table 4.5. IT Infrastructures by Type of Academic Library.

Characteristics		Type of Academic Library			n (%)
		Public university	Private university	University college	
Number of staff's PCs	Less than 10	0 (.0%)	1 (8.3)	6 (50.0)	7 (17.9)
	Between 10 and 50	4 (26.7)	8 (66.7)	4 (33.3)	16 (41.0)
	Between 51 and 100	5 (33.3)	2 (16.7)	2 (16.7)	9 (23.1)
	Between 101 and 190	2 (13.3)	0 (.0%)	0 (.0%)	2 (5.1)
	More than 191	4 (26.7)	1(8.3)	0 (.0%)	5 (12.8)
Number of patrons' PCs	Less than 100	4(26.7)	9 (75.0)	10 (83.3)	23 (59.0)
	Between 101 and 200	2 (13.3)	1(8.3)	1(8.3)	4 (10.3)
	Between 201 and 300	8 (53.3)	2(16.7)	1(8.3)	11 (28.8)
	More than 300	1(6.7)	0(.0%)	0(.0%)	1 (2.6)
Availability of Wireless Connection	Currently piloting	1(6.7)	0(.0%)	2 (16.7)	3 (7.7)
	Yes	14 (93.3)	12 (100.0)	10 (83.3)	36 (92.3)
Operating system	Windows	8 (53.3)	8 (66.7)	8 (66.7)	24 (61.5)
	Windows and Linux	5 (33.3)	1 (8.3)	2 (16.7)	8 (20.5)
	Windows and Other	0 (.0%)	1 (8.3)	1 (8.3)	2 (5.1)
	Windows and Unix Variance	1 (6.7)	2 (16.7)	0 (.0%)	3 (7.7)
	Windows, Linux and Unix Variance	0 (.0%)	0 (.0%)	1 (8.3)	1 (2.6)
	Windows, Linux, Unix Variants and Mac OS X	1 (6.7)	0 (.0%)	0 (.0%)	1(2.6)
Years of ICT implementation	Less than 5 years	1 (6.7)	1 (8.3)	2 (16.7)	4 (10.3)
	5 years to 10 years	6 (40.0)	5 (41.7)	7 (58.3)	18 (46.2)
	10 years to 15 years	5 (33.3)	6 (50.0)	3 (25.0)	14 (35.9)
	More than 19 years	3 (20.0)	0 (.0%)	0 (.0%)	3 (7.7)

It is interesting to note that almost all academic libraries (92.3%) in this study provide wireless services to their patrons and only three (7.7%) academic libraries are currently piloting the services. This appears that academic libraries in Malaysia are taking advantage of the many benefits offered by the wireless data communication. By deploying wireless technology, college and university administrators can save on wiring

the buildings as well as for the continuous maintenance costs (Foster, 1996). It is also believed that the mobility offered by wireless networks could provide better services in fulfilling the computing needs and habits of students and faculty members than the traditional wired version (Foster, 1996).

This study revealed that Windows is the most popular operating system used in these academic libraries especially on the desktops and it is often used interchangeably with other operating systems including Linux, Unix Variance, Solaris and Max OS x.

Approximately 46% of the academic libraries surveyed have five to ten years experience in using ICT and only three (20.0%) public university libraries have implemented ICT since more than 19 years ago. These findings illustrate that academic libraries in Malaysia have sufficient years of experience in development and implementation of ICT to be relevant for this study and permit the assessment of their IS security threats and the common practices to ensure IS security in these libraries are in place.

(b) Information Security Budget in Academic Libraries

Academic libraries (36%) in this study receive between 1% to 3% budget for IS security of their overall library general budgets and only three (27.3%) public university libraries obtained higher budget allocation (i.e. more than 5%) than the other academic libraries (Table 4.6). This situation indicates that the academic libraries in this study seem to receive limited funds for IS security. It is interesting to study how these academic libraries achieve a balance between limited funds and the implementation of necessary ISec protection to best meet their security needs.

Table 4.6. Percentage of Information Systems Security Budget in Academic Libraries

Characteristics		Type of Academic Library			n (%)
		Public university	Private university	University college	
Percentage of IS Security budget of the library general budget	Less than 1%	1 (9.1)	3 (25.0)	4 (44.4)	8 (25.0)
	Between 1% to 3%	3 (27.3)	5 (41.7)	3 (33.3)	11 (34.4)
	Between 4% to 5%	4 (36.4)	3 (25.0)	2 (22.2)	9 (28.1)
	More than 5%	3 (27.3)	1 (8.3)	0 (.0%)	4 (12.5)

4.3 Perceived Information Security Threats and Source of Threats in Malaysian Academic Libraries

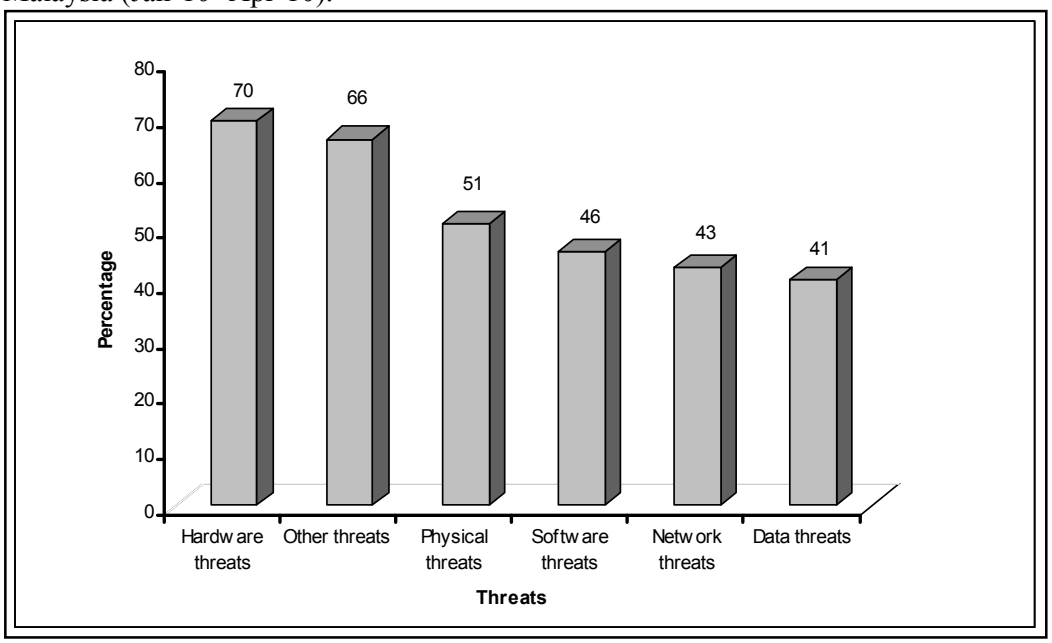
This section provides background information to the information security (ISec) of Malaysian academic libraries from the aspect of IS security threats and their origin of attacks that these libraries must cope with. The statistical findings related to the perceived security threats challenging IS in Malaysian Academic Libraries are also presented and discussed.

4.3.4 Perceived Information Security Threats in Malaysian Academic Libraries

Figure 4.3 provides information on the most common IS security threats experienced by the participating academic libraries during a period of six months. Based on the respondents' opinions, hardware security threats are indicated as the most common security threats in academic libraries (70.0%). The second highest threats in Malaysian academic libraries are from 'other threats' or 'human-related threats' components (66.0%), which include employee misconduct or human errors. Deloitte Global TMT Security Survey 2009 also reported the same results; where forty-one percent of respondents in this survey experienced at least one internal security breach in 12 months (Deloitte Touche Tohmatsu, 2009). The next most frequent threats are physical facilities and environmental threats such as fire, flood, storm, earthquakes, lightning and power supply failure. Unsurprisingly, the academic libraries in this study reported slightly

lower occurrence of software security threats, network security threats and data security threats.

Figure 4.3. Information System Security Threats Experienced by Academic Libraries in Malaysia (Jan'10- Apr'10).



(a) Hardware Security Threats

Table 4.7 illustrates the type of hardware security threats in the participating academic libraries. Hardware maintenance errors are found to be the most commonly (87.2%) reported by these academic libraries. It is noted that regular maintenance is necessary to eliminate hardware failure errors and implications of maintenance errors can cause far greater harm for the hardware. The next most threatening to hardware elements are the failure of communication equipments (79.5%), electromagnetic interference (78.9%) followed by malware and malicious code attacks including virus, worm, Trojan horse, logic bombs and trapdoor (71.8%). Additionally, these academic libraries also associated hardware security threats with theft, physical sabotage, vandalism of ICT hardware equipments (66.7%). This is parallel with a security report on the major breaches in healthcare data security in the United States, which also revealed that theft

of computers and data storage devices account for 56% of all breaches, with stolen laptops leading the pack and lost hardware accounting for another 6% (Lowes and Robert, 2010).

Table 4.7. Hardware Security Threats Experienced by Academic Libraries in Malaysia.

No.	Hardware Threats	n	%
1.	Maintenance errors	34	87.2
2.	Failure of communication equipments	31	79.5
3.	Electromagnetic interference	30	78.9
4.	Malware and malicious code (e.g. virus, worm, Trojan horse, logic/time bombs, trapdoor) e.g. making it impossible to boot the computer.	28	71.8
5.	Theft, physical sabotage, vandalism of ICT hardware equipments	26	66.7
6.	Installation/ use of unauthorised hardware	25	64.1
7.	Hardware/ equipments failure	24	61.5

(b) Software Security Threats

Table 4.8 displays information on software security threats experienced by the participating academic libraries. Software maintenance errors have been reported as the most regular threat (69.2%) followed by corruption by system, program or system errors (64.1%) and installation or use of unauthorised software (61.5%). In addition, these academic libraries also experience adware and spyware threats (51.3%), hacking or unauthorised access (51.3%), malware threats (46.2%) and abuse access control (38.5%). The least likely software threats to the libraries were software piracy (38.5%), use of library Internet for illegal activities (38.5%), weak passwords (38.5%), password attacks (35.9%), unauthorised changes to software settings (35.9%), cyber-terrorism (30.8%) and user abuses (30.8%).

Table 4.8. Software Security Threats Experienced by Academic Libraries in Malaysia.

No.	Software Threats	n	%
1.	Maintenance errors	27	69.2
2.	Corruption by system,Program/system errors or failure of system software	25	64.1
3.	Installation/ Use of unauthorised programmes or software	24	61.5
4.	Adware and Spyware	20	51.3
5.	Hacking/Intrusion/ unauthorised access to system resources	20	51.3
6.	Malware and malicious code (e.g. virus, worm, Trojan horse, logic/time bombs, trapdoor) e.g. program crashes, repeated error messages or periodically reboot your system.	18	46.2
7.	Abuse of computer access control	16	41.0
8.	Software piracy	15	38.5
9.	Use of library Internet for illegal or illicit communications or activities (e.g. surfing for pornography and e-mail harassment)	15	38.5
10.	Weak passwords	15	38.5
11.	Password attacks/sniffing/stealing	14	35.9
12.	Unauthorised changes to software settings	14	35.9
13.	Cyber-terrorism	12	30.8
14.	User abuse/fraud	12	30.8

(c) Network Security Threats

Table 4.9 highlights the type of network security threats faced by academic libraries in this study. IP address spoofing or IP spoofing, re-routing messages and use of weak passwords have been reported as the most frequent attacks in these libraries (46.2%). Many network attacks were due to weak passwords, hacking or intrusion and packing sniffs, transmission errors (41.0%), password attacks (38.5%), probes and scans (38.5%), malware and malicious code (33.3%) and session hijacking (30.8%).

Other network threats that are less frequently faced by academic libraries include website defacement (28.2%), wiretapping (25.6%), wireless network breaches (25.6%), spams (23.1%), zombie networks (23.1%) and denial of service attacks (20.5%). These findings are parallel with a report by Malaysian Cybersecurity, which indicates that incidents caused by denial of service attacks are becoming much lesser, however, system or network administrators should not take these attacks for granted (CyberSecurity Malaysia, 2010).

Table 4.9. Network Security Threats Experienced by Academic Libraries in Malaysia.

No.	Network Threats	n	%
1.	IP spoofing attacks	18	46.2
2.	Misrouting/re-routing of messages	18	46.2
3.	Weak password	18	46.2
4.	Hacking/ Intrusion/ unauthorised access	17	43.6
5.	Packing sniffs	17	43.6
6.	Transmission errors	16	41.0
7.	Password attacks/sniffing/stealing	15	38.5
8.	Probes and scans or unauthorised access to computers, data, services and applications	15	38.5
9.	Malware and malicious code (e.g. virus, worm, Trojan horse, logic/time bombs, trapdoor) e.g. losses associated with the network downtime or lowered network speed.	13	33.3
10.	Session hijacking	12	30.8
11.	Website defacement	11	28.2
12.	Eavesdropping/ wiretapping	10	25.6
13.	Wireless network breach	10	25.6
14.	E-mail attacks /spams/ fraud	9	23.1
15.	Zombie networks	9	23.1
16.	Denial of service attacks (DoS)	8	20.5

(d) Data Security Threats

Table 4.10 ranks the most common data security threats experienced by academic libraries in Malaysia. These participating academic libraries received an overwhelming numbers of threats on social engineering, loss of patron data and phishing or pharming. The next most common data incidents involved exposure of patrons sensitive data through web attacks, malware attacks (46.2% respectively), destruction due to natural disaster (43.6%), unauthorised access (43.6%) and data loss due to wrong procedures of updating or backup (41.0%). Additionally, data residing in the academic libraries' IS are also exposed to risks of delay in updating or dissemination, unauthorised transfer of data, data manipulation, password attacks, data diddling, masquerading of user identity, unauthorised data copying, unauthorised modifications of data and theft of proprietary data. These 17 types of data threats might cause disturbances to these academic libraries if they remain untreated.

Table 4.10. Data Security Threats Experienced by Academic Libraries in Malaysia.

No.	Data Threats	n	%
1.	Impersonation/ social engineering	19	48.7
2.	Loss of patron data/privacy ideas	19	48.7
3.	Phishing/ pharming	19	48.7
4.	Exposure of patrons sensitive data through web attack	18	46.2
5.	Malware and Malicious code (e.g. virus, worm, Trojan horse, logic/time bombs and trapdoor) e.g. destroy your data or wipe your hard drives clean	18	46.2
6.	Destruction due to natural disaster etc.	17	43.6
7.	Unauthorised access	17	43.6
8.	Data loss due to wrong procedures of updating/storage/backup etc.	16	41.0
9.	Delay in updating/dissemination	15	38.5
10.	Unauthorised transfer of data	15	38.5
11.	Data manipulation	14	35.9
12.	Password attacks/sniffing/stealing	14	35.9
13.	Data diddling (Changing data with malicious intent before or during input into the system)	12	30.8
14.	Masquerading of user identity	12	30.8
15.	Unauthorised data copying	12	30.8
16.	Unauthorised/accidental disclosure/modifications/alteration of data	12	30.8
17.	Theft of proprietary data	10	25.6

(e) Physical Security Threats

Table 4.11 indicates that unauthorised access into the library building, leaking and theft or vandalism is ranked as the highest occurring threats in the participating academic libraries. It seems that unauthorised access into library building may be regarded as a very serious offence as it might cause other related offences including theft, sabotage and vandalism. Among the six physical incidents listed, failure of electricity, air-conditioning or water utility are considered as the least physical threatening to these academic libraries as compared to the other common threats caused by fire, flood, storm or lightning and hazardous materials.

Table 4.11. Percentage of Physical Security Threats Experienced by Academic Libraries in Malaysia (Jan'10- Apr'10).

No.	Physical Threats	n	%
1.	Intrusion/unauthorised access into library building	17	43.6
2.	Leaking	17	43.6
3.	Theft, burglary, sabotage, vandalism or physical intrusions	14	41.0
4.	Natural calamity (e.g. fire, flood, storm, earthquakes or lightning)	15	38.5
5.	Hazardous material accident	12	30.8
6.	Power supply failure (e.g. electricity, air-conditioning, water utility)	9	23.1

(f) Human Related Threats

Human errors including data entry errors or carelessness (79.5%), employee misconducts (71.8%) and unfaithful patrons (69.2%) are regarded as the most dangerous human-related security threats to these academic libraries (Table 4.12). These findings correspond to an audit report, which indicated that the biggest data threats come from careless employees who do not properly secure the data they are responsible for (Bosworth, 2006). In addition to these, the academic libraries are also facing threats such as online extortion, social engineering and unfaithful staff. These discoveries are consistent with the Ernst and Young's 12th annual global ISec survey results, which reported that authorised users and employees pose the greatest security threat to an organisation (Ernst and Young, 2009).

Table 4.12. Human Related Threats Experienced by Academic Libraries in Malaysia.

No.	Human Related Threats	n	%
1.	Human errors (data entry errors or carelessness)	31	79.5
2.	Employee misconduct	28	71.8
3.	Unfaithful patrons	27	69.2
4.	Online extortion	24	61.5
5.	Social engineering	22	56.4
6.	Unfaithful staff	22	56.4

4.3.5 Occurrence of Information Security Threats in Malaysian Academic Libraries

This section covers the frequency of occurrence of each IS security threat based on the following choices: never, very rarely, sometimes and always.

(a) Frequencies of Hardware Security Threats

The majority of respondents believed that hardware security threats due to maintenance errors (43.6%), failure of communication equipments or services (64.1%), electromagnetic interference (63.2%), malware and malicious code (35.9%) as well as theft or vandalism of ICT hardware equipments (48.7%) very rarely occurred (Table 13). On the other hand, a majority of respondents also believed that use of unauthorised hardware and equipments failure never happened before in their libraries. The minority of respondents believed that attacks from virus or Trojan horse, maintenance errors, electromagnetic interference, use of unauthorised hardware and equipment failure always occurred in their libraries.

Table 4.13: Frequencies of Hardware Security Threats

No.	Hardware Security Threats	Frequencies of Hardware Security Threats			
		Never	Very rarely	Sometimes	Always
1.	Maintenance errors	5 (12.8%)	17 (43.6%)	16 (41.0%)	1 (2.6%)
2.	Failure of communication equipments and services	8 (20.5%)	25 (64.1%)	6 (15.4%)	0 (0.0%)
3.	Electromagnetic interference	8 (21.1%)	24 (63.2%)	5 (13.2%)	1 (2.6%)
4.	Malware and malicious code (e.g. virus, worm, Trojan horse, logic/time bombs, trapdoor) e.g. making it impossible to boot the computer.	11 (28.2%)	14 (35.9%)	8 (20.5%)	6 (15.4%)
5.	Theft, physical sabotage, vandalism of ICT hardware equipments	13 (33.3%)	19 (48.7%)	7 (17.9%)	0 (0.0%)
6.	Installation/ use of unauthorised hardware	14 (35.9%)	12 (30.8%)	12 (30.8%)	1 (2.6%)
7.	Hardware/ equipment failure	15 (38.5%)	14 (35.9%)	9 (23.1%)	1 (2.6%)

(b) Frequencies of Software Security Threats

It is observed that only a small number of respondents indicated that failure of system software (5.1%), adware and spyware (7.7%), virus attacks (7.7%), abuse of computer access control (2.6%), weak passwords (5.1%) and cyber-terrorism (7.7%) always happened in their academic libraries (Table 4.14). The majority of respondents claimed that these software security threats never happened before in their libraries. However, among various types of software security incidents, 28% of respondents reported that corruption by system, system errors or failure of system software sometimes occurred in their libraries.

Table 4.14. Frequencies of Software Security Threats

No.	Software Security Threats	Frequencies of Software Security Threats			
		Never	Very rarely	Sometimes	Always
1.	Maintenance errors	19 (48.7%)	12 (30.8%)	8 (20.5%)	0 (0.0%)
2.	Corruption by system, system errors or failure of system software	14 (35.9%)	12 (30.8%)	11 (28.2%)	2 (5.1%)
3.	Installation/Use of unauthorised programmes or software	15 (38.5%)	14 (35.9%)	10 (25.6%)	0 (0.0%)
4.	Adware and Spyware	19 (48.7%)	11 (28.2%)	6 (15.4%)	3 (7.7%)
5.	Hacking/ Intrusion/ unauthorised access to system resources	20 (51.3%)	15 (38.5%)	4 (10.3%)	0 (0.0%)
6.	Malware and malicious code (e.g. virus, worm, Trojan horse, logic/time bombs, trap door) e.g. program crashes, repeated error messages or periodically reboot your system.	21 (53.8%)	9 (23.1%)	6 (15.4%)	3 (7.7%)
7.	Abuse of computer access control	23 (59.0%)	9 (23.1%)	6 (15.4%)	1 (2.6%)
8.	Software piracy	24 (61.5%)	10 (25.6%)	5 (12.8%)	0 (0.0%)
9.	Use of library Internet for illegal or illicit communications or activities (e.g. porn surfing, e-mail harassment)	24 (61.5%)	8 (20.5%)	7 (17.9%)	0 (0.0%)
10.	Weak passwords	24 (61.5%)	7 (17.9%)	6 (15.4%)	2 (5.1%)
11.	Password attacks/sniffing/stealing	25 (64.1%)	8 (20.5%)	6 (15.4%)	0 (0.0%)
12.	Unauthorised changes to software settings	25 (64.1%)	10 (25.6%)	4 (10.3%)	0 (0.0%)
13.	Cyber-terrorism	27 (69.2%)	6 (15.4%)	3 (7.7%)	3 (7.7%)
14.	User abuse/fraud	27 (69.2%)	7 (17.9%)	5 (12.8%)	0 (0.0%)

(c) Frequencies of Network Security Threats

A minority of respondents (7.7%) expressed belief that mail attacks, spams or frauds always happened in their libraries, while 23.1% of the respondents noted that these network security threats occurred very rarely in their workplaces (Table 4.15). Some respondents in this study believed that IP spoofing attacks (25.6%) and transmission errors (25.6%) are sometimes threatening their academic libraries' IS. However, the majority of respondents firmly believed that website defacement (71.8%), eavesdropping (74.4%), wireless network breach (74.4%), zombie networks (79.6%) and denial of service attacks (DoS) (79.5%) never occurred in their libraries.

Table 4.15. Frequencies of Network Security Threats

No.	Network Security Threats	Frequencies of Network Security Threats			
		Never	Very rarely	Sometimes	Always
1.	IP spoofing attacks	18 (46.2%)	10 (25.6%)	10 (25.6%)	1 (2.6%)
2.	Misrouting/re-routing of messages	21 (53.8%)	9 (23.1%)	9 (23.1%)	0 (0.0%)
3.	Weak password	18 (46.2%)	10 (25.6%)	9 (23.1%)	2 (5.1%)
4.	Hacking/ Intrusion/ unauthorised access	22 (56.4%)	10 (25.6%)	6 (15.4%)	1 (2.6%)
5.	Packing sniffs	17 (43.6%)	13 (33.3%)	9 (23.3%)	0 (0.0%)
6.	Transmission errors	16 (41.0%)	13 (33.3%)	10 (25.6%)	0 (0.0%)
7.	Password attacks/sniffing/stealing	24 (61.5%)	9 (23.1%)	6 (15.4%)	0 (0.0%)
8.	Probes and scans or unauthorised access to computers, data, services and applications	24 (61.5%)	12 (30.8%)	3 (7.7%)	0 (0.0%)
9.	Malware and malicious code (e.g. virus, worm, Trojan horse, logic/time bombs, trapdoor) e.g. losses associated with the network downtime or lowered network speed.	15 (38.5%)	13 (33.3%)	9 (23.1%)	2 (5.1%)
10.	Session hijacking	27 (69.2%)	8 (20.5%)	4 (10.3%)	0 (0.0%)
11.	Website defacement	28 (71.8%)	8 (20.5%)	3 (7.7%)	0 (%)
12.	Eavesdropping/ wiretapping	29 (74.4%)	9 (23.1%)	1 (2.6%)	0 (0.0%)
13.	Wireless network breach	29 (74.4%)	7 (17.9%)	3 (7.7%)	0 (0.0%)
14.	E-mail attacks/spams/fraud	14 (35.9%)	13 (33.3%)	9 (23.1%)	3 (7.7%)
15.	Zombie networks	30 (79.6%)	7 (17.9%)	2 (5.1%)	0 (0.0%)
16.	Denial of service attacks (DoS)	31 (79.5%)	6 (15.4%)	2 (5.1%)	0 (0.0%)

(d) Frequencies of Data Security Threats

Table 4.16 reveals that a number of respondents expressed belief that virus attacks (17.9%), unauthorised access (20.5%), data manipulation (17.9%) and data loss due to wrong procedures of updating, storage or backup (15.4%) sometimes happened in their academic libraries. On the other hand, delay in data updating or dissemination (51.3%), impersonation or social engineering (46.2%), exposure of patrons' sensitive data through web attack (43.6%) and destruction due to natural disaster (35.9%) are considered less threatening to library IS as many respondents indicated that these incidents very rarely happened in their libraries.

Table 4.16. Frequencies of Data Security Threats

No.	Data Security Threats	Frequencies of Data Security Threats			
		Never	Very rarely	Sometimes	Always
1.	Impersonation/ social engineering	19 (48.7%)	18 (46.2%)	2 (5.1%)	0 (0.0%)
2.	Loss of patron data/privacy ideas	20 (51.3%)	14 (35.9%)	5 (12.8%)	0 (0.0%)
3.	Phishing/pharming	20 (51.3%)	13 (33.3%)	6 (15.4%)	0 (0.0%)
4.	Exposure of patrons sensitive data through web attack	18 (46.2%)	17 (43.6%)	4 (10.3%)	0 (0.0%)
5.	Malware and Malicious code (e.g. virus, worm, Trojan horse, logic/time bombs and trapdoor) e.g. destroy your data or wipe your hard drives clean)	18 (46.2%)	14 (35.9%)	7 (17.9%)	0 (0.0%)
6.	Destruction due to natural disaster etc.	22 (56.4%)	14 (35.9%)	3 (7.7%)	0 (0.0%)
7.	Unauthorised access	22 (56.4%)	9 (23.1%)	8 (20.5%)	0 (0.0%)
8.	Data loss due to wrong procedures of updating/storage/backup etc.	23 (59.0%)	10 (25.6%)	6 (15.4%)	0 (0.0%)
9.	Delay in updating/dissemination	15 (38.5%)	20 (51.3%)	4 (10.3%)	0 (0.0%)
10.	Unauthorised transfer of data	24 (61.5%)	14 (35.9%)	1 (2.6%)	0 (0.0%)
11.	Data manipulation	25 (64.1%)	7 (17.9%)	7 (17.9%)	0 (0.0%)
12.	Password attacks/sniffing/stealing	25 (64.1%)	12 (30.8%)	2 (5.1%)	0 (0.0%)
13.	Data diddling (Changing data with malicious intent before or during input into the system)	27 (69.2%)	6 (15.4%)	6 (15.4%)	0 (0.0%)
14.	Masquerading of user identity	27 (69.2%)	9 (23.1%)	3 (7.7%)	0 (0.0%)
15.	Unauthorised data copying	27 (69.2%)	10 (25.6%)	2 (5.1%)	0 (0.0%)
16.	Unauthorised/accidental disclosure/modification/alteration of data	27 (69.2%)	10 (25.6%)	2 (5.1%)	0 (0.0%)
17.	Theft of proprietary data	29 (74.4%)	5 (12.8%)	5 (12.8%)	0 (0.0%)

It is comforting to notice that a majority of respondents believed that theft of proprietary data (74.4%), data diddling (69.2%), masquerading of user identity (69.2%), unauthorised data copying (69.2%) and unauthorised disclosure or modification of data (69.2%) never occurred in their libraries. These results suggest that the low frequency of occurrence of these data security threats might due to adequacy of implemented controls in these participating academic libraries.

(e) Frequencies of Physical Security Threats

The results revealed that 20% of respondents indicated that leaks sometimes happened in their libraries (Table 4.17). Although these results indicate that this threat is not prevalent in Malaysian academic libraries, serious consideration should be given to minimise its impact. As indicated by Adekanye (2010), more than half of university libraries (53.3%) in Nigeria experienced a leaking roof, which resulted in heavy loss of their vital library resources. About 38% of respondents believed that power supply failure (including electricity, air-conditioning and water utility failure) very rarely happened. In contrast, on other 38% respondents claimed that these threats never happened in their libraries. A vast majority of respondents affirmed that threats due to intrusion into library building (56.4%), theft or vandalism (43.6%), natural calamity (including fire, flood, storm, earthquakes or lightning) (61.5%) and hazardous material accident (69.2%) never occurred in their libraries.

Table 4.17. Frequencies of Physical Security Threats

No.	Physical Security Threats	Frequencies of Physical Security Threats			
		Never	Very rarely	Sometimes	Always
1.	Intrusion/ unauthorised access into library building	22 (56.4%)	11 (28.2%)	6 (15.4%)	0 (0.0%)
2.	Leaking	17 (43.6%)	14 (35.9%)	8 (20.5%)	0 (0.0%)
3.	Theft, burglary, sabotage and vandalism	17 (43.6%)	16 (41.0%)	6 (15.4%)	0 (0.0%)
4.	Natural calamity (e.g. fire, flood, storm, earthquakes or lightning)	24 (61.5%)	8 (20.5%)	7 (17.9%)	0 (0.0%)
5.	Hazardous material accident	27 (69.2%)	10 (25.6%)	2 (5.1%)	0 (0.0%)
6.	Power supply failure (e.g. electricity, air-conditioning, water utility)	15 (38.5%)	15 (38.5%)	9 (23.1%)	0 (0.0%)

(f) Frequencies of Human Related Threats

Table 4.18 shows that only one respondent (2.6%) believed that human errors such as data entry errors or carelessness always occurred in his academic library, while 7% of respondents indicated it might happen 'sometimes' and a vast percent of other respondents (69.2%) believed that it never happened in their libraries. Twelve (30.8%) and eight respondents (20.5%), respectively indicated that 'unfaithful patrons' and 'employee misconduct' are sometimes threatening their library IS.

Quite a number of respondents expressed their opinion that incidents due to online extortion (33.3%) and social engineering (41.0%) never occurred in their academic libraries. This result indicates that circumstances where the possibility of human-related threats exist in these academic libraries regardless of their size and type.

Table 4.18. Frequencies of Human Related Threats

No.	Human Related Threats	Frequencies of Human Related Threats			
		Never	Very rarely	Sometimes	Always
1.	Human errors (data entry errors or carelessness)	27 (69.2%)	8 (20.5%)	3 (7.7%)	1 (2.6%)
2.	Employee misconduct	20 (51.3%)	11 (28.2%)	8 (20.5%)	0 (0.0%)
3.	Unfaithful patrons	14 (35.9%)	13 (33.3%)	12 (30.8%)	0 (0.0%)
4.	Online extortion	24 (61.5%)	13 (33.3%)	2 (5.1%)	0 (0.0%)
5.	Social engineering	17 (43.6%)	16 (41.0%)	6 (15.4%)	0 (0.0%)
6.	Unfaithful staff	17 (43.6%)	14 (35.9%)	8 (20.5%)	0 (0.0%)

4.3.3 Sources of Information Security Threats in Malaysian Academic Libraries

This section describes the causes of ISec incidents in Malaysian academic libraries. The respondents were asked their opinion regarding the most common source of IS security breaches in their libraries. There are many possible sources of security threats, but as illustrated in Figure 4.4, a majority of respondents (56.4%) believed that the most usual source of IS security breaches in their libraries come from hardware and software failures such as power failure, equipment failure, network failure or system malfunction.

Interestingly, the other 41% of respondents believed that their library's IS security threats usually come from people or human threats, including intentional or unintentional acts by library staff or patrons. In contrast, none of the respondents indicated that natural or environmental threats such as fire, flood or earthquake have given any negative impact on the safety of their IS. Only one respondent (2.6%) believed that the cause of IS security incidents in his library come from the unknown source. The results from this study are consistent with findings reported by Samy,

Rabiah and Zuraini (2009), which indicated that the most critical threats in healthcare IS are power failure followed by acts of human error and other technological factors.

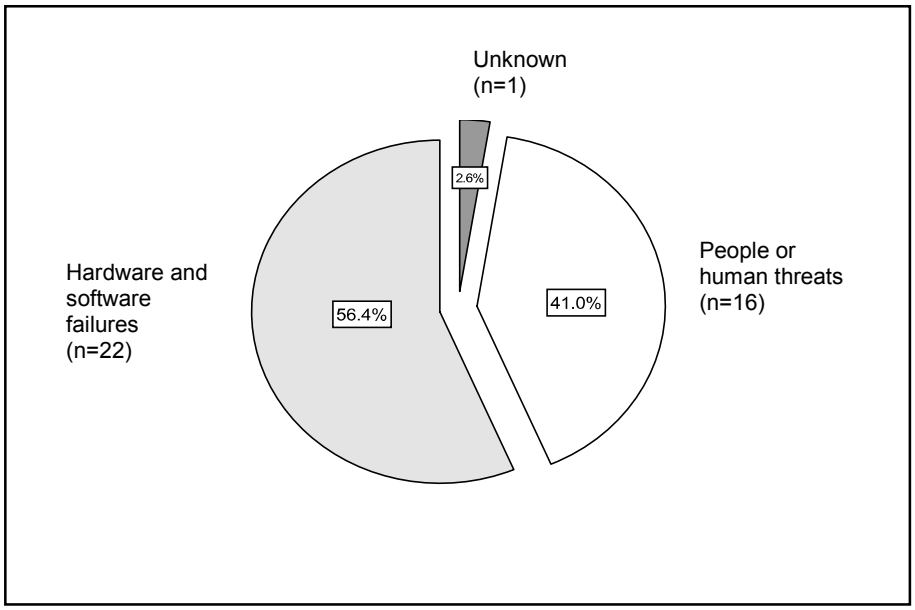


Figure 4.4. Respondents' Perception on the Most Common IS Security Threats Sources in Malaysian Academic Libraries (n=39)

4.4 Chapter Summary

The answers to research questions 1, 2, 3 and 4 are presented and discussed in this Chapter. In summary this chapter indicated the following:

(1) There is low occurrence of software security threats, network security threats and data security threats in Malaysian academic libraries.
(2) Hardware security threats (70.0%), human-related threats (66.0%) and environmental threats (51%) are revealed by respondents as the most common security threats in their academic libraries.
(3) Hardware maintenance errors are found to be the most commonly (87.2%) reported hardware security threats by these academic libraries.
(4) Software maintenance errors have been reported as the most regular (69.2%) of the software security threats in these academic libraries.

(5) IP address spoofing or IP spoofing (46.2%), re-routing messages (46.2%) and use of weak passwords have been reported as the most frequent attacks for servers in these libraries (46.2%).

(6) Social engineering, loss of patron data and phishing or pharming are found to be the most common data security threats to these academic libraries.

(7) Intrusion, leaking and theft are ranked as the highest occurring threats in the participating academic libraries.

(8) Human errors, including data entry errors or carelessness (79.5%), employee misconduct (71.8%) and unfaithful patrons (69.2%) are regarded as the most dangerous human-related security threats to these academic libraries.

(9) A majority of respondents also believed that hardware and software failures as well as intentional or unintentional acts by library staff or patrons (people or human-related threats) are the root cause of IS security incidents in their academic libraries.

Chapter Five

Level of Implementation of Information Security Measures and Differences in Applying These Measures

5.0 Introduction

The focus of this chapter is to provide a descriptive presentation of level of implementation of information security (ISec) measures in Malaysian academic libraries. It explains the level of implementation of technological and organisational measures adopted in these libraries. This chapter answers Research Questions 4, 5, 6, 7 and 8.

Firstly, section 5.1 presents findings related to the extent of technological and organisational measures deployed by Malaysian academic libraries. This would include identifying the level of implementation of hardware, software, workstation, network, server, data and physical security measures in these libraries. Section 5.2 then reveals findings related to the hypotheses testing on the differences between academic libraries in Malaysia in applying technological measures based on type of university, years in ICT implementation, yearly ISec budget, availability of information system security staff and availability of wireless connection. Section 5.3 describes findings related to the hypotheses testing on the differences between academic libraries in Malaysia in applying organisational measures based on type of university, years in ICT implementation, yearly ISec budget, availability of IS security staff and availability of wireless connection. Section 5.4 reports on overall implementation status of technological measures and organisational measures in Malaysian academic libraries based on the proposed Information Security Measures Assessment Tool for Library.

5.1 Descriptive Profiles of Level of Implementation of Information Security Measures in Malaysian Academic Libraries

Using the Organisational Information Security Staircase Model (Hagen, Albrechtsen and Hovden, 2008) as guidance, this study explores the ISec practices in Malaysian academic libraries by focusing on technological security and organisational security measures. This is because the bottom-line for effective security measures would always need a balance between technological and non-technical measures. Technological security measures describe the technical IT security measures, whereas the non-technical measures deal with personnel, security policies, security procedures, security administrative controls and security awareness initiatives. The study used five dimensions based on the 5 levels implementation score (1 = Not Implemented to 5 = Fully Implemented) adapted from the Information Security Measure Benchmark (Information-technology Promotion Agency, 2008) to assess the presence of technological security measures and organisational security measures that reflect the degree of maturity. The implementation index is used to assess which measures or steps are widely implemented and which measures or steps are least implemented in each academic library in Malaysia.

5.1.1 Level of Implementation of Technological Security Measures

Technological security measures evaluated in this study relates to the seven technical mechanism of managing IS security. At the macro level, the seven types of technological security measures are implemented in the 38 participating Malaysian academic libraries (1 academic library did not response to questions in Part C), but the implementation has not been reviewed on regular basis. Table 5.1 shows that server security measures have the highest total mean score with a statistical mean value of 3.32

and standard deviation of 0.69. This is because serves are important for the library's networks and most of the valuable databases and electronic journals provided by the libraries are placed on the web, thus they must be protected at many different levels.

Table 5.1. Total Mean Score for Implementation of Technological Measures

Technological Measures	Mean	SD
Server security measures	3.32	0.69
Workstation security measures	3.13	0.68
Network security measures	3.10	0.72
Hardware security measures	3.02	0.74
Physical and environmental security measures	2.92	0.60
Data security measures	2.89	0.67
Software security measures	2.80	0.74

At the micro level, this study used 67 items to evaluate the level of implementation of technical security countermeasures, including control mechanisms for hardware security, software security, workstation security, network security, server security, data security and physical and environmental security. The distribution of responses among is shown in the following section:

(a) Level of Implementation of Hardware Security Measures

The study used four items to evaluate the level of implementation of hardware security measures based on Yeh and Chang (2007) and INTOSAI (1995). Table 5.2 shows the highest mean with statistical mean value of 3.29 and standard deviation of 1.063 represents the use of CCTV, visual camera, magnetic detection system and electronic anti theft system at strategic places, public computer areas and server areas. Respondents also believed that their academic libraries have used emergency power sources and alternative communication lines including the use of alternative telephone lines or cables and generators (Mean=3.16, SD=0.95). It is apparent that these two hardware security practices are being implemented in these participating academic libraries in Malaysia, However, the stages have not been reviewed. Regarding the use of

locks, security cables, locked cable trays to improve the security of hardware equipments (Mean=2.87, SD=1.14) and periodical remote mirroring or file mirroring to backup disk drives (Mean=2.76, SD=1.02), respondents indicated that these security measures have been implemented but these measures have not been reviewed on regular basis in their respective academic libraries.

Table 5.2. Level of Implementation of Hardware Security Measures

Items	Not implemented	Only some part has been implemented	Implemented but has not been reviewed	Implemented and reviewed on regular basis	Fully implemented and recognised as good example for other libraries	Mean	SD
CCTV, visual camera, magnetic detection system and electronic anti theft system at strategic places, public computer areas and server areas.	0 (0.0%)	13 (34.2%)	5 (13.2%)	16 (42.1%)	4 (10.5%)	3.29	1.06
Emergency power sources and alternative communication lines. (e.g. use of alternative telephone lines or cables and generators)	1 (0.0%)	9 (23.7%)	13 (34.2%)	13 (34.2%)	2 (5.3%)	3.16	0.95
Locks, security cables, locked cable trays, metal cages or anchoring devices to improve the security of hardware equipments.	5 (13.2%)	11 (28.9%)	7 (18.4%)	14 (36.8%)	1 (2.6%)	2.87	1.14
Periodical remote mirroring or file mirroring to backup disk drives.	3 (7.9%)	15 (39.5%)	9 (23.7%)	10 (26.3%)	1 (2.6%)	2.76	1.02
Total	9 (5.9%)	48 (31.6)	34 (22.4%)	53 (34.8%)	8 (5.3%)	3.02	0.74

(b) Level of Implementation of Software Security Measures

The utilisation of several software security tools at these participating academic libraries are affirmed through the respondents' responses as listed in Table 5.3. Respondents in this survey believed that their academic libraries have used anti spyware software to detect and remove any spyware threats (Mean=3.39, SD=1.33), anti-phishing solutions to prevent phishing attacks (Mean=3.00, SD=1.25), cleanup software to erase files or settings left behind by a user (Mean=3.42, SD=1.11), automated ID management software (Mean=3.13, SD=1.28), multi-user operating systems and application software to allow concurrent access by multiple users of a computer

(Mean=3.00, SD=1.41), and web filtering software to prevent access to inappropriate materials or sites (Mean=3.03, SD=1.40). However, these software security controls have never undergone reassessment by these academic libraries.

Next, the respondents agreed that some parts of these software security safeguards were practiced in their academic but the measures have not been reviewed regularly as revealed by their responses to these following items: use of desktop security software at application level and operating level to monitor, restrict usage or disable certain features of the workstations (Mean=2.84, SD=1.20), use of distribution agents to automate the process of installing an application or updates to workstations on a network (Mean=2.84, SD=1.35), use of user entrance log to record and monitor user logs (Mean=2.89, SD=1.23) and use of systems recovery to repair the library computer systems after disaster or crash (Mean=2.74, SD=1.13).

The presence of the following software security tools at the participating academic libraries are affirmed through the respondents' responses for the use of spam filtering software to detect the unwanted spam emails (Mean=2.53, SD=1.45), use of timer software to control the amount of time a patron can use a workstation (Mean=2.50, SD=1.29), use of rollback software to keep track of any changes made to the computers (Mean=2.45, SD=1.31), use of menu replacement software to control timeouts, logging and browsing activities (Mean=2.42, SD=1.18), use of periodical automatic debugging to remove any defects on software or hardware components (Mean=2.37, SD=1.28) and use of single sign on system for user authentication to access all computers and systems (Mean=2.21, SD=1.14).

Table 5.3. Level of Implementation of Software Security Measures

Items	Not implemented	Only some part has been implemented	Implemented but has not been reviewed	Implemented and reviewed on regular basis	Fully implemented and recognised as good example for other libraries	Mean	SD
Cleanup software to erase files or settings left behind by a user.	2 (5.3%)	8 (21.1%)	4 (10.5%)	20 (52.6%)	4 (10.5%)	3.42	1.11
Anti spyware software to detect and remove any spyware threats.	6 (15.8%)	4 (10.5%)	3 (7.9%)	19 (50.0%)	6 (15.8%)	3.39	1.33
ID management software to automate administrative tasks such as resetting user passwords and enabling users to reset their own passwords.	4 (10.5%)	11 (28.9%)	4 (10.5%)	14 (36.8%)	5 (13.2%)	3.13	1.28
Web filtering software to prevent access to inappropriate materials or sites.	8 (21.1%)	8 (21.1%)	1 (2.6%)	17 (44.7%	4 (10.5%)	3.03	1.40
Anti-phishing solutions to prevent phishing attacks.	6 (16.2%)	8 (21.6%)	5 (13.5%)	16 (43.2%)	2 (5.4%)	3.00	1.25
Multi user operating systems and application software to allow concurrent access by multiple users of a computer.	8 (21.1%)	9 (23.7%)	0 (0.0%)	17 (44.7%)	4 (10.5%)	3.00	1.41
User entrance log to record and monitor user logs. These logs are regularly analysed by a library staff.	6 (15.8%)	10 (26.3%)	6 (15.8%)	14 (36.8%)	2 (5.3%)	2.89	1.23
Desktop security software at application level and operating level to monitor, restrict usage or disable certain features of the workstations.	6 (15.8%)	11 (28.9%)	5 (13.2%)	15 (39.5%)	1 (2.6%)	2.84	1.20
Distribution agents to automate the process of installing an application or updates to workstations on a network.	9 (23.7%)	8 (21.1%)	3 (7.9%)	16 (42.1%)	2 (3.3%)	2.84	1.35
Systems recovery to rebuild and repair the library computer systems after disaster or crash.	5 (13.2%)	14 (36.8%)	6 (15.8%)	12 (31.6%)	1 (2.6%)	2.74	1.13
Spam filtering software to automatically detect unwanted spam emails from getting into a user's inbox.	15 (39.5%)	3 (7.9%)	9 (23.7%	7 (18.4%)	4 (10.5%)	2.53	1.45
Timer software to control the amount of time a patron can use a workstation.	12 (31.6%)	9 (23.7%)	3 (7.9%)	14 (36.8%)	0 (0.0%)	2.50	1.29
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.	13 (34.2%)	6 (15.8%)	11 (28.9%)	5 (13.2%)	3 (7.9%)	2.45	1.31
Menu replacement software to replace the standard windows desktop interfaces and provides control on timeouts, logging and browsing activities.	9 (23.7%)	14 (36.8%)	7 (18.4%)	6 (15.8%)	2 (5.3%)	2.42	1.18
Periodical automatic debugging and tests to remove any defects from newly developed software or hardware components.	13 (34.2%)	9 (23.7%)	7 (18.4%)	7 (18.4%)	2 (5.3%)	2.37	1.28
Single sign on system for user authentication and authorisation to access all computers and systems without the need to enter multiple passwords.	12 (31.6%)	14 (36.8%)	5 (13.2%)	6 (15.8%	1 (2.6%)	2.21	1.14
Total	134 (22.1%)	146 (24.0%)	79 (13.1%)	205 (33.7%)	43 (7.1%)	2.80	0.74

(c) Level of Implementation of Workstation Security Measures

It is apparent from Table 5.4, that the use of virus protection programs, configuration settings and security software programs for web browsers and email programs carried the highest mean with a statistical mean value of 3.87 and standard deviation of 0.78. This is unsurprising as security software programs such as antivirus, anti-spyware and anti-adware software programs are widely available and commonly used nowadays for detecting and destroying malicious programs.

The respondents also believed that their academic libraries have practised the use of user identification and authentication before logging into the library's workstations, library network or campus network (Mean=3.29, SD=1.33) and they also believed that all office productivity software and browsers for the workstations and laptops are configured to receive updates in a timely manner (Mean=3.26, SD=0.89). The respondents also confirmed that some of their mobile laptops that connect to the library external local area networks (LANs) are using application firewall (Mean=2.71, SD=1.23) and some of their computer's basic input-output systems (BIOS) are secured by using passwords in order to add an extra layer of security for desktop and laptop computers (Mean=2.50, SD=1.11). However, at the time of this survey, the usage of the above workstation security tools has not been revised.

Table 5.4. Level of Implementation of Workstation Security Measures

Items	Not implemented	Only some part has been implemented	Implemented but has not been reviewed	Implemented and reviewed on regular basis	Fully implemented and recognised as good example for other libraries	Mean	SD
Virus protection programs, configuration settings and security software programs are installed for web browsers and email programs.	0 (0.0%)	3 (7.9%)	5 (13.3%)	24 (63.2%)	6 (15.8%)	3.87	0.78
User identification and authentication are required before logging into the library's workstations, laptops screensavers, library network or campus network.	5 (13.2%)	7 (18.4%)	5 (13.2%)	14 (36.8%)	7 (18.4%)	3.29	1.33
All office productivity software and browsers for the workstations/laptops are configured to receive updates in a timely manner.	1 (2.6%)	7 (18.4%)	12 (31.6%)	17 (44.7%)	1 (2.6%)	3.26	0.89
An application firewall is used for mobile laptops that connect to the library external LANs.	6 (15.8%)	14 (36.8%)	6 (15.8%)	9 (23.7%)	3 (7.9%)	2.71	1.23
The computer's BIOS are secured in order to create a secure public access computer.	8 (21.1%)	13 (34.2%)	7 (18.4%)	10 (26.3%)	0 (0.0%)	2.50	1.11
Total	20 (10.5%)	44 (23.16%)	35 (18.42%)	74 (38.95%)	17 (8.95%)	3.13	0.68

(d) Level of Implementation of Network Security Measures

In terms of network security controls (Table 5.5), the respondents revealed that their academic libraries have configured their antivirus and desktop security software to receive frequent updates (Mean=3.53, SD=0.86), used firewall (Mean=3.26, SD=1.20), used digital signatures to assure the authenticity of any electronic document sent via the library's network (Mean=3.13, SD=1.12), implemented server segregation or perimeter network (DMZ) (Mean=3.11, SD=1.25), segmented the network with a router to increase the bandwidth (Mean=3.11, SD=1.16), used a variety of wireless security products (Mean=3.11, SD=1.18) to protect the internal network from any security breaches. However, these network security controls have not been revised. The respondents also noted that their academic libraries have restricted access to the libraries high-risk applications or databases via configuration routines (Mean=2.92, SD=1.32), used separate cabling for each network to provide alternative circuit for the public and staff's local area networks (LANs) (Mean=2.92, SD=1.34) and installed

firewall with virtual private network (VPN) for remote and wireless access connections (Mean=2.82, SD=1.20). However, at the time of this survey, the usage of the above network security tools has not been revised.

Table 5.5. Level of Implementation of Network Security Measures

Items	Not implemented	Only some part has been implemented	Implemented but has not been reviewed	Implemented and reviewed on regular basis	Fully implemented and recognised as good example for other libraries	Mean	SD
Antivirus software and desktop security software to receive regular updates to protect the internal network from any security breaches.	0 (0.0%)	6 (15.8%)	9 (23.7%)	20 (52.6%)	3 (7.9%)	3.53	0.86
Firewall to protect the internal network from external threats.	4 (10.5%)	8 (21.1%)	3 (7.9%)	20 (52.6%)	3 (7.9%)	3.26	1.20
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)	3 (7.9%)	10 (26.3%)	6 (15.8%)	17 (44.7%)	2 (5.3%)	3.13	1.12
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.	6 (15.8%)	7 (18.4%)	4 (10.5%)	19 (50.0%)	2 (5.3%)	3.11	1.25
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.	3 (7.9%)	12 (31.6%)	3 (7.9%)	18 (47.4%)	2 (5.3%)	3.11	1.16
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))	4 (10.5%)	8 (21.1%)	3 (7.9%)	20 (52.6%)	3 (7.9%)	3.11	1.18
Limitation of connection time is performed via configuration routines to control and restrict access for the library's high-risk applications or databases.	9 (23.7%)	6 (15.8%)	3 (7.9%)	19 (50.0%)	1 (2.6%)	2.92	1.32
Public and staff's local area networks (LANs) are physically separated by means of separate cabling for each network to provide alternative circuit.	10 (26.3%)	3 (7.9%)	7 (18.4%)	16 (42.1%)	2 (5.3%)	2.92	1.34
Firewall with virtual private network (VPN) capabilities is installed for remote and wireless access connections.	8 (21.1%)	6 (15.8%)	10 (26.3%)	13 (34.2%)	1 (2.6%)	2.82	1.20
TOTAL	47 (13.7%)	66 (19.3%)	48 (14.0%)	162 (47.4%)	19 (5.6%)	3.10	0.72

(e) Level of Implementation of Server Security Measures

The study used ten items to evaluate the presence of server security measures in Malaysian academic libraries. Table 5.6 shows that the highest mean with a statistical mean value of 5.55 and standard deviation of 1.03 is for the use of authentication systems to prevent unauthorised access to the library's server. Respondents also believed that their academic libraries have restricted access to file system in a server by using the file or directory permissions (Mean=3.53, SD=1.06), placed server(s) in a secure location (Mean=3.53, SD=1.18), used up-to-date anti-virus software on servers (Mean=3.39, SD=1.13), used firewalls to protect the library network from unwarranted intrusion (Mean=3.34, SD=1.21) and reviewed the server logs periodically using a log file monitor utility (Mean=3.34, SD=1.05). Next, the respondents also agreed that their academic libraries have performed regular backups for vital data and documents related to the server and stored them at an offsite location (Mean=3.32, SD=1.02), the library servers' operating systems (OS) and applications are hardened to protect from any vulnerabilities (Mean=3.32, SD=1.04), implemented fault tolerance to assure there is a backup system if one system fails (Mean=3.16, SD=1.05) and used intrusion detection software and host auditing software to monitor for signs of intrusion (Mean=2.76, SD=1.22). It is apparent that academic libraries in Malaysia have implemented some kind of security measures to secure their servers. However, there is a worry that those security measures have not been reviewed regularly. The practice of regularly reviewing any security measure is vital to allow an academic library to implement the best possible security solutions.

Table 5.6 Level of Implementation of Server Security Measures

Items	Not implemented	Only some part has been implemented	Implemented but has not been reviewed	Implemented and reviewed on regular basis	Fully implemented and recognised as good example for other libraries	Mean	SD
Authentication systems to prevent unauthorised access to the library's server.	1 (2.6%)	7 (18.4%)	5 (13.2%)	20 (52.6%)	5 (13.2%)	3.55	1.03
The server is placed in a secure location, such as in a lockable cage, a locked room and place it with environmental controls.	4 (10.5%)	4 (10.5%)	3 (7.9%)	22 (57.9%)	5 (13.2%)	3.53	1.18
The file system in a server is restricted access to the directory structure using file or directory permissions.	2 (5.3%)	6 (15.8%)	4 (10.5%)	22 (57.9%)	4 (10.5%)	3.53	1.06
Anti-virus software on servers and anti-virus virus definition files are kept up-to-date.	2 (53.4%)	7 (18.4%)	9 (23.7%)	14 (36.8%)	6 (15.8%)	3.39	1.13
Firewalls to protect the library network from unwarranted intrusion.	4 (10.3%)	6 (15.4%)	6 (15.4%)	17 (43.6%)	5 (12.8%)	3.34	1.21
Server logs are reviewed periodically by using a log file monitor utility to monitor any signs of intrusion or security violations.	2 (5.3%)	8 (21.1%)	5 (13.2%)	21 (55.3%)	2 (5.3%)	3.34	1.05
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.	3 (7.9%)	4 (10.5%)	11 (28.9%)	18 (47.4%)	2 (5.3%)	3.32	1.02
The library servers' operating systems (OS) and applications are hardened to protect from any vulnerabilities.	2 (5.3%)	9 (23.7%)	3 (7.9%)	23 (60.5%)	1 (2.6%)	3.32	1.04
Fault tolerance is implemented to make sure if one system fails, then there is a backup system that immediately takes over.	1 (2.6%)	13 (34.2%)	5 (13.2%)	17 (44.7%)	2 (5.3%)	3.16	1.05
Intrusion detection software and host auditing software are installed to monitor the servers or computers for signs of intrusion.	6 (15.8%)	14 (36.8%)	2 (5.3%)	15 (39.5%)	1 (2.6%)	2.76	1.22
TOTAL	27 (7.1%)	78 (20.5%)	53 (14.0%)	189 (49.7%)	33 (8.7%)	3.32	0.69

(f) Level of Implementation of Data Security Measures

The changing shifts of library users' needs from physical to online resources require a change in the paradigm by which a library provides access and protect information. The study used fifteen items to evaluate the presence of data security measures in Malaysian academic libraries. Respondents in this survey believed that their academic libraries

have regularly backed up the library's vital business information or records (Mean=3.55, SD=0.95), properly recorded the attributes for each removable media application and kept the media from any unauthorised devices (Mean=3.32, SD=1.12), used combination of authentication systems to restrict access of library data and resources based on a variety of access rights (Mean=3.21, SD=1.07) and used log management software to ensure the library computer security records are stored in sufficient detail for an appropriate period of time (Mean=3.16, SD=1.17). Unfortunately, according to the respondents these kinds of security measures have not been reviewed regularly at their libraries (Table 5.7).

The presence of the other elements of the server security tools at the participating academic libraries are affirmed through the respondents' responses on the proper management of disposable of unused media and sensitive media in order to maintain an audit trail (Mean=2.95, SD=1.09), use of various security tools to ensure the safety of online transactions such as use of password protection, firewalls, and Internet Protocol Virtual Private Networks (Mean=2.95, SD=1.16), use of web access management systems to manage and validate user access to devices, applications and library systems (Mean=2.89 SD=1.16), use of web content filtering or monitoring systems at the proxy server or Internet server (Mean=2.89 SD=1.39), use of enforced path between a user terminal and other library services to reduce risks of unauthorised access (Mean=2.79 SD=1.26), the library network and IS security services are properly managed in-house or outsourced to a service provider (Mean=2.79 SD=1.49) and use of RFID tags to manage and secure the library collection and access into the library building (Mean=2.71 SD=1.31). However, at the time of this survey, the usage of the above data security measures has not been revised.

The respondents also confirmed that their academic libraries have adopted some elements of these data security controls including some systematic approaches conducted in-house or outsourced to a service provider to address the library vulnerabilities (Mean=2.59 SD=1.24), use of some cryptography techniques, hardware tokens, software tokens and single sign on systems to control data access (Mean=2.47 SD=1.16), use of public key infrastructure (PKI) to secure the exchange of personal data via the library network and Internet (Mean=2.47 SD=1.27) and use of address verification system (AVS), multiple login monitoring, password verification on transactions or data access controls to control fraudulent activity and disclosure of information (Mean=2.45 SD=1.37). However, the usage of the above data security tools has not been assessed.

Table 5.7. Presence of Data Security Measures in Malaysian Academic Libraries

Items	Not implemented	Only some part has been implemented	Implemented but has not been reviewed	Implemented and reviewed on regular basis	Fully implemented and recognised as good example for other libraries	Mean	SD
Library's vital 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 (2.6%)	5 (13.2%)	8 (21.1%)	20 (52.6%)	4 (10.5%)	3.55	0.95
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, tape	3 (7.9%)	8 (21.1%)	3 (7.9%)	22 (57.9%)	2 (5.3%)	3.32	1.12
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)	2 (5.3%)	10 (26.3%)	6 (15.8%)	18 (47.4%)	2 (5.30%)	3.21	1.07
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).	3 (7.9%)	12 (31.6%)	1 (2.6%)	20 (52.6%)	2 (5.3%)	3.16	1.17
Disposable of unused media and sensitive media are properly managed to maintain an audit trail.	4 (10.5%)	10 (26.3%)	9 (23.7%)	14 (36.8%)	1 (2.6%)	2.95	1.09

Table 5.7. Continued.

Items	Not implemented	Only some part has been implemented	Implemented but has not been reviewed	Implemented and reviewed on regular basis	Fully implemented and recognised as good example for other libraries	Mean	SD
Use of password protection of user accounts, antivirus 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.	6 (15.8%)	6 (15.8%)	12 (31.6%)	12 (31.6%)	2 (5.3%)	2.95	1.16
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).	3 (7.9%)	16 (42.1%)	3 (7.9%)	14 (36.8%)	2 (5.3%)	2.89	1.16
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).	8 (21.1%)	10 (26.3%)	2 (5.3%)	14 (36.8%)	4 (10.5%)	2.89	1.39
Your library network and IS 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).	11 (28.9%)	8 (21.1%)	2 (5.3%)	12 (31.6%)	5 (13.2%)	2.79	1.49
Enforced path is created between a user terminal and other library services that the user is authorised to reduce the risk of unauthorised access.	7 (18.4%)	12 (31.6%)	2 (5.3%)	16 (42.1%)	1 (2.6%)	2.79	1.26
RFID tags to manage and secure the library collection as well as to track attendance and prevent unauthorised access into the library building.	9 (23.7%)	9 (23.7%)	7 (18.4%)	10 (26.3%)	3 (7.9%)	2.71	1.31
Systematic approaches conducted in house or outsourced to a service provider to address the library vulnerabilities (e.g. managing on vulnerability discovery, prioritization, remediation, dynamic protection, verification and customizable reporting).	8 (21.6%)	12 (32.4%)	6 (16.2%)	9 (24.3%)	2 (5.4%)	2.59	1.24
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).	12 (31.6%)	9 (23.7%)	4 (10.5%)	13 (34.2%)	0 (0.0%)	2.47	1.27
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.	9 (23.7%)	12 (31.6%)	8 (21.1%)	8 (21.1%)	1 (2.6%)	2.47	1.16

Table 5.7. Continued.

Items	Not implemented	Only some part has been implemented	Implemented but has not been reviewed	Implemented and reviewed on regular basis	Fully implemented and recognised as good example for other libraries	Mean	SD
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).	13 (34.2%)	9 (23.7%)	5 (13.2%)	8 (21.1%)	3 (7.9%)	2.45	1.37
TOTAL	99 (17.4%)	148 (26.0%)	78 (13.7%)	210 (36.9%)	34 (6.0%)	2.89	0.67

(g) Level of Implementation of Physical and Environmental Security Measures

Physical and environmental safeguards play important roles to ensure that academic libraries appropriately protect their IS equipments from physical and environmental threats. Areas within the library building, especially the computer rooms, should be well-ventilated and air-conditioned in order to solve overheating problems that can cause serious damage to the equipments. Thus, it is understandable why the use of air conditioning has the highest mean with statistical value of 3.92 and standard deviation of 0.97 (Table 5.8). Next, the use of automatic sprinkler systems, smoke detectors, fire extinguishers and fireproof installations in the library buildings to detect and prevent fires, toxic chemical spills and explosions has the second highest mean with statistical value of 3.61 and standard deviation equal of 0.86. The provisions of these environmental security protectors in any library are necessary, as indicated by Matthews and Feather (2003), that smoke detection may provide an opportunity as the 'first aid' action with portable extinguishers before the fire grows to a large size and will activate the sprinkler heads.

Respondents in this survey believed that their academic libraries have used lightning and surge protectors to protect any valuable equipment from lighting strikes, voltage spikes and surges (Mean=3.42 SD=0.95), have security guards to monitor people entering and leaving the library buildings and sites (Mean=3.18 SD=1.27), used magnetic stripe swipe cards, bar code cards or biometrics to control access to restricted library areas (Mean=3.13 SD=1.32) as well as used warning signs, fencing, vehicle height-restrictors, site lightings and trenches around the library areas to provide initial layer of security for a library building (Mean=3.11 SD=1.25). Sadly, the respondents revealed that the status of these security measures have not been reviewed regularly at their libraries.

Furthermore, these physical and environmental safeguards such as the wireless gates, biometrics or other user identifications and authentication forms are implemented at the library main entrances, exits and public access areas to control access into the library building (Mean=2.74 SD=1.27). However, at the time of this survey, the usage of the above physical and environmental security tools has not been revised. It is quite surprising to find that the use of flood detector to sense the presence of water as an early warning of developing floods in a library (Mean=1.63 SD=1.05) and the use of earthquake early warning system as an emergency warning prior to damaging ground movement (Mean=1.25 SD=1.06) have slightly lower mean values. This result may be due to the common perception that Malaysia is an earthquake-free country, thus many would assume that this country is unlikely to suffer from any earthquake threats. Another reason preventing most of the buildings from installing sufficient number of earthquake early warning systems may be due to the high purchase and installation prices.

Table 5.8. Level of Implementation of Physical and Environmental Security Measures Security

Items	Not implemented	Only some part has been implemented	Implemented but has not been reviewed	Implemented and reviewed on regular basis	Fully implemented and recognised as good example for other libraries	Mean	SD
Air conditionings to stabilise the air temperature and humidity within the library building.	0 (0.0%)	4 (10.5%)	7 (18.4%)	15 (39.5%)	12 (31.6%)	3.92	0.97
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.	0 (0.0%)	3 (7.9%)	15 (39.5%)	14 (36.8%)	6 (15.8%)	3.61	0.86
Lightning protectors and surge protectors to protect any valuable machines or equipments from lighting strikes, voltage spikes and surges.	0 (0.0%)	9 (23.7%)	7 (18.4%)	19 (50.0%)	3 (7.9%)	3.42	0.95
Security guards to monitor people entering and leaving the library buildings and sites.	5 (13.2%)	8 (21.1%)	4 (10.5%)	17 (44.7%)	4 (10.5%)	3.18	1.27
Use of magnetic stripe swipe cards, electronic lock, proximity cards, bar code card or biometrics to secure and control access to restricted library areas.	7 (18.4%)	5 (13.2%)	6 (15.8%)	16 (42.1%)	4 (10.5%)	3.13	1.32
Warning signs, fencing, vehicle height-restrictors, site lightings and trenches around the library areas to provide initial layer of security for a library building.	7 (18.4%)	5 (13.2%)	4 (10.5%)	21 (55.3%)	1 (2.6%)	3.11	1.25
Flood detector to sense the presence of water to provide an early warning of developing floods in a library.	24 (63.2%)	9 (23.7%)	1 (2.6%)	3 (7.9%)	1 (2.6%)	1.63	1.05
Earthquake early warning system to provide an emergency warning to the library staff and patrons prior to damaging ground shaking.	27 (71.1%)	5 (13.2%)	1 (2.6%)	5 (13.2%)	0 (0.0%)	1.58	1.06
TOTAL	77 (22.5%)	61 (17.8%)	48 (14.0%)	123 (36.1%)	33 (9.6%)	2.92	0.60

5.1.2 Level of Implementation of Organisational Security Measures

Organisational security measures should be integrated together with technological security measures to form sound ISec controls. It is recognised that significant security can often be achieved through or supported by administrative measures such as organisational, personnel, physical and procedural controls (Common Criteria for IT Security Evaluation, 2006). Thus, an assessment of the academic libraries' security measures in a particular case should also consider management and organisational security measures. At the macro level, the three types of organisational measures

including ISec policies, ISec procedures and security awareness creation are implemented in the 38 participating Malaysian academic libraries (1 academic library did not response to questions in Part C), but the implementation has not been reviewed on a regular basis. However, Table 5.9 shows that administrative tools and methods has the lowest total mean score with a statistical value of 2.52 and standard deviation of 1.11. This might be because administrative tools and methods are not seen as important elements in a library's ISec programmes.

Table 5.9. Total Mean Score for Implementation of Organisational Measures

Organisational Measures	Mean	SD
Information Security Policies	3.13	0.68
Information Security Procedures and Controls	2.85	0.97
Information Security Awareness Creation Activities	2.73	0.91
Information Security Administrative Tools and Methods	2.52	1.11

The following sections present a micro view of the level of implementation of ISec policies; ISec procedures and controls; ISec administrative tools and methods; and ISec awareness creation in Malaysian academic libraries.

(a) Implementation of Information Security Policies

The presence of ISec policies in Malaysian academic libraries is assessed based on the twelve items as shown in Table 5.10. It can be seen that policies on acceptable use of wireless devices such as laptops and hand phones has the highest mean with a statistical value of 3.50 and standard deviation of 1.01. This result agrees with the findings of this research where 92.3% of participating academic libraries in this study have wireless Internet connection. Policies on acceptable use of workstations, e-mails, databases, intranet and Internet (Mean=3.24, SD=1.15) have the second highest mean value of 3.24 and standard deviation of 1.15. This is true as the use of workstations, e-mails,

databases, intranet and Internet are the most common services at modern academic libraries.

Respondents in this survey believed that their academic libraries have implemented several types of ISec policies including those on reporting, notification and response of IS security events to affected parties (Mean=3.21 SD=1.17), even though these policies have not been revised regularly. These types of policies imply that all members of academic libraries should be responsible for reporting any known or suspected IT security incidents to affected parties. Affected parties would include the legitimate owners, operators and users of the relevant computing facilities (Brownlee and Guttman, 1998).

Respondents also reported availability of policies on identity management for the library IS user registration and password management (Mean=3.18, SD=0.87), policies on sharing, storing and transmitting of library data via ISPs, external networks or contractors' systems (Mean=3.18, SD=1.06), policies on access control, authentication and authorisation practices for using the library IS (Mean=3.16, SD=0.92), policies on protection of library IS assets to protect the library's hardware, software, data and people (Mean=3.16, SD=1.05), job responsibility policy related to the library IS security practices (Mean=3.05, SD=1.11), policies on managing privacy and confidentiality issues, including breaches of personal information (Mean=3.05, SD=1.14) and secure disposal policies of library data, media or materials that contain sensitive information (Mean=3.00, SD=0.99). However, at time of this study, these policies have never been revised in the participating academic libraries.

When assessed on the presence of policies on backups and off-site storage (Mean=2.92, SD=1.05) and policies on data classification, retention and destruction for library data or materials that contain sensitive information (Mean=2.87, SD=1.23), respondents revealed that these policies have been implemented but the policies never been assessed in their libraries. This is somehow contradictory with the general assumption that academic libraries are expected to have regular data backed up and the backup media should be sent to an off-site storage location to provide a copy of the data in case of unforeseen disasters.

Table 5.10. Implementation Level of Information Security Policies

Items	Not implemented	Only some part has been implemented	Implemented but has not been reviewed	Implemented and reviewed on regular basis	Fully implemented and recognised as good example for other libraries	Mean	SD
Policies on acceptable use of wireless devices in your library such as laptops and hand phones.	2 (5.3%)	5 (13.2%)	6 (15.8%)	22 (57.9%)	3 (7.9%)	3.50	1.01
Policies on acceptable use of workstations, e-mails, databases, intranet and Internet in your library.	3 (7.9%)	9 (23.7%)	5 (13.2%)	18 (47.4%)	3 (7.9%)	3.24	1.15
Polices on reporting, notification and response of IS security events to affected parties such as individuals, law enforcement and campus or parent organisations.	4 (10.5%)	8 (21.1%)	4 (10.5%)	20 (52.6%)	2 (5.3%)	3.21	1.17
Identity management policies for library IS user registration and password management.	1 (2.6%)	8 (21.1%)	12 (31.6%)	17 (44.7%)	0 (0.0%)	3.18	0.87
Policies on sharing, storing and transmitting of library data via ISPs, external networks or contractors' systems.	2 (5.3%)	9 (23.7%)	10 (26.3%)	14 (36.8%)	3 (7.9%)	3.18	1.06
Policies on access control, authentication and authorisation practices for using the library IS.	1 (2.6%)	10 (26.3%)	9 (23.7%)	18 (47.4%)	0 (0.0%)	3.16	0.92
Policies on protection of library IS assets to protect your library's hardware, software, data and people.	3 (7.9%)	9 (23.7%)	5 (13.2%)	21 (55.3%)	0 (0.0%)	3.16	1.05
Policies on managing privacy and confidentiality issues, including breaches of personal information.	2 (5.3%)	14 (36.8%)	5 (13.2%)	14 (36.8%)	3 (7.9%)	3.05	1.14
Job responsibility policy for individual employee responsibilities related to the library IS security practices.	4 (10.5%)	10 (26.3%)	4 (10.5%)	20 (52.6%)	0 (0.0%)	3.05	1.11

Table 5.10. Continued.

Items	Not implemented	Only some part has been implemented	Implemented but has not been reviewed	Implemented and reviewed on regular basis	Fully implemented and recognised as good example for other libraries	Mean	SD
Secure disposal policies to dispose library data, media or materials that contain sensitive information.	2 (5.3%)	12 (31.6%)	8 (21.1%)	16 (42.1%)	0 (0.0%)	3.00	0.99
Backups and off-site storage policies for your library data, media or materials that contain sensitive information.	3 (7.9%)	12 (31.6%)	9 (23.7%)	13 (34.2%)	1 (2.6%)	2.92	1.05
Data classification, retention and destruction policies for your library data, media or materials that contain sensitive information.	9 (23.7%)	4 (10.5%)	8 (21.1%)	17 (0.0%)	0 (0.0%)	2.87	1.23
TOTAL	36 (7.9%)	110 (24.1%)	85 (18.6%)	210 (46.1%)	15 (3.3%)	3.13	0.68

(b) Implementation Level of Information Security Procedures and Controls

In terms of the presence of information security (ISec) procedures and controls, the respondents revealed (Table 5.11) that their academic libraries have implemented but never reviewed the controls and disciplinary procedures such as verbal warning, written warning, suspension and dismissal in case a library staff or patron breaches the IS security policies or rules (Mean=3.16, SD=1.03). ISACA (2009) suggests that organisations should establish and apply a consistent formal disciplinary process in dealing with those who commit security breaches such as employees and third parties. The same goes with the procedures on intellectual property rights and copyrights as means in controlling and protecting any digital work or resources that are stored, transmitted, accessed, copied or downloaded via the library IS (Mean=3.08, SD=1.10).

Respondents in this survey also affirmed that their academic libraries have implemented procedures for updating and reviewing existing ISec policies (Mean=2.82, SD=1.14), procedures for non-disclose agreement or confidentiality

agreement (Mean=2.71, SD=1.23), procedures on requirements to outsource any library IS service or activity (Mean=2.66, SD=1.17) and procedures for handling sensitive library data and personal data of library patrons (Mean=2.68, SD=1.23). However, these procedures have never been revised in the participating academic libraries.

The purpose of handling sensitive library data procedures is to provide detailed guidance on how to handle sensitive library data, including physical security of information as well as the distribution of classified information both internally and externally. For instance, sensitive library data stored in databases and spreadsheets are more vulnerable to exposure; therefore they require strong passwords for better protection.

Table 5.11. Implementation Level of Information Security Procedures

Items	Not implemented	Only some part has been implemented	Implemented but has not been reviewed	Implemented and reviewed on regular basis	Fully implemented and recognised as good example for other libraries	Mean	SD
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).	1 (2.6%)	11 (28.9%)	10 (26.3%)	13 (34.2%)	3 (7.9%)	3.16	1.03
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 (7.9%)	11 (28.9%)	5 (13.2%)	18 (47.4%)	1 (2.6%)	3.08	1.10
Procedures for update and review existing information security policies.	5 (13.2%)	12 (31.6%)	7 (18.4%)	13 (34.2%)	1 (2.6%)	2.82	1.14
Procedures for handling library sensitive data and personal data of library patrons to prevent errors, unauthorised disclosure or misuse by those who handle it.	8 (21.1%)	10 (26.3%)	8 (21.1%)	10 (26.3%)	2 (5.3%)	2.68	1.23
Procedures that list all requirements with regard to outsourcing any library IS service or activities.	6 (15.8%)	15 (39.5%)	4 (10.5%)	12 (31.6%)	1 (2.6%)	2.66	1.17

Table 5.11. Continued.

Items	Not implemented	Only some part has been implemented	Implemented but has not been reviewed	Implemented and reviewed on regular basis	Fully implemented and recognised as good example for other libraries	Mean	SD
Procedures for non-disclose agreement or confidentiality agreement to all library staff and patrons to protect any type of confidential and proprietary information.	7 (18.4%)	12 (31.6%)	6 (15.8%)	11 (28.9%)	2 (5.3%)	2.71	1.23
TOTAL	30 (13.2%)	71 (31.1%)	40 (17.5%)	77 (33.8%)	10 (4.4%)	2.85	0.97

(c) Implementation Level of Information Security Administrative Tools and Methods

Information security (ISec) administrative tools and methods should also be viewed as part of any library's ISec programmes. As can be seen in Table 5.12, procedures on handling, reporting, notification and response of IS security events to affected parties are considered an important part of security monitoring even though respondents in this study revealed that only some parts of these procedures are implemented in their academic libraries (Mean=2.92, SD=1.32). As highlighted by Scarfone, Grance and Masone (2008) establishing clear procedures for assessing current and potential business impact of incidents as well as building relationships and establishing suitable means of communication with other internal groups (e.g., human resources, legal) and with external groups (e.g. other incident response teams, law enforcement) are vital in any organisation.

Additionally, risk analysis process is also required to be performed in any security programme. As indicated by Wold and Shriver (1997), security programme helps to identify the most probable and related threats to an organisation and provide the foundation for the entire recovery planning effort. In this study, respondents noted that

there are procedures for the development and implementation of risk analysis to protect their academic libraries from all types of threats (Mean=2.50, SD=1.29). But the procedures have never been assessed periodically in the participating academic libraries.

Other types of administrative tools and methods implemented in Malaysian academic libraries include procedures for owner accountability to that ensure appropriate protection is maintained for each library IS asset (Mean=2.42, SD=1.31), procedures on asset classification in order to organise it according to its importance and sensitivity to loss (Mean=2.39 SD=1.37) and regular internal and external audits programmes appropriate for the library IS (Mean=2.34 SD=1.28).

Table 5.12. Implementation Level of Administrative Tools

Items	Not implemented	Only some part has been implemented	Implemented but has not been reviewed	Implemented and reviewed on regular basis	Fully implemented and recognised as good example for other libraries	Mean	SD
Procedures on handling, reporting, notification and response of IS security events to affected parties such as individuals, law enforcement, campus or parent organisation.	8 (21.1%)	7 (18.4%)	6 (15.8%)	14 (36.8%)	3 (7.9%)	2.92	1.32
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 measure)	10 (26.3%)	12 (31.6%)	6 (15.8%)	7 (18.4%)	3 (7.9%)	2.50	1.29
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).	12 (31.6%)	11 (28.9%)	4 (10.5%)	9 (23.7%)	2 (5.3%)	2.42	1.31
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)	13 (34.2%)	11 (28.9%)	3 (7.9%)	8 (21.1%)	3 (7.9%)	2.39	1.37

Table 5.12. Continued.

Items	Not implemented	Only some part has been implemented	Implemented but has not been reviewed	Implemented and reviewed on regular basis	Fully implemented and recognised as good example for other libraries	Mean	SD
Regular internal and external audits programs appropriate for your library's IS size, complexity of activities, scope of operations, risk profile and compliance with the relevant standards.	12 (31.6%)	12 (31.6%)	6 (15.8%)	5 (13.2%)	3 (7.9%)	2.34	1.28
TOTAL	55 (28.9%)	53 (27.9%)	25 (13.2%)	43 (22.6%)	14 (7.4%)	2.52	1.11

(e) Implementation Level of Information Security Awareness Creation Activities

Awareness creation is an essential element in any security control management and it requires close attention by all levels of management and in all types of organisations including libraries. Table 5.13 indicates types of information security (ISec) awareness initiative in academic libraries. Respondents indicated that their academic libraries have regularly identified and updated any threat that could harm and adversely affect critical operations of the library IS' security, but this stage have never been reviewed (Mean=3.05 SD=1.11). It is necessary that each staff and patron is made aware security threats. This is because today's computer threats are more invisible, numerous, escalating rapidly, complex and increasingly dangerous like parasites (Trend Micro White Paper, 2009).

Respondents in this study also revealed that staff and patrons are made aware of their responsibilities with regard to protecting the library's IS' security and trained to report any security breach incidences (Mean=2.87 SD=1.17). The same goes for ISec awareness trainings, which are only compulsory to staff and patrons in their libraries

(Mean=2.82 SD=1.20). NIST Special Publication Recommended Security Controls for Federal IS, suggests "An effective ISec program should include...security awareness training to inform personnel (including contractors and other users of IS that support the operations and assets of the organisation) of the ISec risks associated with their activities and their responsibilities in complying with organisational policies and procedures designed to reduce these risks." (Ross, et al., 2007).

Respondents also noted that there are some positive support and commitment from the top management to coordinate the implementation of IS' security controls in academic libraries, in terms of allocation of budget, strong interest and active involvement (Mean=2.79 SD=1.09). They also indicated that there are identified and regular updating of the library IS vulnerabilities and their related processes (Mean=2.76 SD=1.36), staff and patrons at various levels received regular updates on the library IS' policies and procedures (Mean=2.71 SD=1.27) and there exists risk assessment approach that follows a defined documented process (Mean=2.63 SD=1.13). Unfortunately, at the time of this study these awareness activities have never been revised in the participating academic libraries.

However, some other awareness creations activities have the lowest mean values that indicate those initiatives have been implemented in Malaysian academic libraries but the awareness activities have never been revised. These security awareness initiatives include all staff and patrons received appropriate ISec trainings and education (Mean=2.58 SD=1.20), used of balanced set of key performance indicators (KPIs) and metrics to assess the effectiveness of security awareness programmes (Mean=2.58 SD=1.06) and staff and patrons are trained to handle the library's IS on their own (Mean=2.55 SD=1.01).

Table 5.13. Level of Implementation of Information Security Awareness Creation Activities

Items	Not implemented	Only some part has been implemented	Implemented but has not been reviewed	Implemented and reviewed on regular basis	Fully implemented and recognised as good example for other libraries	Mean	SD
Threats that could harm and adversely affect critical operations of your library IS' security are identified and up dated regularly.	2 (5.3%)	12 (31.6%)	10 (26.3%)	10 (26.3%)	4 (10.5%)	3.05	1.11
All staff and patrons at various levels are made aware of their responsibilities with regard to protecting the library's IS' security and trained to report any security breach incidences.	5 (13.2%)	11 (28.9%)	8 (21.1%)	12 (31.6%)	2 (5.3%)	2.87	1.17
ISec awareness trainings have become mandatory to all staff and patrons at various levels.	7 (18.4%)	9 (23.7%)	7 (18.4%)	14 (36.8%)	1 (2.6%)	2.82	1.20
There are positive supports and commitments from the top management to coordinate the implementation of IS' security controls in your library. (e.g. via allocation of budget, strong interest and active involvements).	2 (5.3%)	18 (47.4%)	7 (18.4%)	8 (21.1%)	3 (7.9%)	2.79	1.09
Vulnerabilities in your library IS and related processes are identified and up dated regularly.	8 (21.1%)	12 (31.6%)	3 (7.9%)	11 (28.9%)	4 (10.5%)	2.76	1.36
All staff and patrons at various levels receive regular updates on your library IS' policies and procedures.	7 (18.4%)	13 (18.4%)	5 (13.2%)	10 (26.3%)	3 (7.9%)	2.71	1.27
Risk assessment approach exists and follows a defined process that is documented.	7 (18.4%)	12 (31.6%)	7 (18.4%)	12 (31.6%)	0 (0.0%)	2.63	1.13
All staff and patrons at various levels receive appropriate ISec trainings and education.	8 (21.1%)	13 (34.2%)	5 (13.2%)	11 (28.9%)	1 (2.6%)	2.58	1.20
There are balanced set of key performance indicators (KPIs) and metrics used to provide the real insight into the effectiveness of security awareness programs.	4 (10.5%)	18 (47.4%)	8 (21.1%)	6 (15.8%)	2 (5.3%)	2.58	1.06
Staff and patrons at various levels are trained to monitor and handle the library's IS on their own.	4 (10.5%)	19 (50.0%)	5 (13.2%)	10 (26.3%)	0 (0.0%)	2.55	1.01
TOTAL	54 (14.2%)	137 (36.0%)	65 (17.1%)	104 (27.4%)	20 (5.3%)	2.73	0.91

5.2 Differences in Applying the Technological Measures due to Selected Demographic Variables

This section presents result of hypotheses testing on the differences among academic libraries in Malaysia in applying technological measures due to the type of university, number of staff, years in ICT implementation, yearly information system security budget, availability of information system (IS) security staff and availability of wireless connection.

5.2.1 Hypothesis 1

There is no significant different between academic libraries in Malaysia in applying the technical measures by type of university, number of staff, years in ICT implementation, yearly ISec budget, availability of information system (IS) security staff and availability of wireless connection.

To test this hypothesis, the researcher uses Kruskal-Wallis test and Mann-Whitney U Test for testing the differences between Malaysian academic libraries in applying technical measures. The hypothesis is separated into six sub-hypotheses and every sub-hypothesis is tested separately.

Testing hypothesis 1.1

There is no significant difference between academic libraries in Malaysia in applying technological measure due to type of university.

The statistical result from the Kruskal-Wallis test shows no significant differences between Malaysian academic libraries in applying technological measures due to type of university ($H(2)=4.898$, $p \rangle 0.05$) (Table 5.14). Therefore, the sub-hypothesis 1.1 can

be accepted and it was concluded that there is no difference in applying technical measures among the three types of the academic libraries, at public and private universities as well as college universities.

Table 5.14. Kruskal-Wallis Test for Testing the Differences between Academic Libraries in Applying Technological Measure due to Type of Universities.

No	Variable	Chi-Square	df	p	Finding
1.	Technological measures	4.898	2	0.086	Not Significant

Testing Hypothesis 1.2

There is no significant difference between academic libraries in Malaysia in applying technological measures due to number of staff.

The Kruskal-Wallis test result shows no significant differences between Malaysian academic libraries in applying technological measures due number of staff ($H(4)=5.822$, $p \rangle 0.05$) (Table 5.15). Therefore, the sub-hypothesis 1.2 can also be accepted and it is concluded that there is no difference in applying technical measures among academic libraries that have less than 10 staff with academic libraries that have more than 191 staff.

Table 5.15. Kruskal-Wallis Test for Testing the Differences between Academic Libraries in Applying Technological Measure due to Number of Staff.

No	Variable	Chi-Square	df	p	Finding
1.	Technological measures	5.822	4	0.213	Not Significant

Testing Hypothesis 1.3

There is no significant difference between academic libraries in Malaysia in applying technological measures due to years in ICT implementation.

The results in the table (5.16) shows that the significance of technical measures is above 0.05, (H(3)=2.144, p › 0.05), denoting that there are no differences between academic libraries in Malaysia in applying technological measures due to the number of years in ICT implementation. Therefore, the sub-hypothesis 1.3 is accepted and it is concluded that there is no difference in applying technical measures among academic libraries that have less than five years ICT implementation than academic libraries that have ten years or more than ten years of ICT implementation.

Table 5.16: Kruskal-Wallis Test for Testing the Differences between Academic Libraries in Applying Technological Measure due to Years in ICT implementation.

No	Variable	Chi-Square	df	p	Finding
1.	Technological measures	2.144	3	0.543	Not Significant

Testing Hypothesis 1.4

There is no significant difference between academic libraries in Malaysia in applying technological measures due to yearly information systems security budget.

The result of Kruskal-Wallis test (Table 5.17) shows that the significance of technological measures is below 0.05 (H(3)=11.776, p ‹ 0.05). This implies that there is a difference between Malaysian academic libraries in applying technological measures due to the current budget allocated for IS security. According to this result, the sub-hypothesis 1.4 is rejected. It was summarised that there is a difference in applying technical measures in academic libraries in Malaysia that receive more than 5% yearly IS security budget compared to academic libraries that receive less than 1% budget allocation for their annual IS security.

Table 5.17. Kruskal-Wallis Test for Testing the Differences between Academic Libraries in Applying Technological Measure due to Yearly Information System Security Budget.

No	Variable	Chi-Square	df	P	Finding
1.	Technological measure	11.776	3	0.008	Significant

Testing Hypothesis 1.5

There is no significant difference between academic libraries in Malaysia in applying technological measures due to availability of information system (IS) security staff.

The results of rank test (Table 5.18) shows that academic libraries in Malaysia that have designated staff responsible for IS security had the highest score in applying technical measures.

Table 5.18. Rank Test between Academic Libraries in Applying Technological Measures due to Availability of Information System (IS) Security Staff.

	Availability of IS Security staff	N	Mean Rank	Sum of Ranks
Technological measures	No	16	14.41	230.50
	Yes	22	23.20	510.50
	Total	38		

Mann-Whitney U test (Table 5.19) reveals that there is a statistically significant difference between the academic libraries that have staff responsible for IS security and academic libraries that do not have staff responsible for IS security in applying technical measures (**U** = 94.500, **P** = 0.016). It can be further concluded that the availability of staff for IS security elicited statistically significant different in applying technical measures in Malaysian academic libraries.

Table 5.19. Mann-Whitney U Test for Testing the Differences between Academic Libraries in Applying Technological Measure due to Availability of Information System (IS) Security Staff.

No	Variable	U	p	Finding
1.	Technological measure	94.500	0.016	Significant

Testing Hypothesis 1.6

There is no significant difference between academic libraries in Malaysia in applying technological measures due to availability of wireless connection.

The results in the table 5.20 shows that the significance of technical measures is above 0.05, (H(1)=1.484, p › 0.05), which illustrates that there are no differences between Malaysian academic libraries in applying technical measures due to the availability of wireless connection. This result denotes that the sub-hypothesis 1.6 is accepted and therefore there is no difference in applying technical measures among academic libraries in Malaysia that have wireless connection and academic libraries that do not have wireless connection.

Table 5.20. Kruskal-Wallis Test for Testing the Differences between Academic Libraries in Applying Technological Measure due to Availability of Wireless Connection.

No	Variable	Chi-Square	df	P	Finding
1.	Technological measures	1.484	1	0.223	Not Significant

5.3 Differences in Applying the Organisational Measures by Selected Demographic Variables

This section presents the result of hypotheses testing on the differences among academic libraries in Malaysia in applying the organisational measures due to the type of university, number of staff, years in ICT implementation, yearly information system security budget, availability of information system (IS) security staff and availability of wireless connection.

5.3.1 Hypothesis 2

There are no differences denoting a statistical significance between academic libraries in Malaysia in applying organisational measures by type of university, years in ICT implementation, yearly ISec budget, availability of information system (IS) security staff and availability of wireless connection.

Testing Hypothesis 2.1

There is no significant difference between academic libraries in Malaysia in applying organisational measure dues to type of university.

The statistical result of Kruskal-Wallis test shows no significant differences between Malaysian academic libraries in applying organisational measures due to type of university ($H(2)=2.576$, $p > 0.05$) (Table 5.21). Therefore, hypothesis 2.1 can be accepted and it is concluded that there is no difference in applying organisational measures among academic libraries in the public and private universities as well as university colleges.

Table 5.21. Kruskal-Wallis Test for Testing the Differences between Academic Libraries in Applying Organisational Measures due to Type of Universities.

No	Variable	Chi-Square	df	p	Finding
1.	Organisational measures	2.576	2	0.276	Not Significant

Testing Hypothesis 2.2

There is no significant difference between academic libraries in Malaysia in applying organisational measures due to number of staff.

Kruskal-Wallis test result shows no significant difference between Malaysian academic libraries in applying organisational measures due number of staff ($H(2)=2.576$, $p < 0.05$) (Table 5.22). Therefore, the following hypothesis could be accepted and it is concluded that there is a difference in applying organisational measures between academic libraries that have 101 staff with academic libraries that have between 10 and 15 staff.

Table 5.22. Kruskal-Wallis Test for Testing the Differences between Academic Libraries in Applying Organisational Measures due to Number of Staff.

No	Variable	Chi-Square	df	p	Finding
1.	Technological measures	11.827	4	0.019	Significant

Testing Hypothesis 2.3

There is no significant difference between academic libraries in Malaysia in applying organisational measures due to years in ICT implementation.

The results in the table 5.23 shows that the significance of organisational measures is above 0.05, ($H(3)=1.706$, $p > 0.05$). This denotes that there are no differences between academic libraries in Malaysia in applying organisational measures due to years in ICT implementation. Therefore, sub-hypothesis 2.3 is accepted and it is concluded that there is no difference in applying organisational measures among academic libraries that have less than five years of ICT implementation with academic libraries that have 10 years or more of ICT implementation.

Table 5.23. Kruskal-Wallis Test for Testing the Differences between Academic Libraries in Applying Organisational Measures due to Years in ICT Implementation.

No	Variable	Chi-Square	df	p	Finding
1.	0rganisational measures	1.706	3	0.636	Not Significant

Testing Hypothesis 2.4

There is no significant difference between academic libraries in Malaysia in applying organisational measures due to yearly information system security budget.

The results of Kruskal-Wallis test (Table 5.24) shows that the significance of organisational measures is below 0.05 ($H(3)=15.548$, $p < 0.05$), which implies that there is a difference between Malaysian academic libraries in applying organisational measures due to the library's yearly information system security budget. According to this result, sub-hypothesis 2.4 is rejected. It is concluded that there is a difference in applying organisational measures among academic libraries in Malaysia that receive more than 5% yearly IS security budget with academic libraries that receive less than 1% budget allocation for their annual IS security.

Table 5.24. Kruskal-Wallis Test for Testing the Differences between Academic Libraries in Applying Organisational Measures due to Yearly Information System Security Budget.

No	Variable	Chi-Square	df	p	Finding
1.	Organisational measures	15.548	3	0.001	Significant

Testing Hypothesis 2.5

There is no significant difference between academic libraries in Malaysia in applying organisational measures due to availability of information system (IS) security staff.

The results of the rank test (Table 5.25) shows that Malaysian academic libraries that have designated staff for IS security had the highest score in applying organisational measures.

Table 5.25: Rank Test between Academic Libraries in Applying Organisational Measures due to Availability of IS Security Staff.

	Availability of IS Security staff	N	Mean Rank	Sum of Rank
Organisational measures	No	16	15.00	240.00
	Yes	22	22.77	501.00
	Total	38		

The Mann-Whitney U test reveals that there is a statistically significant difference between academic libraries that have designated staff for IS security and academic libraries that do not have staff responsible for IS security in applying organisational measures (U = 104.000, P = 0.033) (Table 5.26). It can be further concluded that the availability of staff for IS security elicited statistical significance in applying organisational measures in Malaysian academic libraries than academic libraries that have designated staff for IS security.

Table 5.26. Mann-Whitney U Test for Testing the Differences between Academic Libraries in Applying Organisational Measures due to Availability of Information System (IS) Security Staff.

No	Variable	U	p	Finding
1.	Organisational measures	104.000	0.033	Significant

n=38

Testing Hypothesis 2.6

There is no significant difference between academic libraries in Malaysia in applying organisational measures due to availability of wireless connection.

The results in the table 5.27 shows that the significance of organisational measures is above 0.05, (H(1)=3.390, p › 0.05), which illustrates that there are no differences between Malaysian academic libraries in applying organisational measures due to the

availability of wireless connection. This result denotes that sub-hypothesis 2.6 is accepted. Thus, there is no difference in applying organisational measures among Malaysian academic libraries that have wireless connection and academic libraries that do not have wireless connection.

Table 5.27. Kruskal-Wallis Test for Testing the Differences between Academic Libraries in Applying Organisational Measures due to Availability of Wireless Connection.

No	Variable	Chi-Square	df	p	Finding
1.	Organisational measures	3.390	1	0.066	Not Significant

5.4 Assessing the Status of Information Security Measures Implementation Using Information Security Measures Assessment Tool

Not much is known about the actual scenario of ISec practices specifically in the library setting. Thus, one could not assert whether libraries are lacking or adequate in information security. As highlighted by Newby (2002), ISec is often under-appreciated in libraries and this is surprising as information is the library's main business. Therefore, we attempt to propose an assessment tool for assessing the current ISec practices deployed by Malaysian libraries in managing their information security. This assessment tool is designed based on the proposed Library Information Security Assessment Model (LISAM) to encourage academic libraries to adopt the best practices for ISec measures. It represents a roadmap for the implementation, evaluation and improvement of IS security practices for a library that adopts it.

5.4.1 Assessment and Scoring Instrument

A scoring tool is designed specifically to determine the overall score for ISec safeguarding measures in a library as well as a total score for each component of ISec measures. This tool is an adaptation of the Information Security Governance (ISG) Assessment Tool for Higher Education (EDUCAUSE/Internet2 Security Task, 2004).

(a) Assessing the Overall Implementation Status of Technological Measures

As can be seen from Table 5.28, the status of technological measures in the sampled academic libraries (73.7%) in Malaysia is high. This result reveals that these academic libraries have implemented necessary technological security countermeasures to protect their hardware, workstations, servers, software, data, network and its physical facilities.

Table 5.28 Status of Technological Measures by Types of Academic Libraries in Malaysia

Status of Technological Measures		Type of University			Total
		Public university	Private university	University college	
Very High	Count	2	0	2	4
	% within column	14.3%	.0%	16.7%	10.5%
High	Count	10	10	8	28
	% within column	71.4%	83.3%	66.7%	73.7%
Medium	Count	2	2	2	6
	% within column	14.3%	16.7%	16.7%	15.8%
Total	Count	14	12	12	38
	% within column	100.0%	100.0%	100.0%	100.0%

Table 5.29 shows that academic libraries in this study have high presence of technological security controls for their hardware, software, workstations, servers, data, networks and physical facilities.

Table 5.29. Presence of Technological Measures in Malaysian Academic Libraries

Status of Technological Measures		Type of Academic Libraries at…			Total
		Public University	Private University	University College	
Hardware Security	Medium	1 (7.1%)	**6 (50.0%)**	**6 (50.0%)**	13 (34.2%)
	High	**8 (57.1%)**	4 (33.3%)	5 (41.7%)	**17 (44.7%)**
	Very High	5 (35.7%)	2 (16.7%)	1 (8.3%)	8 (21.1%)
	Total	14 (100.0%)	12 (100.0%)	12 (100.0%)	38 (100.0%)
Software Security	Medium	4 (28.6%)	**6 (50.0%)**	**6 (50.0%)**	16 (42.1%)
	High	**7 (50.0%)**	5 (41.7%)	4 (33.3%)	**16 (42.1%)**
	Very High	3 (21.4%)	1 (8.3%)	2 (16.7%)	6 (15.8%)
	Total	14 (100.0%)	12 (100.0%)	12 (100.0%)	38 (100.0%)
Workstation Security	Medium	2 (14.3%)	2 (16.7%)	2 (16.7%)	6 (15.8%)
	High	**6 (42.9%)**	**8 (66.7%)**	**8 (66.7%)**	**23 (60.5%)**
	Very High	**6 (42.9%)**	2 (16.7%)	2 (16.7%)	9 (23.7%)
	Total	14 (100.0%)	12 (100.0%)	12 (100.0%)	38 (100.0%)
Network Security	Medium	2 (14.3%)	3 (25.0%)	4 (33.3%)	9 (23.7%)
	High	**8 (57.1%)**	**6 (50.0%)**	**5 (41.7%)**	**19 (50.0%)**
	Very High	4 (28.6%)	3 (25.0%)	3 (25.0%)	10 (26.3%)
	Total	14 (100.0%)	12 (100.0%)	12 (100.0%)	38 (100.0%)
Server Security	Medium	2 (14.3%)	1 (8.3%)	2 (16.7%)	5 (13.2%)
	High	**6 (42.9%)**	**8 (66.7%)**	**8 (66.7%)**	**22 (57.9%)**
	Very High	**6 (42.9%)**	3 (25.0%)	2 (16.7%)	11 (28.9%)
	Total	14 (100.0%)	12 (100.0%)	12 (100.0%)	38 (100.0%)
Data Security	Medium	4 (28.6%)	4 (33.3%)	2 (16.7%)	10 (26.3%)
	High	**7 (50.0%)**	**7 (58.3%)**	**8 (66.7%)**	**22 (57.9%)**
	Very High	3 (21.4%)	1 (8.3%)	2 (16.7%)	6 (15.8%)
	Total	14 (100.0%)	12 (100.0%)	12 (100.0%)	38 (100.0%)
Physical Security	Medium	3 (21.4%)	3 (25.0%)	5 (41.7%)	11 (28.9%)
	High	**10 (71.4%)**	**9 (75.0%)**	**5 (41.7%)**	**24 (63.2%)**
	Very High	1 (7.1%)	0 (.0%)	2 (16.7%)	3 (7.9%)
	Total	14 (100.0%)	12 (100.0%)	12 (100.0%)	38 (100.0%)

Only four (10.5%) academic libraries have 'very high' implementation level for technological security controls. A cross tabulation between the status of technological measures and percentage of IS security budget reveals that these four academic libraries have received the highest percentage of budget allocation for IS security (Table 5.30). The assessment also reveals that six (15.8%) academic libraries have a medium level of technological security countermeasures. Unsurprisingly, two of these academic libraries received less than 1% of financial support for IS security.

Table 5.30 Status of Technological Measures by Percentage of Security Budget in Malaysian Academic Libraries

Status of Technological Measures		Percentage of Security Budget				Total
		Less than 1%	Between 1% to 3%	Between 4% to 5%	More than 5%	
Medium	Count	2	0	1	0	3
	% within column	25.0%	.0%	11.1%	.0%	9.4%
	% of Total	6.3%	.0%	3.1%	.0%	9.4%
High	Count	6	11	5	3	25
	% within column	75.0%	100.0%	55.6%	75.0%	78.1%
	% of Total	18.8%	34.4%	15.6%	9.4%	78.1%
Very High	Count	0	0	3	1	4
	% within column	.0%	.0%	33.3%	25.0%	12.5%
	% of Total	.0%	.0%	9.4%	3.1%	12.5%
Total	Count	8	11	9	4	32
	% within column	100.0%	100.0%	100.0%	100.0%	100.0%
	% of Total	25.0%	34.4%	28.1%	12.5%	100.0%

When comparing the status of technological countermeasures at three different types of academic libraries (Figure 5.1), it is apparent that 71.4% (10) of academic libraries at public universities, 83.3% (10) of academic libraries at private universities and 66.7% academic libraries at university colleges have high technological measures. Surprisingly, 16.7% (2) of academic libraries in university colleges and 14.3% (2) of academic libraries in public universities have very high technological countermeasures. In comparison, none of the academic libraries in private universities have very high technological security protection. However, 14.3% (2) of academic libraries in public universities, 16.7% (2) of academic libraries at private universities and 16.7% (2) of academic libraries in university colleges indicated medium level of technological countermeasures; thus pointing to the need of improvement to improve the situation.

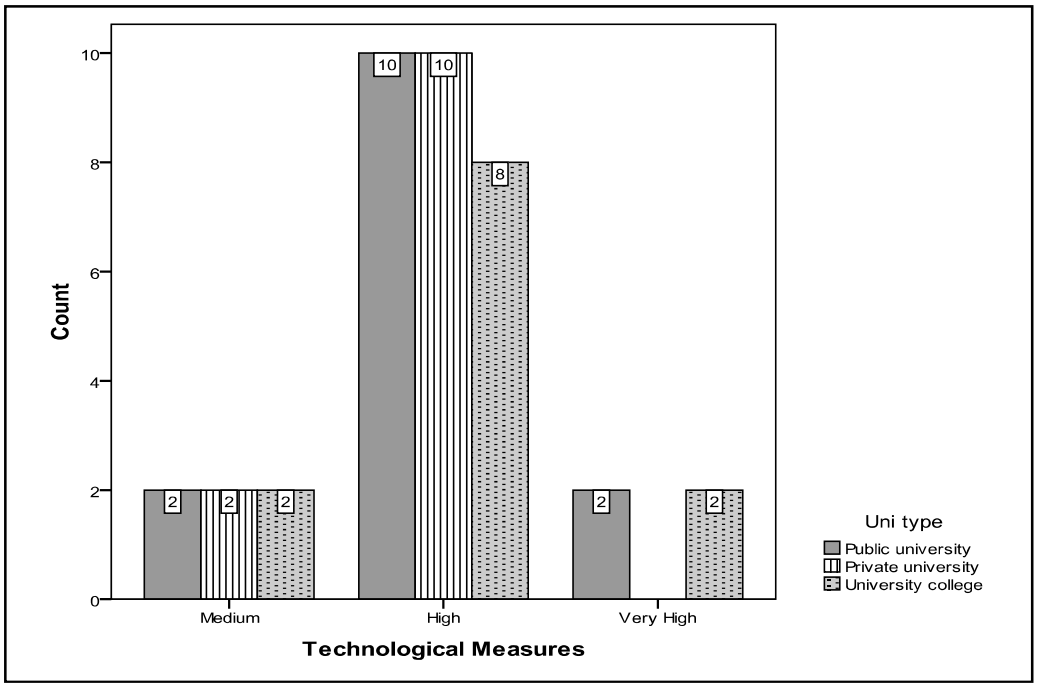


Figure 5.1 Status of Technological Measures by Type of Academic Library in Malaysia

(c) Assessing the Overall Implementation Status of Organisational Measures

In addition to the technological measures, this assessment tool also assesses organisational measures that encompass elements and issues related to governance, management and people. The second step is used to assess the presence of ISec 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 a library's daily routine. The final step evaluates the presence of ISec awareness activities in an academic library to strengthen the IS security initiatives within its community. Results indicated in Table 5.31 reveal that a majority of academic libraries (65.8%) in Malaysia require improvement on organisational countermeasures, whereas 22.0% are considered poor at the implementation of organisational security measures and a small number (13.2%) of academic libraries have good practices for organisational security measures. This

implies that academic libraries in Malaysia need to improve their security measures by strengthening the elements related to governance, managerial and people.

Table 5.31. Status of Organisational Measures by Type of Academic Library

Status of Organisational Measures		Type of University			
		Public university	Private university	University college	Total
Good	Count	3	1	1	5
	% within column	21.4%	8.3%	8.3%	13.2%
Needs improvement	Count	9	8	8	25
	% within column	64.3%	66.7%	66.7%	65.8%
Poor	Count	2	3	3	8
	% within column	14.3%	25.0%	25.0%	21.1%
Total	Count	14	12	12	38
	% within column	100.0%	100.0%	100.0%	100.0%

Table 5.32 clearly reveals that most academic libraries in public universities (64.3%), private universities (66.7%) and university colleges (66.7%) need to improve their organisational security measures. Table 6.5 also reveals that a number of public university libraries (14.3%), private university libraries (625.0%) and college university libraries (25.0%) have poor security practices for organisational measures. However, there are a small number of academic libraries in public universities (21.4%), private universities (8.3%) and university colleges (8.3%) that have implemented good security practices for organisational measures.

The results show an average emphasis on administrative tools and methods in the sampled academic libraries (Table 5.32). However, the presence of ISec policies, security procedures and controls and awareness creation activities is high among a majority of the academic libraries in this study.

Table 5.32. Presence of Organisational Measures in Malaysian Academic Libraries

Status of Organisational Measures		Type of Academic Libraries at…			Total
		Public University	Private University	University College	
ISec Policy	Medium	2 (14.3%)	4(33.3%)	2 (16.7%)	8 (21.1%)
	High	**9 (64.3%)**	**5 (41.7%)**	**8 (66.7%)**	**22 (57.9%)**
	Very High	3 (21.4%)	3 (25.0%)	2 (25.0%)	8 (21.1%)
	Total	14 (100.0%)	12 (100.0%)	12 (100.0%)	38 (100.0%)
Procedures and Controls	Low	1 (7.1%)	1 (8.3%)	1 (8.3%)	3 (7.9%)
	Medium	3 (21.4%)	3 (25.0%)	**6 (50.0%)**	12 (31.6%)
	High	4 (28.6%)	**6 (50.0%)**	3 (25.0%)	**13 (34.2%)**
	Very High	**6 (42.9%)**	2 (16.7%)	2 (16.7%)	10 (26.3%)
	Total	14 (100.0%)	12 (100.0%)	12 (100.0%)	38 (100.0%)
Administrative Tools and Methods	Low	1 (7.1%)	0 (.0%)	1 (8.3%)	2 (5.3%)
	Medium	5 (35.7%)	7 (58.3%)	7 (58.3%)	**19 (50.0%)**
	High	6 (42.9%)	3 (25.0%)	3 (25.0%)	12 (31.6%)
	Very High	2 (14.3%)	2 (16.7%)	1 (8.3%)	5 (13.2%)
	Total	14 (100.0%)	12 (100.0%)	12 (100.0%)	38 (100.0%)
Awareness Creation	Low	2 (14.3%)	0 (.0%)	0 (.0%)	2 (5.3%)
	Medium	**5 (35.7%)**	**6 (50.0%)**	3 (25.0%)	14 (36.8%)
	High	4 (28.6%)	4 (33.3%)	**7 (58.3%)**	**15 (39.5%)**
	Very High	3 (21.4%)	2 (16.7%)	2 (16.7%)	7 (18.4%)
	Total	14 (100.0%)	12 (100.0%)	12 (100.0%)	38 (100.0%)

When comparing the status of organisational and technological measures, it is apparent that a large number of academic libraries that have a high status of technological measures do not necessarily have the best or good organisational measures. As can be seen in Table 5.33, a majority of academic libraries that needs improvement (76.0%) and have poor practices (62.5%) for organisational measures have high technological security measures. This study has found that generally, many academic libraries in Malaysia have been focusing on technological countermeasures rather than organisational measures. Thus, it is necessary for these libraries to put organisational measures in place to secure the libraries' ISec which may require many approaches and methods and cannot rely solely on technology alone.

Table 5.33. Status of Organisational Measures by Status of Technological Measures

Status of Organisational Measures		Status of Technological Measures			
		Medium	High	Very High	Total
Good	Count	0	4	1	5
	% within column	.0%	14.3%	25.0%	13.2%
Needs improvement	Count	3	19	3	25
	% within column	50.0%	67.9%	75.0%	65.8%
Poor	Count	3	5	0	8
	% within column	50.0%	17.9%	.0%	21.1%
Total	Count	6	28	4	38
	% within column	100.0%	100.0%	100.0%	100.0%

(e) Assessing the Implementation Status of Information Security Measures in Malaysian Academic Libraries

Table 5.34 shows the results of overall status of IS security measures in Malaysian academic libraries. Findings indicate that approximately half of the academic libraries (55.3%) surveyed have good practices of IS security measures but require improvement on organisational measures. On the other hand, 21.1% of academic libraries have poor practices and need immediate attention on organisational measures. Only a small number of academic libraries (15.8%) have very good practices on IS security measures. A minority of the participating academic libraries (7.9%) has average practices but need improvement on organisational measures.

Table 5.34. Overall Implementation Status of Information Security Measures in Malaysian Academic Libraries

Overall Implementation Status of ISec Measures		Type of Academic Libraries at…			Total
		Public university	Private university	University college	
Very good	Count	3	1	2	6
	% within column	21.4%	8.3%	16.7%	15.8%
Good practices but needs improvement on organisational measures	Count	9	7	5	21
	% within column	64.3%	58.3%	41.7%	55.3%
Average practices but needs improvement on Organisational measures	Count	0	1	2	3
	% within column	.0%	8.3%	16.7%	7.9%
Poor practices needing immediate attention on organisational measures	Count	2	3	3	8
	% within column	14.3%	25.0%	25.0%	21.1%
Total	Count	14	12	12	38
	% within column	100.0%	100.0%	100.0%	100.0%

When comparing the three different types of academic libraries (see Table 5.34 and Figure 5.2), the striking results that emerged from the data are as follows: 64.3% of public university libraries, 58.3% of academic libraries in private universities and 41.7% of academic libraries in university colleges have good practices but need improvement on organisational measures. In contrast, only 21.4% of public university libraries, 8.3% of academic libraries in private universities and 16.7% of academic libraries in university colleges have very good practices on securing their information security. Only one (8.3%) academic library in public university and two (16.7%) academic libraries in university colleges have average practices but need improvement on organisational measures. The remaining 14.3% of the public university libraries, 25.0% of academic libraries at private universities and 25.0% of academic libraries in university colleges have poor practices, thus require immediate action for organisational measures.

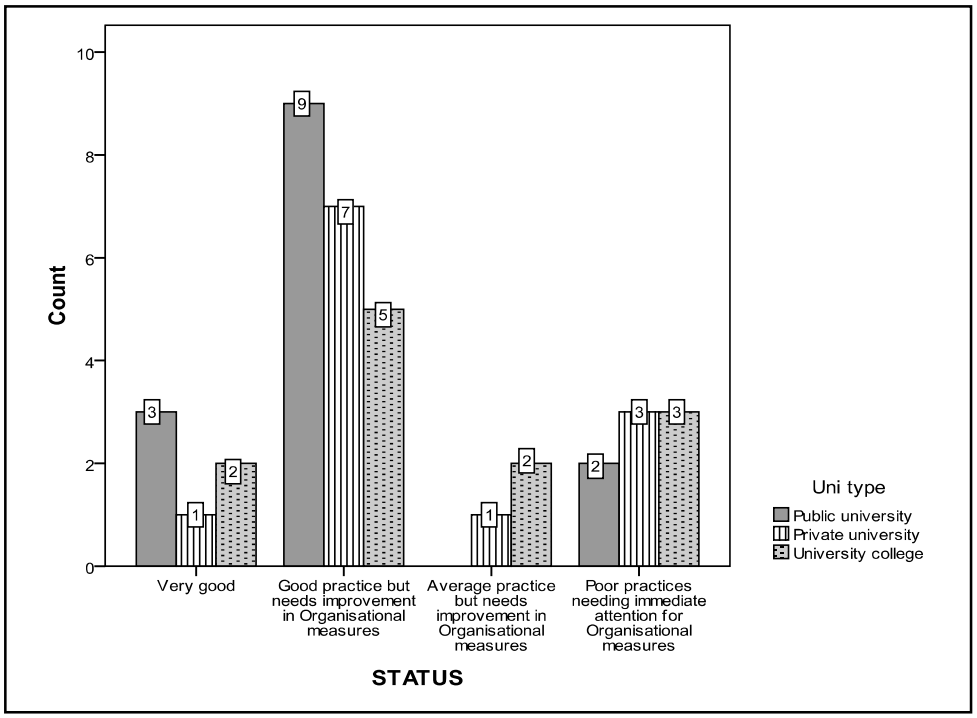


Figure 5.2 Overall Status of Information Security Practices in Malaysian Academic Libraries

5.5 Chapter Summary

This chapter presented an Information Security Measures Assessment Tool (adapted from Information Security Governance Assessment Tool for Higher Education) for academic libraries which assess technological measures and organisational measures as an attempt to determine the status of ISec measures in Malaysian academic libraries. The chapter started with a discussion on a scoring tool or assessment tool specifically designed to asses the status of technological measures and organisational measures as well as the overall status of ISec measures in Malaysian academic libraries.

The summary of results from assessing the implementation level of security measures in academic libraries in Malaysia has indicated the following:

(a) With regard to the level of implementation of hardware security measures, the use of CCTV, visual camera, magnetic detection system and electronic anti-theft

system at strategic places, public computer areas and server areas have the highest mean with a statistical value of 3.29 and standard deviation of 1.063.

(b) With regard to the level of implementation of workstation security measures, use of virus protection programs, configuration settings and security software programs for web browsers and email programs carried the highest mean with a statistical value of 3.87 and standard deviation of 0.78.

(c) In terms of network security controls, academic libraries in this study have configured their antivirus software and desktop security software to receive frequent updates (Mean=3.53, SD=0.86), used firewall (Mean=3.26, SD=1.20), and used digital signatures to assure the authenticity of any electronic documents sent via the library's network (Mean=3.13, SD=1.12). However, these network security controls have not been revised.

(d) Respondents believed that their academic libraries have restricted access to the file system in a server by using the file or directory permissions (Mean=3.53, SD=1.06), placed server(s) in a secure location (Mean=3.53, SD=1.18) and used up-to-date anti-virus software on servers (Mean=3.39, SD=1.13).

(e) Academic libraries in this study have regularly backed up the libraries' vital business information or records (Mean=3.55, SD=0.95), properly recorded the attributes for each removable media application and kept the media from any unauthorised device (Mean=3.32, SD=1.12) and used a combination of authentication systems to restrict access of library data and resources based on a variety of access rights (Mean=3.21, SD=1.07) but these kinds of security measures have not been reviewed regularly at their libraries.

(f) Administrative tools and methods had the lowest total mean score with a statistical value of 2.52 and standard deviation of 1.11.

(g) In terms of presence of ISec procedures and controls, the academic libraries in this study have implemented but never reviewed the controls and disciplinary procedures such as verbal warning, written warning, suspension and dismissal in case a library staff or patron breaches the IS security policies or rules (Mean=3.16, SD=1.03).

(h) Respondents indicated that their academic libraries have regularly identified and updated any threats that could harm and adversely affect critical operations of the libraries' IS security, but this stage has never been reviewed (Mean=3.05 SD=1.11).

(i) There is a difference between Malaysian academic libraries in applying technological measures due current budget allocated to the information system security ($H(3)=11.776$, $p < 0.05$).

(j) The availability of dedicated staff for IS security elicited statistical significance in applying technical measures in Malaysian academic libraries than academic libraries that do not have dedicated staff for IS security (**U** = 94.500, **P** = 0.016).

(k) There is a difference between Malaysian academic libraries in applying organisational measures due to the library's yearly information system security budget ($H(3)=15.548$, $p < 0.05$).

(l) Results revealed that 73% of academic libraries are at high level of implementation of technological measures, signifying that these academic libraries have implemented the necessary technological security countermeasures to protect their hardware, workstations, servers, software, data, network and physical facilities.

(m) The assessment on organisational measures revealed that 65% of academic libraries in Malaysia require improvement on organisational countermeasures.

(n) Findings revealed that 21% of the academic libraries are considered poor in implementation of organisational security measures, thus they need to improve their ISec measures by strengthening the elements related to governance, managerial and people.

(o) The overall status of ISec measures in Malaysian academic libraries revealed that less than 20% of academic libraries surveyed have very good practices of ISecmeasures and 50% of academic libraries have good practice of ISec measures but require improvement on organisational measures.

Chapter Six
Discussion and Conclusion

6.0 Introduction

It is claimed that a library, regardless of its size and type, might face the same security challenges, thus it requires effective information security management (ISM) in order to protect its critical library information systems (IS) services from interruptions and to make them available to its end users. It is also argued that the actual status of information security (ISec) practices within the library settings remains unclear as very few empirical studies related to ISec has been conducted specifically in a library setting.

The rationale of this research was to conduct ISec assessment in academic libraries by ascertaining the types of ISec threats faced and the level of implementation of security measures deployed by these libraries to ensure the security of their IS. The research also assessed the level of implementation of technical security measures (hardware, workstations, servers, software, data, network and physical facilities) and organisational security measures (security policy, procedures and controls, tools and methods, and awareness measures) in these libraries. The research also determined the overall status of ISec practices in these academic libraries.

The first section of this chapter provides an overview of all the previous chapters. It also summarises the main findings of the research. The next section discusses the contributions of this research. The third section presents the limitation of the research design and framework. The final section of this chapter closes with a suggestion on further research areas.

6.1 Overview of the Thesis

A sound ISec practice depends on effective ISec solutions, which encompass technical and non-technical safeguards to minimise vulnerabilities associated with a variety of threats (Westby and Allen, 2007; Scarfone, et al., 2008, Gupta and Sharman, 2009). This explains why many organisations have invested millions in securing their IT infrastructures in various forms of physical, personnel and administrative defences 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 necessary to be aware of IS security because much of the value of a library's main business or services is concentrated in the value of its IS.

The literature review in chapter two demonstrated there was a gap between findings in the library setting with other areas as many attempts have been made to understand the ISec landscape in health industries, banking industries, public governments, public offices and higher learning institutions, but very few research have paid attention to libraries. Research focusing on ISec threats recognised that security threats can be

found through natural disaster, technical error and human error (Bryson, 1999; Yeh and Cheng, 2007; Samy, Rabiah and Zuraini, 2009). Therefore, there is an encouragement to incorporate non IT-related countermeasures (some organisational and people issues) in dealing with ISec threats rather than just relying on the traditional approaches (technology-related countermeasures) (Dhillon, 2001; Calder and Watkins, 2003; Chan, et al., 2005; Ma and Pearson, 2005; Dhillon and Torkzadeh, 2006; Suhazimah, 2007; and Vaast, 2007). Chao (2005) described several methods, models, tools and packages for assessing general ISec programmes. However, these available tools have different target audiences and their coverage might not be suitable to the library characteristics and environments. By combining technical and organisational approaches, a model of to assess library ISec system was proposed and developed. The model was used as a basis for the research framework in this empirical study.

The research methodology and design that has been deployed in the study was presented in chapter three. It outlines the presentation of research design approach and discussion of the instrument development and measures taken to verify the reliability and validity of the instrument. Procedures for data collection are explained; the sample collected was described and this was followed by the plans for the data analysis phase. All these are associated with the research purposes and research questions in order to show the manner by which data are to be collected and analysed. Subsequently, collection of evidence and analysis through quantitative methods were performed in order to understand the ISec landscape in Malaysian academic libraries.

The research results are presented in two parts; chapter four reported and discussed findings related to research objectives 1 to 3, whereas the findings to objective 4 are revealed in chapter five. Chapter five presented the descriptive findings of the most

common perceived ISec threats experiences over six months in Malaysian academic libraries, the frequency of occurrence of these incidents, the most common perceived source of ISec threats and most importantly, the highlight on types and extent of technological measures and organisational measures deployed by these libraries to ensure the security of their information and resources. Chapter six reported the overall security status of all technological measures and organisational measures in Malaysian academic libraries, based on the proposed scoring tool and the Library Information Security Assessment Model (LISAM).

6.2 Discussion

6.2.10 The General Background of IT Infrastructures in Malaysian Academic Libraries

In this section, IT infrastructures refer to the number of PC allocations, availability of wireless connection, type of operating system used, years of Information Communication Technology (ICT) adoption, percentage of IS security budget and availability of IS security staff. Academic libraries in this study have demonstrated appropriate years of experience in the development and implementation of ICT, as approximately 46% of the libraries surveyed have five to 10 years experiences in using the ICT. It is not surprising that a majority of academic libraries in Malaysia have adopted wireless services. The mobility provided via wireless networks can better fulfill the computing needs of students and faculty members than the traditional wired version (Foster, 1996). Accordingly, a majority of these libraries (59.0%) provide less than 100 PCs for their patrons as patrons are allowed to use their own laptops in the library and connect to the free wireless connection. This study also serves as an evidence that

employees in academic libraries rely on PCs as their primary computing devices while performing their work, thus it is likely that their PCs contain all of their critical personal and business data. It is also apparent that many academic libraries in Malaysia, especially the libraries in university colleges, received inadequate financial support for IS security. This is parallel with Raymond (1990) who reported that smaller organisations often suffer from a lack of human and financial resources. As the implementation of security technologies can be costly, lack of financial support is likely to be one of the critical factors of ineffective IS security. Breeding (2003) asserted that libraries often do not have full-time systems administrators and security specialists to take charge of IS security. Inconsistent with Breeding's view, this study demonstrates some positive progress and concerns regarding the availability of IS staff in the majority of Malaysian academic libraries, even though some academic libraries in university colleges are still lagging in this regard.

6.2.11 The Most Common Perceived Information Security Threats in Malaysian Academic Libraries in Terms of Hardware, Software, Data, Network and Human-Related Threats.

Parallel with existing research findings, hardware security threats, human-related threats and physical threats were perceived as the most common security threats in Malaysian academic libraries. However, there is hope that data security threat is perceived as the least threatening to academic libraries. Since a library stores, processes and provides access to vast amounts of data, it will definitely need to ensure the security of its data against accidental loss, unauthorised modification and access by taking appropriate measures. Maintenance error is viewed as the most prevalent threat to hardware and software security in Malaysian academic libraries. On the other hand, IP spoofing attacks, use of weak passwords and unauthorised access are revealed as the most

ordinary network security threats faced by these libraries. Social engineering, loss of patron data and malicious code attacks have caused considerable disturbance to these academic libraries as dangerous to their vital data. It is possible that social engineering attacks may became common in libraries, because reference inquiries made by a patron about the IS resources available at a library may be used for nefarious purposes (Thompson, 2006).

Intrusion or unauthorised access into the library building is seen as another dangerous threat to academic libraries, which can lead to theft of valuable materials. This is why, unauthorised access into the library building, theft and leaking are still ranked as the popular threats to the academic libraries' physical facilities. This finding is supported by Lowes (2010) who reported that theft of computers and data storage devices account for 56% of all the breaches in healthcare data security in the United States. Many surveys and studies indicated that human errors are the most highly ranked security threats (Loch et al., 1992; Whitman, 2003; Im and Baskerville, 2005). Thus, there is little surprise that human error including data entry errors or carelessness, employee misconduct and unfaithful patrons were found to be the most commonly perceived IS security threats in Malaysian academic libraries. These erroneous actions by employees or users can threaten the integrity, availability, confidentiality and reliability of data.

6.2.12 The Frequency of Occurrence of Hardware Security Threats, Software Security Threats, Data Security Threats, Network Security Threats, Physical Security Threats and Human-Related Threats in Malaysian Academic Libraries.

It is interesting to discover the frequency of occurrence for hardware security threats, software security threats, data security threats, network security threats, physical security threats and human-related threats in these academic libraries. This survey

suggests that there were slightly high frequencies of occurrence of hardware maintenance errors, use of unauthorised hardware and malicious code attacks. Findings also indicated that these libraries experienced software maintenance errors, system errors and use of unauthorised software relatively frequently. In addition to unauthorised access, data loss due to wrong procedures of updating or backup, loss of patron data or privacy and phishing sometimes happened in these libraries. As for network security threats, findings indicated that there were slightly high frequencies of occurrence of IP spoofing attacks, use of weak password, spamming and malicious code attacks. Results also highlighted failure of power supply, leaking, theft, vandalism and unauthorised access into the library building occured relatively frequently in Malaysian academic libraries. As for human-related threats, findings show that employee misconduct, unfaithful staff, social engineering and unfaithful patrons sometimes posed as threats in Malaysian academic libraries. The same scenario have been reported by Deloitte Global TMT Security Survey 2009, where 41% of respondents in their survey experienced at least one internal security breach due to employee misconduct or human errors in the 12 months (Deloitte Touche Tohmatsu, 2009).

6.2.13 The Most Common Perceived Source of Information Security Threats in Malaysian Academic Libraries.

Judging from the security incidents that occurred in Malaysian academic libraries, there is a necessity to identify the main source of threats in these libraries. Findings revealed that there are similarities between the main source of threats in this study and those described by Bryson (1999). Bryson (1999) also reported that most of the security threats can be found through human error, natural disasters and hardware or software failures. A possible explanation for this might be that equipment failure and software failure always happens accidentally and it is undeniably difficult to handle unknown

and unpredictable failures, therefore, they can become a great source of threat to any computer system. As explained by Pearson (2001), 'many network failures have been due to such unpredictability [and] making an apparently small adjustment to a network can have devastating effects'. Another possible explanation for this is that ICT infrastructures require proper temperature, dust and humid-free area and undeniably, the environmental factors also play an important role to sustain these infrastructures. However, natural disasters sometimes bring loss to human beings and properties. For instance, the huge tsunami that struck Japan on March 11, 2011 affected Japan's eastern coast, killing 13,500 people and 17,000 people are still missing. This phenomenon has affected the US Cable Network (JUCN) and Asia Pacific Cable Network 2 (APCN2) cable networks that connect Malaysia to the United States of America (USA) and Hong Kong (HK). As a result, Malaysian Internet users experienced some difficulty in accessing international websites hosted in the USA, Europe and North Asia (Telekom Malaysia Berhad, 2011).

6.2.14 Level of Implementation of Technological Measures in Malaysian Academic Libraries.

Overall, the results suggest that Malaysia academic libraries have implemented several technical security controls for hardware security, software security, workstation security, network security, server security, data security and physical and environmental security. 42% of respondents reported that their academic libraries have implemented and regularly reviewed the use of close-circuit television (CCTV), visual camera, magnetic detection system and electronic anti-theft system at strategic places, public computer areas and server areas. Since security incidents may be caused by internal and external users, the video surveillance and CCTV systems serve as an economical

security tool to monitor work areas, identify visitors and employees, deter theft and ensure safety of the library building and other facilities (Rajendran and Rathinasabapathy, 2007). It is encouraging to find that almost half of respondents confirmed that the use of anti spyware software to detect and remove spyware threats was implemented and reviewed on regular basis in these libraries. It is probable that many library employees and patrons are aware of Internet security threats, thus, libraries should use anti-spyware software, spam filtering software, anti-phishing solutions and web filtering software to prevent any spyware, spamming, phishing attacks and access to inappropriate materials or sites (Ferrer and Mead, 2003; Ohaya, 2006; Ormes, 2001). 36% of respondents believed that their academic libraries have implemented and regularly reviewed the use of user identification and authentication before logging into the library's workstations, library network or campus network. A possible explanation for this might be that identification, authentication and authorisation are the most common access controls used in most IS to protect against access by unauthorised users. In a library, patrons must identify and authenticate themselves before gaining access to the library computers, databases and servers. If attempts of identification and authentication fail repeatedly, access is to be denied.

The current study also found that 47% of respondents agreed that their library's vital data and documents related to the server were regularly backed up and stored at an offsite location and the action is regularly reviewed. This finding is in agreement with Eisenberg and Lawthers (2005) suggested libraries to perform regular backups for the data, installation software, hardware specifications and installation passwords as they are vulnerable to viruses, hackers, fire or flood. 34% of respondents revealed that their libraries did not implement any data security measures to control unethical activity and disclosure of information. One of the possible reasons for this survey result is that

subjects in this study are all academic libraries in higher education institutions. The people in these organisations are students, academicians and staff; thus we can perceive that they have less malevolent intentions than external hackers. Nonetheless, according a survey report, the most common of internal IS security threats came from internal users, including employees, due to their curiosity, recklessness, lack of time, malevolence and ignorance (Vaast, 2007).

It is interesting to note that in this study, 71% of respondents agreed that their libraries did not use flood detectors or earthquake early warning systems as an emergency warning prior in case of flood and damaging ground movement. These findings are rather disappointing as flooding is the most significant natural hazard in Malaysia in terms of frequency and affected areas especially in East and West Malaysia. This result may be explained by the fact that most of the construction technology of integrated floating house system for flood-prone areas is still a new idea and approach in Malaysia. Also, not much has been written on the actual loss of data or access denial to computing resources due to floods in Malaysian libraries. Moreover, Malaysia is fortunate in the sense that it is not directly affected by serious disasters like earthquakes and volcanic eruptions. Therefore, there is no perceived need to consider the use of such mitigating measures to ensure the safety of these libraries from floods and earthquake threats.

6.2.15 Differences in Applying the Technical Measures due to Selected Academic Libraries' Demographic Profiles

It is reported that limitations of budget, time and staff to focus on security are seen as barriers to good security measures in an organisations (CIO Magazine and PriceWaterhouseCooper Worldwide Information Security Research Sudy, 2003). It is

rational to expect that management support should bring positive and proactive measures of ISec in libraries. This study found significant differences among academic libraries in Malaysia in applying technological measures due to yearly information system's security budget and availability of IS security staff. The implementation of security technologies can be costly. Therefore, it is likely true that high levels of implementation of technological measures in Malaysian academic libraries are associated with higher percentages of yearly IS security budget and availability of a designated individual for IS security in these libraries. However, this study revealed no significant differences among academic libraries in Malaysia in applying the technological measures due to type of university, number of staff, years in ICT adoption and availability of wireless connection in these libraries.

6.2.16 Level of Implementation of Organisational Measures in Malaysian Academic Libraries.

Prior studies have noted the importance of non IT-related countermeasures including some organisational and people issues in dealing with IS security threats (Backhouse and Dhillon, 2001; Chan, et al., 2005; Ma and Pearson, 2005; Dhillon and Torkzadeh, 2006; Suhazimah, 2007; and Vaast, 2007). However, very little was found in the literature on the types and implementation statuses of organisational measures such as security policies, security procedures and controls, administrative methods and awareness activities especially in libraries. The present study was designed to determine the types and actual implementation levels of organisational measures in Malaysian academic libraries. The results of this study show that 57% of respondents indicated that their academic libraries have implemented and regularly reviewed policies on acceptable use of wireless devices such as laptops, PDAs and hand phones. A possible explanation for this might be that accessing the Internet through a wireless network is

not always secure. Through this policy, patrons are alerted on the safety of their devices or laptop configurations resulting from the library's wireless connection and the risks of data transmitted across its wireless network. There is a possibility that data sent to or from an individual wireless device may be monitored, captured or altered by party outside a library.

It is interesting to note that 34% of respondents in this study believed that their academic libraries have implemented and regularly reviewed the controls and disciplinary procedures if a library staff or patron breaches IS security policies or rules. These findings further support the idea of ISACA (2009), which suggested that organisations establish and consistently apply a formal disciplinary process in dealing with those who commit security breaches such as employees and third parties. The current study also found that 31% of respondents noted that their libraries did not implement procedures for owner accountability to ensure protection of library IS assets. A possible explanation for these results may be a lack of awareness on the importance of creating guidelines and procedures in an organisation as one of the best tools in defending against human-created security problems as well as establishing details on the roles and responsibilities for security administrators and users to maintain the security of the systems and networks (Conklin, et al., 2005). Only 36% of respondents believed that their academic libraries have fully implemented procedures on handling, reporting and responding to ISec events to affected parties such as individuals, law enforcement and campus or parent organisations.

This study has been unable to demonstrate the importance of ISec awareness programmes in Malaysian academic libraries. Findings revealed that 21% of respondents noted that all staff and patrons at various levels did not receive appropriate ISec training and education in their academic libraries. Thus, organisations, including

libraries, are suggested to focus on educating personnel through a security programmes that addresses user education, awareness and training on policies and procedures that affect them (Merkow and Breithaupt, 2005). Many respondents (47%) indicated that they received only some support and commitment from the top management to coordinate the implementation of IS security controls in their libraries. This study produced results that corroborate the findings of a great deal of the previous work in this field. As highlighted by Hight (2005), top management must take an active approach to the security of an organisation by supporting and following the policy themselves. 41% of respondents also revealed that vulnerabilities related to their library IS were not identified and regularly updated. This finding is somewhat discouraging as properly designed and periodically updated ISec awareness policies within an organisation is vital in order to make the end-users aware of IS security issues, including the potential breaches to security and of the risks associated with these breaches (Vaast, 2007).

6.2.17 Differences in Applying Organisational Measures due to Selected Academic Libraries' Demographic Profiles

This study found significant differences among academic libraries in Malaysia in applying the organisational measures due to number of staff, yearly information system security budget and availability of IS security staff. This study is parallel with findings from Chang and Ho (2006), who also concluded that factors such as top management support and organisation size are related to the implementation of security controls in various organisations in Taiwan. It is possible that larger academic libraries could offer more sophisticated security measures than small academic libraries. In ISec management, it is more meaningful to use number of employees to measure the size of a

firm because each employee is an independent variable in managing ISec (Kim and Kbzullak, 2008).

It is also highlighted that a security education and awareness effort would benefit ISec efforts more than lack of support from the management of an organisation (Hight, 2005). This implies that it is not easy to implement security controls when people do not have enough orientation or education about the best ISec practices. Therefore, it is evident that availability of designated staff IS security elicited statistical significance in applying organisational measures in Malaysian academic libraries. However, this study revealed no significant differences among academic libraries in Malaysia in applying the organisational measures due to type of university, years in ICT adoption and availability of wireless connection in these libraries.

6.2.18 The Overall Security Status of Technological Measures and Organisational Measures in Malaysian Academic Libraries.

This study set out with the aim of assessing the overall security status of all technological and organisational security measures in Malaysian academic libraries. The most important finding was a general picture on the status of IS security measures of academic libraries in Malaysia. The results revealed that these academic libraries demonstrated a higher implementation of technological measures than organisational measures in protecting each library's IS security. As predicted earlier, results also showed that technological and organisational security measures have been more widely adopted in public university libraries as compared with other academic libraries in private universities and the university colleges.

The current study also found that the presence of technological measures is high as there was visible presence of technological security controls for the hardware, software, workstations, servers, network and physical facilities in Malaysian academic libraries.

This result may be explained by the fact that these academic libraries have been focusing more on 'visible' prevention measures demonstrated by observable physical aspects of monitoring tools such as security cameras, locks, warning signs and fences that are more noticeable to library staff, users and outsiders as compared to less visible security controls such as implementation of security policies, procedures and awareness programmes for staff. This is undeniably true as some solutions to security challenges have been technological (Volonino and Robinson, 2004).

In general, the presence of organisational security measures in most academic libraries is average. Detailed analysis showed there was clear presence of ISec policies, security procedures and awareness creation activities in Malaysian academic libraries. However, there was a lack of emphasis on administrative tools and methods in Malaysian academic libraries. Therefore, it is necessary to put organisational measures in place as relying on technology alone will not solve the security problems (Conklin, et al., 2005). Overall, half of the academic libraries (55.3%) surveyed have good practices of IS security measures but require improvement on organisational measures. This improperly secured situation could result in a variety of security issues as most of today's security challenges are related to human and organisational aspects (Anderson, 2007). This result corroborates the findings of a great deal of the previous work in other fields. Many researchers has highlighted the importance of creating the policies, standards, guidelines and procedures in an organisation as one of the best tools in protecting against human-created security problems as well as establishing details on the roles for security administrators and users to maintain the security of the systems (Dhillon, 2001; Conklin, et al., 2005).

6.4 Contributions

Information is the lifeblood of a library and obviously, there are risks involved in the library environments as libraries are increasingly dependent on IS and Internet connectivity to provide online resources and digitally delivered services to local and remote patrons. With the rising number of security breaches and the complexities of computer attacks, security managers everywhere are looking for new solutions and approaches in ISec management. Only after knowing the current security threats and assessing the implementation level of information security, can academic libraries understand the clear picture of their security programmes. This research has aimed to study the perceived ISec threats in Malaysian academic libraries and propose an approach to assess ISec management in libraries.

6.4.1 Framework Contributions

The model put forth in this research contributes in several ways to the Library and Information Science (LIS) research community. Firstly, this study interpreted and re-contextualise the works of Hagen, Albrechtsen and Hovden (2008) who developed the Organisational Information Security Staircase Model to assess the implementation of organisational ISec measures and the effectiveness of such measures in a selection of Norwegian organisations (Figure 6.1).

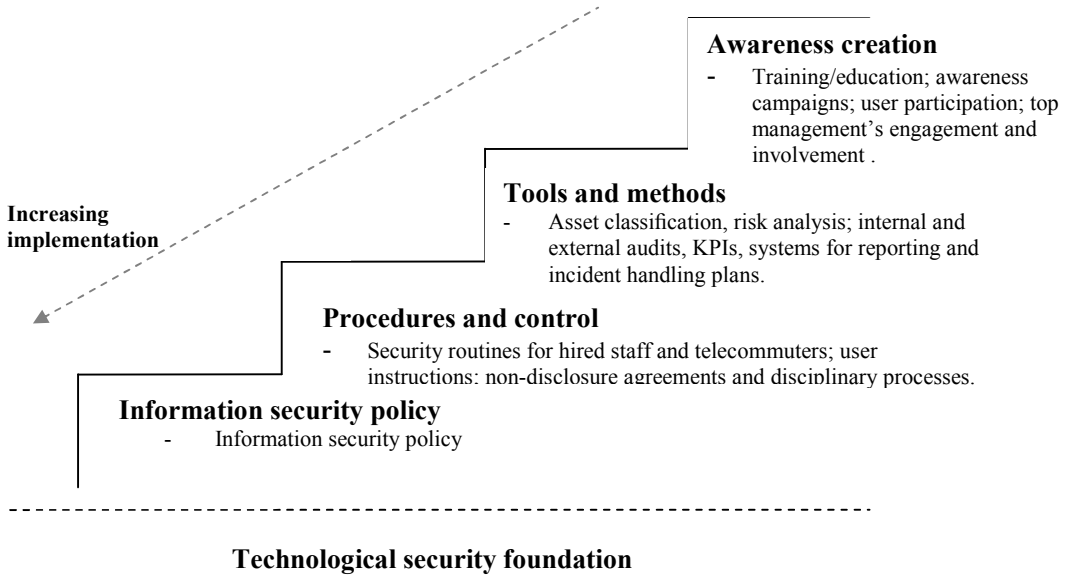


Figure 6.1. Organisational Information Security Staircase Model (Hagen, Albrechtsen and Hovden, 2008).

This interpretation is adopted and adapted by the researcher to formulate and frame the use of countermeasures to design an information security assessment instrument in the library context. The framing should allow for more accurate classifications of existing and future technological and organisational countermeasures. By classifying countermeasures, their strengths, weaknesses as well as gaps could be identified more clearly in terms of which countermeasures have been implemented and those which have not. The new proposed instrument is named a Library Information Security Assessment Model (LISAM) and was also developed as a research framework used as a basis for data collection and subsequent analysis of the findings (Figure 6.2).

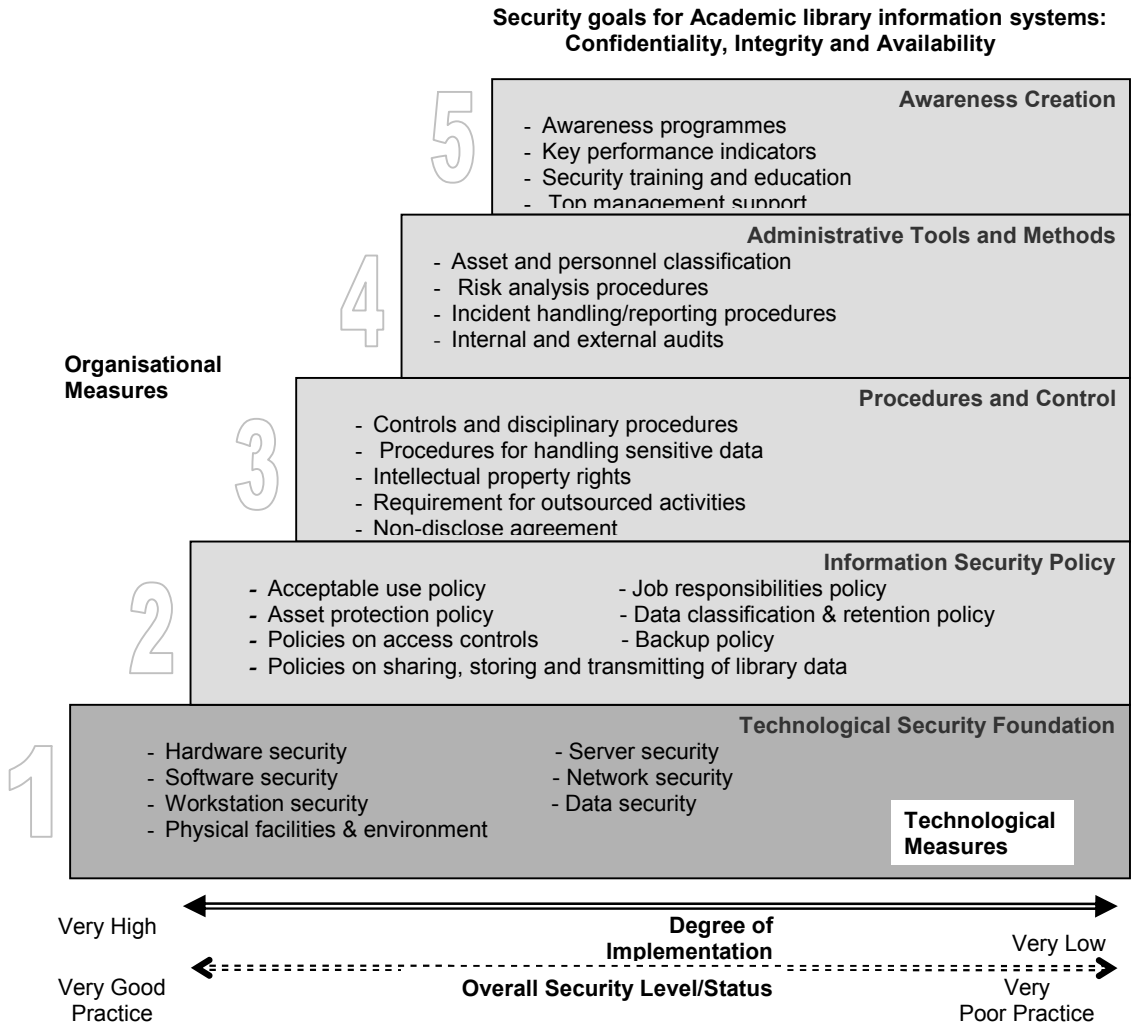


Figure 6.2. Library Information Security Assessment Model (LISAM)

6.3.2 Methodological Contributions

This quantitative survey shows how to apply the framework developed with the type of data required in assessing the status of ISec in academic libraries. The researcher has proposed a library information security assessment model (LISAM) model that is used for data collection. This framework can be used as an alternative model in the organisational studies of ISec in libraries. Although it may not be sufficient to explain the complexities of technological and organisational related security issues, this model may be used by researchers of ISec as a frame of reference or a starting point to explore

the dynamics of technological and organisational issues surrounding security in libraries. This research can be replicated using the same research instrument and data collection techniques when assessing the status of an ISec in other types of libraries or organisations.

6.3.3 Assessment Instrument to Assess the Level of Information Security Measures Implementation

It is highlighted that many organisations, including libraries, have put too much focus on technological factors to secure their IS while neglecting the necessary and important factors of organisational issues. This current study extends the constructs in the Organisational Information Security Staircase Model by specifying the assessment of technological as well as organisational measures, thus providing a more thorough understanding of the status of all technological measures as well as organisational measures in a library setting. The five constructs assessed in the instruments have been validated with Cronbach's alpha correlation coefficients above $\alpha = 0.70$. The findings of this research contributed to the ISec domain in the library field as knowledge in understanding the types of security tools academic libraries have, their implementation levels as well as their overall ISec statuses.

6.3.4 Practical Contributions

The results of the current study are also relevant to practitioners. Firstly, the proposed information security assessment model consists of technical and organisational approaches for IS security assessment in library. This is parallel with the current evolving body of knowledge around the principles and practices of cyber security that gives proper attention to the roles of people (i.e. organisational dimensions), process (i.e.

policies and procedures dimensions) and technology (i.e. technical dimensions) in order to implement an effective digital security programmes (Volonino and Robinson, 2004).

Secondly, this study reveals that security is more than just a traditional technological problem as has been generally perceived. This study offers insights into the people and processes as issues affecting ISec in libraries; which may be helpful to researchers who adopt research approaches that may have been based on an understanding of security issues from social and technical standpoints. This infers that the knowledge of ISec issues must be included in the training of future librarians and knowledge workers. Academic institutions, particularly the libraries or information science faculties and the National Library of Malaysia may want to include ISec in the syllabus of training programme as the current library services and in the future will be very much globalised and dependent on IS.

Thirdly, the model can provide more insight into understanding information security management in a library. It can be used by system librarians as an assessment tool for libraries by enabling them to compare their outfits to similar or different libraries in terms of size and type. This approach would allow a library to compare specific types of countermeasures in use by their own libraries and compare them to those of their competitors, thus enabling them to gain insight into how effectively they are managing there is security risks. The model could also be used by libraries to provide a guide on security budget planning. Analysis based on this model provides libraries with insight into their current status of IS security practices and use of various countermeasures. Based on their own analyses, they could then target specific allocation of funds to improve or add new additional security measures at any times based on their security needs and requirements.

Reviewing the literature related to library ISec threats reveals insufficiency of available studies in that particular area of research. The study assesses current ISec threats in Malaysian academic libraries and presents a potential categorisation of general ISec threats in a library setting (Table 6.1). Based on the findings, the researcher has attempted to develop an index of the most common perceived threats to ISec in academic libraries, which are classified into hardware, software, network, data, physical and human threats in Malaysian academic libraries. This is another important research contribution to the ISec domain in the library field.

Table 6.1: Index of the Most Common Perceived Hardware, Software, Network, Data, Physical and Human Threats in Malaysian Academic Libraries.

Threat Category	The Most Common Perceived Threats
Hardware	Maintenance errors
	Failure of communication equipments
	Electromagnetic interference
	Malware and malicious code
	Theft, physical sabotage, vandalism of ICT hardware equipments
	Installation/ use of unauthorised hardware
Software	Maintenance errors
	System errors or failure
	Installation/ Use of Unauthorised programmes or software
	Adware and Spyware
	Hacking/Intrusion/ unauthorised access to system resources
	Malware and malicious code
Network	IP spoofing attacks
	Misrouting/re-routing of messages
	Weak password
	Hacking/ Intrusion/ unauthorised access
	Packing sniffs
	Transmission errors
Data	Impersonation/ social engineering
	Loss of patron data/privacy ideas
	Phishing/ pharming
	Exposure of patrons sensitive data through web attack
	Malware and malicious code
	Destruction due to natural disaster

Table 6.1: Continued.

Threat Category	The Most Common Perceived Threats
Physical	Intrusion/unauthorised access into library building
	Leaking
	Theft, burglary, sabotage, vandalism or physical intrusions
	Natural calamity
	Hazardous material accident
	Power supply failure
Human (Other threats)	Human errors
	Employee misconduct
	Unfaithful patrons
	Online extortion
	Social engineering
	Unfaithful staff

6.4 Limitations

This study is not without limitations. The main contribution of the research is the assessment of implementation status of each technological measure as well as organisational measure in Malaysian academic library setting. Due to the small sample size, the findings may not be applicable to other types of libraries and organisations in Malaysia.

Secondly, with respect to data collection, 66% of individuals sampled were in managerial positions with responsibility for ISec in their respective academic libraries. It is likely that they were all sensitive to ISec concerns. However, it is also possible that some of the respondents may have little or no understanding of ISec issues. In that sense, they may be detached from the realities of ISec issues. This is common when using survey responses from the same source because a single respondent for each survey can only yield one perspective. Others within the same organisation may perceive conditions to be significantly different. However, adequate confidence can be

placed in the findings of this research because of the diversity among participants, which minimise the influence of bias. The majority (90%) of respondents were from the management division, which include the librarians or library executives, heads of automation unit, IT officers or IS officers, senior librarians, automation librarians and chief librarians or deputy chief librarians.

Another possible limitation is the way threats are treated using the current research design. For ease of analysis, threats of IS in academic libraries were treated holistically based on six security threats components. This means that all threats were grouped together and treated equally. Realistically, this is not likely to be the case. More likely, some threats are more serious than others in terms of potential damage, costs and so on. As a result, caution should be used when drawing conclusions from the results of this study.

Fourthly, although the choice of a quantitative survey method in this research was adequate in obtaining data to answer the research questions, future research may employ qualitative research design involving case studies or observations. Integrative triangulation approach is another possible method that can be used by combining both quantitative and qualitative design involving in-depth interviews with top-level management. Interviews with the top-level management could shed light on key metrics that could possibly be used to identify the number of stages present as well as key characteristics of particular stage and the conditions necessary for moving from one stage to the next.

This research is a PhD requirement, thus it is a result of a learning process and a 'one-man show' with no additional labour or aid. The limitations of fund, time and manpower restricted researcher's ability to further explore many other domains of ISec management in other types of libraries. Also, due to time limitation, the scoring tool proposed for assessing ISec measures for library was not validated.

6.5 Suggestions for Future Research

The knowledge gained from this research is not only important for researchers of information security, but will also be useful for other researchers in the field of library and information science (LIS) as there are other possible ISec areas to be explored. In future investigations, it might be possible to use the proposed model in this research and explore the relationship between the various countermeasures and library characteristics. It is also possible to further refine or redesign the model for additional important insights regarding issues affecting security in libraries. More research is also needed to collate evidence from libraries in other developing countries. A comparative study could be carried out to investigate the significant differences between developing and developed countries regarding the IS security issues investigated.

There will always be new threats to safe Internet use and library IS security. Being aware of the threats should always be the first step in establishing a sound security policy and security control. This study had identified the common perceived IS security threats in Malaysian academic libraries in terms of hardware, software, data, network and human-related threats. Additional research should further explore the relationship between these threats and library characteristics. Further research should also be performed to investigate the impacts of these security threats in terms of potential damage and costs to libraries.

This study revealed that inadequate financial support for IS security was prevalent among the academic libraries, especially those university colleges. It is interesting to discover how these academic libraries adjust their security posture over time as well as striking a balance between limited funds and implementation of necessary ISec protection that best meet their security needs.

In this research, social engineering was found to be one of the most commonly perceived ISec threats in Malaysian academic libraries. Another line of research that could be extended from this current research is the exploration of issues related to social engineering (i.e. the use of non-technical means to gain unauthorised access to information or computer systems) through the reference interviews or when using the real-time digital reference services.

One of the issues that emerged from this study is the actual status of IS security readiness among librarians in Malaysian libraries. A further study could focus on assessing the information security readiness, infrastructures, computer literacy and daily security practices. There is also a need for a comprehensive assessment to better understand the factors that may challenge security readiness of librarians in Malaysian libraries.

6.6 Conclusion

Security is not easy to describe. Information security (ISec) assessment is a step to evaluate the status of an information system security. This study provides a quantitative approach that investigated the implementation status of ISec measures through the opinions of individuals responsible for IS and ICT in Malaysian academic libraries. It makes a contribution by providing an insight into what extent ISec practices are being implemented within these libraries. It was evident that the levels of implementation of technological measures are high as there is clear presence of technological security controls for the hardware, software, workstations, servers, network and physical facilities in Malaysian academic libraries. This may be related to the years of experiences in ICT or computerisation in each library. However, the implementation levels of organisational measures in these academic libraries are considered average. This may be due to the over-emphasis on technology as the sole solution to all security problems and needs to be investigated further. The study pointed that if ISec is to be effective, libraries need to incorporate technical measures as well as ISec policies, security procedures and awareness creation activities in their security programmes. This survey also revealed that hardware security threats, human-related threats and physical threats were perceived as the most common security threats in Malaysian academic libraries. As human-created security problems remain rampant, it is necessary to strengthen ISec policies and security awareness initiatives in these academic libraries. To conclude, evaluating ISec should not be a one-time exercise, rather the assessment efforts need to be continuous to ensure that progress is made towards better ISec environments.

References

Abdul-Gader, A. (1999). *Managing Computer Based Information Systems in Developing Countries: A Cultural Perspective.* Idea Group Publishing, London.

Adam, J. A. (1992). Data Security-Threats and Countermeasures. *IEEE Spectrum*. 29(8):21-28.

Adekanye, E.A. (2010). Insurance Coverage in Nigerian Academic Libraries. *Library Philosophy and Practice.* Retrieved January 19, 2011, from http://www.webpages.uidaho.edu/~mbolin/adekanye1.htm.

Adomi, E.E. and Eruvwe, U. (2004) Staff discipline in Nigerian university libraries. *Library Management*. 25 (4/5):223 – 229.

Ahmad A. A. M. (2005). Investigating the Perceived Threats of Computerized Accounting Information Systems in Developing Countries: An Empirical Study on Saudi Organizations J. King Saud Univ. *Computer and Information Science*. 18:1-6. Retrieved August 10, 2007, from http://digital.library.ksu.edu.sa/V42M340R2631.pdf.

Ahmed, Md. I.. (2011). A new theory of management information security systems In libraries. *DSpace at Jindal Global University*. Retrieved July 19, 2011, from http://dspace.jgu.edu.in:8080/dspace/bitstream/123456789/156/1/A%20NEW%20THEORY%20OF%20MANAGEMENT%20INFORMATION%20001.pdf.

Akintunde S.A. (2004). Libraries as tools for ICT development. *Nigerian Library Association 42nd National Conference and AGM at Akure, Nigeria June 20-25, 2004*. p10.

Akuezuilo, ED. and Agu .N. (2002) *Research arid Statistics in Education and Social Sciences*, Nuel Centi Publishers and Academic Press Ltd.

AlAboodi, S.S. (2006). A New Approach for Assessing the Maturity of Information Security. *ISACA: Journal Online*. Retrieved January 5, 2007, from http://www.itgi.org/Template.cfm?Section=Home&CONTENTID=34805&TEMPLATE=/ContentManagement/ContentDisplay.cfm.

Al-Salihy, W., Ann, J. and Sures, R. (2003). Effectiveness of Information Systems Security in IT Organizations in Malaysia. *The 9th Asia-Pasific Conference on Communications, 2003. APCC 2003. 2: 716-720. Retrieved Nov 10, 2007, from IEEE Xplore Database.*

Al-Suqri M. and Afzal W. (2007). Digital age: Challenges for libraries. *Information, Society and Justice* . 1(1), 43-48.

American Insurance Group (AIG). (2003). AIGnetAdvantage Suit, Information Security Self Assessment. Version 3.0. *American Insurance Group,* Inc. Retrieved February 20, 2008, from http://www.aignetadvantage.com/content/netad/netadvantage_assessment.doc.

Anday, A., Francese, E., Huurdeman, H.C., Yilmaz, M. and Zengenene, D. (2012). Information Security Issues in a Digital Library Environment: A Literature Review. *Bilgi Dünyasi*. 13 (1):117-137. Retrieved November 20, 2012, from bd.org.tr/index.php/bd/article/download/7/27.

Andrew G., Kotulic, J. and Clark, G. (2004). Why there aren't more information security research studies. *Information & Management*. 41(5): 597-607.

Arizona Cyber Security Alliance (ACSA). (2004). Arizona Cyber Alliance Self Assessment Questionnaire. Retrieved February 20, 2008, from http://www.azsecurity.org/toolkit_questions.asp.

Backhouse, J. and Dhillon, G. (2001). Current directions in IS security research: toward socio-organisational perspectives. *Information Systems Journal* 11 (2): 127-153.

Badilah S., Shahar B. J. and Chew, W. F. (1996). Malaysian libraries for national development: a country report. In *the Tenth Congress of Southeast Asian Libraries (CONSAL X), 21 – 25 May 1996, Kuala Lumpur.*

Bakari, J.K., Tarimo, C.N., Yngstrom, L., and Magnusson, C. (2005). State of ICT Security Management in Institutions of Higher Learning in Developing Countries: Tanzania Case Study. Proceedings of the Fifth IEEE International Conference on Advanced Learning Technologies (ICALT'05). p. 1007-1010. *IEEE Computer Society*. Retrieved January 12, 2009 from IEEE Explore.

Banerjee, K. (2003). How much security does your library need? *Computers in Libraries*. 23(5), 12-16.

Basariah S., Mahamad T. and Shamharir, A.(2000) Computer Crime and Security: A Survey of Malaysian Financial Institutions. *Proceedings of the International Conference on Electronic Commerce: Emerging Trends in E-Commerce. Malaysian Multimedia University 21-23 November 2000, Kuala Lumpur.* Retrieved November 5, 2008, from www.psb1.uum.edu.my/tesis/.../2002/Basariah%20Salim,%20Dr,%20Mahamad%20Tayib%.

Baskerville, R. (1996). *A taxonomy for analyzing hazards to information systems, Information systems security: facing the information society of the 21st century*. Chapman & Hall, Ltd., London, UK.

Bell, D. E. and Lapadula, L. (1975). Secure Computer System: Unified Exposition and Multics Interpretation. *Technical Report ESD-TR-75-306.*

Berghel, H. (2005) The Two Sides of RoI: Return on Investment vs. Risk of Incarceration, *Communications of the ACM*. 48 (4): 15-20.

Beznosov, K. and Beznosova, O. (2007). On the imbalance of the security problemspace and its expected consequences. *Information Management and Computer Security*. 15(5):420 – 431.

Bishop, M. (2005). An introduction to computer security. *The NIST handbook*. Boston: Addison Wesley.

Bolan, C. and Mende, D. (2004). *Computer Security Research: Approaches and Assumptions*. Retrieved November 1, 2007, from http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2004/aism/Bolan-Mende.pdf.

Boudreau, M.-C., Gefen, D., and Straub, D. (2001). Validation in IS Research: A State-of-the-Art Assessment. *MIS Quarterly*. 25(1): 1-16.

Bradbard, D. A., Norris, D.R. and Kahai, P.H. (1990). Computer Security in Small Business: An Empirical Study. *Journal of Small Business Management.* 14(1):9-19.

Brainstorming Report. (2001). Digital Libraries: Future Directions for a European Research Programme. San Cassiano, Alta Badia-Italy, June 13-15. Retrieved April 23, 2006, from http://delosnoe.iei.pi.cnr.it/activities/researchforum/Brainstorming/brainstorming-report.pdf.

Breeding, M. (2006). Wireless Networks in Libraries. *SOLINET Workshop* (Warner Robins, GA).

Breeding, M. (2003). Protecting your library's data. *Computers in Libraries*. Retrieved November 12, 2007, from http://www.librarytechnology.org/diglibfulldisplay.pl?SID=20110116654235839&ode =bib&RC=10343&Row=31&.

Brownlee, N. and Guttman, E. (1998). *Expectations for Computer Security Incident Response.* Retrieved November 5, 2007, from http://tools.ietf.org/html/rfc2350.

Bruhn, M., Gettes, M., and West, A. (2003). Identity and access management and security in higher education. *EDUCAUSE Quarterly*, 26(4): 12–16. Retrieved October 12, 2008, from http://www.nmiedit.org/CAMP/EDIT_IdM/Resources/Docs/eqm0342.pdf.

Bryson, J. (1999). *Effective library and information center management*. 2nd Ed. Hampshire: Gower Publishing Ltd. p. 148 -149.

Buecker, A., Borrett, M., Lorenz, C., and Powers, C. (2010). Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security. *IBM RedGuide, New York.* Retrieved January 1, 2011, from http://www.redbooks.ibm.com/redpapers/pdfs/redp4528.pdf.

Brns, N., and Grove, S. (2004). *The Practice of Nursing Research: Conduct, Critique & Utilization*. 5 ed. Saunders.

Cain, M. (2003). Cybertheft, Network Security, and the Library without Walls. *The Journal of Academic Librarianship*. 29 (4):245-248.

Calder, A., and Watkins, S. (2003). IT governance: a manager's guide to data security & BS 7799 / ISO 17799. 2nd ed. London: Kogan Page.

Casmir, R. (2005). A Dynamic and Adaptive Information Security Awareness (DAISA). *Stockholm University, Department of Computer and Systems Sciences*.

Centers For Medicare & Medicaid Services (CMS). (2002). CMS Information Systems Threat Identification Resource. *Center for Medicare and Medicaid Services, Baltimore*. Retrieved November 1, 2007, from http://www.iwar.org.uk/comsec/resources/fasp/Threat_ID_resource.pdf.

Centers for Medicare & Medicaid Services (CMS). (2005). *HIPAA Security Series. Security Standards: Administrative Safeguards.* Retrieved April 15, 2007, from http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf.

Chan, Y. E., Culnan, M. J., Greenaway, K., Laden, G., Levin, T. and Smith, H. J. (2005). Information privacy: management, marketplace, and legal challenges. *Communications of the Association for the Information Systems.* 16: 270-298.

Chan, M., Woon, I. M. Y. and Kankanhalli, A. (2005). Perceptions of Information Security at the Workplace: Linking Information Security Climate to Compliant Behavior. *Journal of Information Privacy and Security*. 1(3).

Chang, S. E. and Ho, C. B. (2006). Organisational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*. 106(3):345–361.

Chao, Shu-chuan. (2005). *An approach to information system security assessment*. D.B.A., Cleveland State University, 2005. 159 pages. Retrieved December 21, 2007, from AAT 3195528. http://proquest.umi.com/pqdlink?did=1023147851&Fmt=7&clientId=79356&RQT=309&VName=PQD.

Clifford, L. and Lynch, C. (2000). From automation to transformation: forty years of libraries and information technology in higher education. *Educause Review*. 35 (1):60 – 68. Retrieved November 14, 2007, from http://net.educause.edu/ir/library/pdf/erm0018.pdf.

Cline, N.M. (2000). Virtual Continuity: The Challenge for Research Libraries Today 22 *EDUCAUSE review*. p. 22-28. Retrieved May 9, 2007, from http://net.educause.edu/ir/library/pdf/ERM0031.pdf.

CLUSIF. (2008). *Information Systems Threats and Security Practices in France*. Retrieved January 17, 2009, from https://www.clusif.asso.fr/fr/production/sinistralite/docs/CLUSIF-rapport-2008-en.pdf.

Cohen, F. (1997). Information System Attacks: A Preliminary Classification Scheme. *Computers & Security*. 16(1): 29-46.

Common Criteria for Information Technology Security Evaluation (2006). *Part 1: Introduction and general model*. Retrieved May 9, 2007, from http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R1.pdf.

Computer security. (2010). In *Wikipedia, The Free Encyclopedia*. Retrieved August 16, 2010, from http://en.wikipedia.org/w/index.php?title=Computer_security&oldid=445075873

Conklin, W.A., White, G.B., Cothren, C., William, D. and Davis, R.L. (2005). *Principles of Computer Security: Security and Beyond.* Illinois: McGrawHill Technology Education.

CSI. (2002). Information Protection Assessment Kit (IPAK). *Computer Security Institute*. Retrieved June 23, 2008, from http;//www.gocsi.com/press/prelea991122.jhtml.

CyberSecurity Malaysia (2009). *Incident Statistics for 2008*. Retrieved January 2, 2010, from http://www.mycert.org.my/en/services/statistic/mycert/2008/main/detail/566/index.html

CyberSecurity Malaysia. (2010). Malaysia Vs Malware. *Futures Magazine*. 5(1). Retrieved November 12, 2010, from http://www.cybersecurity.my/en/knowledge_bank/news/2010/main/detail/1900/index.html.

D. Icove, K. Seger, and W. VonStorch. (1999). *Computer Crime: A Crimefighter's Handbook*. O'Reilly & Associates, Sebastopol, CA.

D'arcy, A. (2005). The development of linguistic constraints: Phonological innovations In St. John's English. *Language Variation and Change*. 17: 327-355.

Daniels, T., E., and Spafford, E. H. (1999). Identification of Host Audit to Detect Attacks on Low-level IP. *Journal of Computer Security*. 7(1): 3-35.

Data recovery. (2010). In *Wikipedia, The Free Encyclopedia*. Retrieved August 19, 2010, from http://en.wikipedia.org/w/index.php?title=Data_recovery&oldid=444815695.

Davamanirajan, P., Kauffman, R. J., Kriebel, C. H., and Mukhopadhyay, T. (2006). Systems Design, Process Performance, and Economic Outcomes in International Banking. *Journal of Management Information Systems.* 23(2), 65-90.

Davis, C.E. (1996). Perceived security threats to today's accounting information systems: a survey of CISAs. *IS Audit & Control Journal*. 3:38-41.

Deloitte Touche Tohmatsu. (2009). *Deloitte Global TMT Security Survey 2009*. Retrieved January 19, 2010, from http://www.deloitte.com/view/en_SK/sk/industries/tmt/9966d588572a2210VgnVCM100000ba42f00aRCRD.htm.

Delone, W. and Mclean, E.R. (1992). Information systems success: The quest for the dependent variables. *Information Systems Research*. 3:60-95.

Delone, W.H. (1988). Determinants of Success for Computer Usage in Small Business. *MIS Quarterly.* 12(1):51-61.

Denning, D. (2000). Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism. *U.S. House of Representatives, Comm. Armed Services*. Retrieved August 3, 2009, from http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html.

Dhillon, G. and Torkzadeh, G. (2006). Value Focused Assessment of Information System Security in Organizations. *Information Systems Journal*. 16(3): 293-314.

Dhillon, G. (2001). Challenges in Managing Information Security in the New Millennium, In, Dhillon, G. (2002). Information Security Management: Global Challenges in the New Millennium, Hershey, PA: Idea Group Publishing: pp. 1-8.

Digital Guards. (2005). Countermeasures. *Web Security Glossary*. Retrieved August 19, 2009, from http://www.digitalguards.com/glossary.php.

Dimopoulos, V., Furnell, S., Barlow, I. and Lines, B. (2004). Factors affecting the adopt Ion of IT risk analysis. In *Proceedings of 3rd European Conference on Information Warfare and Security, Royal Holloway, University of London, UK, 28-29 June 2004.*

Dionysiou, I. Kokkinaki, A. and Magirou, S. (2010). Preliminary Survey Results On IT Security Practices In Cyprus Private And Public Sectors. *MCIS 2010 Proceedings.* Paper 25. Retrieved December 12, 2010, from http://aisel.aisnet.org/mcis2010/25.

Dlamini, M.T., Eloff, J.H.P. and Eloff, M.M. (2009). Information security: The moving target. *Computers & Security*. 28(3-4):189-198.

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

Drevin, L., Kruger, H.A. and Steyn, T. (2007). Value- focused assessment of ICT security awareness in an academic environment. *Computers & Security.* 26(1):36-43.

EDUCAUSE/Internet2 Security Task. (2004). *The Information Security Governance (ISG) Assessment Tool for Higher Education*. Retrieved February 10, 2006 from http://net.educause.edu/ir/library/pdf/SEC0421.pdf.

Ein-Dor, P. and Segev, E. (1978). Organisational Context and the Success of Management Information Systems. *Management Science.* 24 (10):1067-1077.

Eisenberg, J. and Lawthers, C. (2005).Library computer and network security. *Infopeople.* Retrieved Feb 5, 2007, from http://www.infopeople.org/resources/security/.

Encyclopædia Britannica Online. (2009). *Information system*. Retrieved January 05, 2009, http://www.britannica.com/EBchecked/topic/287895/information-system.

Ernst and Young. (2008). *Moving beyond compliance: Ernst & Young's 2008 Global Information Security Survey*. Retrieved Jan 5, 2009, from http://www.ey.com/global/Content.nsf/International/Assurance_&_Advisory_-_Technology_and_Security_Risk_-_Global_Information_Security_Survey_2008.

Ernst and Young (2009). *Outpacing change Ernst & Young's 12th annual global information security survey.* Retrieved Oct 24, 2010. http://www.ey.com/Publication/vwLUAssets/12th_annual_GISS/$FILE/12th_annual_GISS.pdf.

Farahmand, F., Navathe, S. B., Sharp, G. P., and Enslow, P. H. (2003). Managing Vulnerabilities Of information systems to security incidents, *ACM ICEC 2003*, Pittsburgh.

Farahmand, F., Navathe, S.B., Sharp, G.P. and Enslow, P.H. (2005). Assessing Damages of Information Security Incidents and Selecting Control Measures, a Case Study Approach. *Workshop on the Economics of Information Security 2005*. Retrieved Nov 5, 2007, from http://infosecon.net/workshop/pdf/39.pdf.

Ferrer, D.F. and Mead, M. (2003). Uncovering the 'spy' network : is spyware watching your library computers?. *Computers in Libraries, 23*(5). 16-21.

Foo, S., Chaudhry, A. S., Majid, S. M. and Logan, E. (2002). Academic libraries in transition: challenges ahead. *Proceedings of the World Library Summit, Singapore, April 22-26.* Retrieved August 19, 2007, from http://islab.sas.ntu.edu.sg:8000/user/schubert/publications/2002/02wls_fmt.pdf.

Forcht, K.A. (1994). *Computer Security Management*, Boyd and Fraser: Danvers, MA.

Foster, C. D. (1996). A Wireless Future: College and University Libraries Unplugged. Broadening Our Horizons: Information, Services and Technology. In *Proceedings of the 1996 CAUSE Annual Conference. 1-11*. Retrieved August 19, 2007, from http://net.educause.edu/ir/library/pdf/CNC9640.pdf.

Fowler, F.J.(1984). *Survey Research Methods*. Beverly Hills, CA: Sage Publications.

Fox, E. and ElSherbiny, N. (2011). Security and digital libraries, digital libraries – methods and applications. In: Kuo Hung Huang (Ed.), InTech, Retrieved April 12, 2011 from http://www.intechopen.com/articles/show/title/security-and-digital-Libraries.

Frank, J., Shamir, B., and Briggs, W. (1991). Security-related behavior of PC users in organizations. *Information & Management*. 21(10):127-135.

Galliers, R.D. (1991). Choosing appropriate information systems research approaches: A revised taxonomy. In: Nissen, Hirschheim and Klein (1991). *The Information Systems Research Arena of the 90's,* North Holland, Amsterdam,. p. 168.

Gawde, V. (2004). Information Systems Misuse - Threats & Countermeasures. *Infosecwriters.* Retrieved January 11, 2008, from http://infosecwriters.com/text_resources/pdf/information_systems_misuse.pdf.

Georgia State University. (2003*). Georgia State University, University Computing and Communication Services. Security Assessment Questionnaire*, Version 1.1.3.

Goodhue, D.L. and Straub, D.W. (1991). Security Concerns of System Users: A Study of Perceptions of the Adequacy of Security. *Information and Management*. 20(1): 13-27.

Guel, M.D. (2007). *A Short Primer for Developing Security Policies.* Retrieved August 9, 2009, from http://www.sans.org/resources/policies/Policy_Primer.pdf.

Guimaraes, T. and Ramanujam, V. (1986). Personal Computing Trends and Problems: An Empirical Study. *MIS Quarterly.* 10(2):179-187.

Gupta, Y., Guimaraes, T. and Raghunathan, T.S. (1989). Personal Computing Problems and Some Organisational Factors: A Multivariate Analysis. *Computers and Operations Research*. 16(5):419-430.

Gupta, M. and Sharman, R. (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*. Retrieved November 15, 2007, from http://books.google.com.my/books?id=VyB_7hokxf4C&dq=Guttman,+B.+and+Roback+An+Introduction+to+Computer+Security&source=gbs_summary_s&cad=0

Hagen, J. M. (2008). *How do employees comply with security policy? A comparative case study of four organizations under the Norwegian Security Act.*

Hagen, J.M., Albrechtsen, E. and Hovden, J. (2008). Implementation and effectiveness of organisational information security measures. *Information Management & Computer Security.* 16(4):377-397. Retrieved February 1, 2009, from Emerald Database.

Haniza S. (2009). *Users' perception of the information security policy at Universiti Teknologi Malaysia.* Master's thesis, Universiti Teknologi Malaysia, Faculty of Computer Science and Information System.

Hermanson D.R, Hill, M.C. and Ivancevich, D.M. (2000). Information technology-related activities of internal auditor. *Journal of Information System*. 14(1): 39. Retrieved July 20, 2008, from Business Source Premier database.

Hight, S. D. (2005). *The Importance of a Security, Education, Training and Awareness Program.* Retrieved April 23, 2010, from Infosec Writers: http://www.infosecwriters.com/text_resources/pdf.

Hinson, G. (2003). Human factors in information security. *IsecT Ltd.* Retrieved August 19, 2008, from http://www.infosecwriters.com/text_resources/pdf/human_factors.pdf

Hoffer, J.A. and Straub, D.W. (1994). The 9 to 5 Underground: Are You Policing Computer Crimes?" in Gray, P., King, W.R., Mclean E.R. and Watson, H. (eds.) (1989). *Management of Information Systems,* Harcourt Brace: Fort Worth, TX, p. 388-401.

Hone, K. and Eloff, J.H.P. (2002) Information security policy – what do international security standards say? *Computers and Security*, .21(5): 402-409.

Hong Kong Special Administrative Region. (2008). An Overview Of Information Security Standards. Retrieved November 13, 2012, from http://www.infosec.gov.hk/english/technical/files/overview.pdf.

IBM. (2003). IBM Security Self-Assessment Survey. *IBM.* Retrieved August 19, 2008, from https://www-3.ibm.com/security/services/esurvey/.

Im, G. P. and Baskerville, R. L. (2005). A longitudinal study of information system threat categories: the enduring problem of human error. *SIGMIS Database*. 36(4): 68-79.

Information system. (2009). In *Encyclopædia Britannica*. Retrieved August 1, 2007, from http://www.britannica.com/EBchecked/topic/287895/information-system.

Information Technology Promotion Agency. (2008). *Information Security Management Benchmark (ISM-Benchmark)*. Retrieved August 16, 2008, from http://www.ipa.go.jp/security/english/benchmark/.../Howtouse_ISM_Benchmark.pdf.

INSUREtrust. (2000). Security Assessment Qustionnaire. *INSUREtrust.com*. Retrieved August 16, 2008, from http://www.insuretrust.com/pdfs/Security%20Questionnaire.pdf.

INTOSAI. (1995). *Information System Security Review Methodology: A Guide for Reviewing Information System Security in Government Organizations.* Retrieved February 3, 2008, from http://www.issai.org/media(421,1033)/ISSAI_5310_E.pdf.

IPTS Management Sector, Ministry of Higher Education Malaysia. (2010). *List of Private Universities in Malaysia.* Retrieved August 16, 2010, from http://www.mohe.gov.my/portal/institusi/ipts.html

ISAAlliance (2002). *Internet Security Alliance. Common Sense Guide For Senior Managers-Top Ten Recommended Information Security Practices*. 1st Edition.

ISACA (2009). *IS Auditing Guideline: G40 Review of Security Management Practices*. Retrieved December 23, 2009, from http://www.isaca.org/Knowledge-Center/Standards/Pages/IS-Auditing-Guideline-G40-Review-of-Security-Management-Practices1.aspx.

Ismail A.and Maznan D. (2005). Information Technology Security In Malaysia: A Study Of Problems, Control Measures And Challenges. Retrieved November 25, 2007, from www.ftsm.ukm.my/programming/prosiding05/26-Ismail.xml.

James, H.L. (1996). Managing information systems security: a soft approach. *Information Systems Conference of New Zealand (ISCNZ '96),* p.10.

J.H. Schuessler. (2009). General deterrence theory: Assessing information systems security effectiveness in large versus small businesses. *University of North Texas.* Retrieved March 29, 2010, from http://joseph.schuesslersounds.com/Research/Dissertation/Schuessler_Dissertation.pdf.

Jarvenpaa, S.L. and Ives, B. (1990). Information Technology and Corporate Strategy: A View from the Top. *Information Systems Research*. 1(4): 351-375.

Jung, B., Han, I., and Lee, S. (2001). Security Threats to Internet: A Korean Multi-Industry Investigation. *Information &Management*. 38: 487-498. Retrieved August 16, 2008, from ScienceDirect.

Kahan, S. (2004). Information Security: On the Cusp of a Management Evolution. *Management of Information Security*. Canada: Thomson Course Technology:18-19.

Kankanhalli, A., Teo, H.-H, Tan B.C.Y. and Wei, K.-K.(2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*. 23:139-54. Retrieved December 1, 2008, from www.comp.nus.edu.sg/~atreyi/papers/sec-eff.pdf.

Ke, X.R. (1997). *Gist of Banking Law*. Banchiau City, Taipei. Publisher of LiJian, Taiwan.

Kerlinger, F.N. (1986). *Foundations of behavioral research Foundations of behavioral research* (3rd ed.). Fort Worth: Holt Rinehart and Winston.

Kim, E.B. and Kbzullak, M. (2008). Does Enterprise Size Matter in Achieving Information Security?. *Review of Business Research.* 8(6): 41-49. Retrieved August 16, 2008, from http://www.mendeley.com/research/enterprise-size-matter-achieving-information-security/#.

Kim, J. (1992). *An Empirical Investigation Of Factors Influencing The Effectiveness Of Information Systems Security*. Mississippi State University. DBA. 138p.

Kimwele, M., Mwangi, W., and Kimani, S. (2005). Adoption of information technology security policies: Case study of Kenyan small and medium enterprises (SMES). *Journal of Theoretical and Applied Information Technology*. 18(2): 1-11. Retrieved September 15, 2008, from http://www.jatit.org/volumes/research-papers/vol18no2/1vol18no2.pdf.

King, W.R. (1994). Organisational Characteristics and Information Systems Planning: An Empirical Study. *Information Systems Research.* 5(2): 75-109.

Klete, H. (1978). Some Minimum Requirements for Legal Sanctioning Systems Special Emphasis on Detection. in Blumstein, A., Cohen, J. and Nagin, D. (eds.). (1978) *Deterrence and Incapacitation: Estimating the Effects of Criminal Sanctions on Crime Rates,* National Academy of Sciences: Washington, DC. p.95-139.

Knapp, K. J., Marshall, T. E., Rainer, R. K, and Ford, F. N. (2005). *Managerial Dimensions in Information Security: A Theoretical Model of Organisational Effectiveness.* Retrieved Jan 16, 2009 from https://www.isc2.org/download/auburn_study2005.pdf.

Kochtanek, T.R. and Matthews, J.R. (2002). *Library Information Systems: From Library Automation to Distributed Information Access Solutions. Englewood, CO:* Libraries Unlimited.

Kongsved, S.M., Basnov, M, Holm-Christensen, K. and Hjollund, N.H. (2007). Response Rate and Completeness of Questionnaires: A Randomized Study of Internet Versus Paper-and-Pencil Versions. *Journal of Medical Internet Research*. Retrieved September 10, 2008, from http://www.jmir.org/2007/3/e25/.

KPMG. (2004). *Fraud Survey 2004 Report*. Retrieved Nov 25, 2007, from www.kpmg.com.my/kpmg/publications/fas/fsurvey_2004.pdf.

Kruger, H., Drevin, L., and Steyn, T. (2007). Email Security Awareness: A Practical Assessment of Employee Behaviour. In the Fifth World Conference on Information Security Education. 237:33-40. Publisher: Springer Boston.

Kwok, L.F. (1997). Hypertext information security model for organizations. *Information Management & Computer Security*. 5(4):138-148.

Kwok, L.F. and Longley, D. (1996). A Security Officier's Workbench. *Computer and Security*. 15(8):695-705.

Kwok, Lam-for (1997). Hypertext information security model for organizations. *Information Management and Computer Security*. 5(4):138 – 148.

Hong, K.S., Chi, Y.P, Chao, L.R., and Tang, J.H. (2006) .An empirical study of information security policy on information security elevation in Taiwan. *Information Management & Computer Security*. 14(2):104 – 115.

Laprie, J.C. ed. (1992). Dependability: Basic Concepts and Terminology. Springer-Verlag, Vienna.

Lee, K. H. and Teh, K. H. (2000). Evaluation of academic library web sites in Malaysia. *Malaysian Journal of Library and Information Science.* 5(2):95-108.

Lin, T.Y. (1992). Bell-LaPadula Axioms: a 'new' paradigm for an 'old' model. *ACM SIGSAC New Security Paradigms Workshop*.p. 82-93.

Lin, Y.C., and Huang, M.X. (1999). Technology of Internet system security. *Communication of Information Security* (15:3): 12–22.

Lindstrom, P. (2003). Let's Get Physical: The Emergence Of The Physical Threat. *A Spire Research Report*. Retrieved September 25, 2008, http://www.netbotz.com/library/Physical_Threat_Security.pdf.

Loch, K.D., Carr, H.H. and Warkentin, M.E., (1992). Threats to information systems: today's reality, yesterday's understanding. *MIS Quarterly*. 16 (2): 173-186.

Loch, Karen D. and Carr, Houston H. (1991). Threats To Information System Security: An Organisational Perspective. *Proceedings of the Twenty-Fourth Annual Hawaii International Conference on System Sciences, 1991. 4: 551 – 557.* Retrieved November 26, 2008, from IEEE Database.

Loch, Karen D., Carr, Houston H and Warkentin, M. (1992). Threats to Information Systems: Today's Reality, Yesterday's Understanding. *MIS Quarterly*. 16(2): 173-186.

Loukis, E and Spinellis, D. (2001). Information Systems Security in the Greek Public Sector. *Management and Computer Security*, 9(1):21–31. Retrieved November 25, 2007, from Emerald Database.

Lowes, R. (2010). Privacy Lapses Underscore Need to Keep Patient Data Off Portable Devices and Desktops. *Medscape Medical News.* Retrieved October 22, 2010, from http://www.medscape.com/viewarticle/721284.

M.T. Dlamini, J.H.P. Eloff, and M.M. Eloff. (2009). Information security: The moving Target. *Computers & Security*, p.189-198. Retrieved March 15, 2019, from Science Direct.

Ma, Q. and Pearson, J. M. (2005). ISO 17799: "Best practices" in information security management. *Communications of the Association for the Information Systems*. 15(32). Retrieved September 15, 2008, http://aisel.aisnet.org/cais/vol15/iss1/32.

Madnick, S.E. (1978). Management Policies and Procedures Needed for Effective Computer Security. *Slogan Management Review*. 19(3):61-73.

Maiwald, E. (2004). Fundamentals of network security. NY: McGraw Hill.

Malmgreen, C., Graham, P., Shortridge-Bagget, L. M., Courtney, M. D., and Walsh, A. M. (2009). Establishing content validity of a survey research instrument: the older patients in acute care survey -United States. Journal for Nurses in Staff Development, 25(6):E14-E18.

Matthews, G. and Feather, J. (eds.) (2003). *Disaster management for libraries and archives*. Aldershot: Ashgate.

May, L. and Lane, T. (2006). A Model for Improving e-Security in Australian Universities. *Journal of Theoretical Applied Electronic Commerce Research*. 1(2):90-96. Retrieved January 16, 2007 from www.jtaer.com.

McAuliffe, M. (2000). Hacker hits Australian National Library Intranet. *ZD Net Asia: Where Technology Means Business.* Retrieved August 26, 2007, from http://www.zdnetasia.com/news/security/0,39044215,21153000,00.htm.

Mell, P., Kent, K., and Nusbaum, J. (2005). Guide to Malware Incident Prevention and Handling. *National Institute of Standards and Technology, Special Publication 800-83, Gaithersburg, MD, U.S. Dept. of Commerce, Technology Administration, National Institute of Standards and Technology, November.* Retrieved September 15, 2008, http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf.

Mercuri, R.T. (2004). Superscaled security. *Communications of the ACM.* .47(3). [doi>10.1145/971617.971631].

Merkow, M. and Breithaupt, J. (2005). *Principles of Information Security: Principles and Practices.* Pearson Prentice Hall: Upper Saddle River, New Jersey.

MHCC. (2002). HIPPA Security Assessment Guide. *Maryland Health Care Commission*. Retrieved September 1, 2008, from http://www.hipaadvisory.com/action/security/MDMHCCsecurityassessment02.pdf.

Microsoft Whitepaper on Security (2000). Security Threat Classification. Retrieved September 1, 2008, from http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/itsolutions/security/bestprac/secthret.asp.

Ministry of Higher Education Malaysia. (2009). *List of Public Universities in Malaysia*. Retrieved December 5, 2009, http://www.mohe.gov.my/portal/institusi/ipta.html.

Mohammed Imtiaz, A. (2001) . *A New Theory Of Management Information Security Systems In Libraries*. Retrieved September 12, 2011, from http://dspace.jgu.edu.in:8080/dspace/handle/10739/156

MOSTI. (2007). IT Governance and the Public Sector. *IT Governance 2007, 22 – 23 May 2007 Sheraton Subang.* Retrieved January 5, 2009, from www.isaca.org.my/doc/itgc07/day1-1.pdf.

Nachtigal, S. (2009). E-business Information Systems Security Design Paradigm and Model. Retrieved September 5, 2008, from http://www.ma.rhul.ac.uk/static/techrep/2009/RHUL-MA-2009-16.pdf.

National Information Systems Security (INFOSEC). (1992). *Information Systems Security Glossary , NSTISSI No. 4009.* Retrieved May 15, 2007 from http://www.its.bldrdoc.gov/fs-1037/dir-019/_2730.htm.

National Institute of Standards and Technology (NIST). (2000). Federal Information Technology Security Assessment Framework. *National Institute of Standards and Technology. Computer Security Division, Systems and Network Security Group*. Retrieved January 15, 2009 from http://www.cio.gov/archive/federal_it_security_assessment_framework.html.

National Institute of Standards and Technology (NIST) (2002). International Standard ISO/IEC 17799:2000 Code of Practice for Information Security Management, Frequently Asked Questions. *National Institute of Standards and Technology (NIST), Computer Security Division, Systems and Network Security Group*. Retrieved January 15, 2009 from http://csrc.nist.gov/publications/secpubs/otherpubs/reviso-faq.pdf.

National Library of Malaysia. (2008). *Database Directory of Libraries in Malaysia*. Retrieved February15, 2008 from http://www.pnm.gov.my/index.php?id=924.

National Security Telecommunications and Information Systems Security Committee (NSTISSC). (2000). Threat. National Information Systems Security (Infosec) Glossary. Retrieved January 15, 2009 from http://security.isu.edu/pdf/4009.pdf.

National Security Telecommunications and Information Systems Security Committee (NSTISSC). (2000). Vulnerability. National Information Systems Security (Infosec) Glossary. Retrieved January 15, 2009 from http://security.isu.edu/pdf/4009.pdf.

Newby, G. B. (2002). Information Security for Libraries. Retrieved April 5 2007, from http://www.petascale.org/papers/library-security.pdf.

Neumann, P.G. (2005). Computer related risks, ACM Press/Addison-Wesley Publishing Co., New York, NY, 1995 in IM, G.P. and Baskerville, R.L. (2005). A Longitudinal Study of Information Systems Threat Categories: The Enduring Problem of Human Error. *The Database Advances in Information Systems.* 36(4).

NICDER (2003) Malaysia ISMS Survey. Retrieved April 15, 2007 from www.cybersecurity.org.my/data/content_files/19/124.pdf?.diff=1177114006.

Nielsen, E.K. (2002). Library Security Management: the Responsibility of the Chief Executive. *Liber Quarterly*. 12: 296-302.

NIST IR 7298 (2006). Security control. Kissel, R. (ed.). *Glossary of Key Information Security Terms. U.S. Department of Commerce.* Retrieved January 15, 2009 from http://csrc.nist.gov/publications/nistir/NISTIR7298_Glossary_Key_Infor_Security_Terms.pdf.

NIST IR 7298 (2006). Threat Agent/Source. Kissel, R. (ed.). *Glossary of Key Information Security Terms.* U.S. Department of Commerce. Retrieved January 15, 2009 from http://csrc.nist.gov/publications/nistir/NISTIR7298_Glossary_Key_Infor_Security_Terms.p df.

Nunnally, J.C. (1978). Psychometric theory (2nd ed.). New York: McGraw Hill.

Oder, N. (2004). Fallout from Philadelphia attack: More security. *Library Journal 129 (*9):16.

Ohaya. C. (2006). Managing phishing threats in an organization. In *Proceedings of the 3rd annual conference on Information security curriculum development* (InfoSecCD '06). ACM, New York, NY, USA, 159-161. DOI=10.1145/1231047.1231083. Retrieved May 9, 2007, from http://doi.acm.org/10.1145/1231047.1231083.

Olayemi, O.A., 2005. University of East London School of Computing and Technology, System Integration, CNM009. Retrieved January 15, 2009 from http://homepages.uel.ac.uk/u0430614/classification_of_security_threa.htm.

Olnes, J. (1994). Development of Security Policies. *Computers and Security*. 13(8):628-636.

Orme, B. (2004). Work anywhere, anytime, securely. *Infosecurity Today*, 1(1):44-45.

Ormes, S. (2001). An Introduction to Filtering EARL: The Consortium for Public Library Networking. Retrieved January 12, 2008 from http://www.ukoln.ac.uk/public/earl/issuepapers/filtering.html.

Ortiz-Caceres, G. L. (2006). Information Security – Whose Responsibility Is It? Retrieved January 15, 2009 from Http://www.Infosecwriters.Com/Text_Resources/Pdf/Gocaceres_Responsibility.Pdf.

Ozkan, S. and Karabacak, B. (2010). Collaborative risk method for information security management practices: A case context within Turkey. International Journal of Information Management , 30 (6), 567-572. Parker, D.B. (1981). *Computer Security Management*, Reston Publishing: Reston, VA.

Pearson, I. (2001). What's next?. Retrieved January 15, 2009 from www.futurizon.com/future/whatsnext.rtf.

Pethia, R. D. (2003). Viruses and Worms: What Can We Do About Them?. *InfoSec News*. Retrieved January 15, 2009 from http://seclists.org/isn/2003/Sep/89.

Pfleeger, C.P. and Pfleeger, S.L. (2003). *Security in Computing*. 3rd. ed. New Jersey: Prentice Hall Professional Technical Reference.

Phelps, D. C. (2005). *Information Systems Security: Self-Efficacy and Security Effectiveness in Florida Libraries* (Dissertation): Florida State University. 112 p. AAT 3183102. Retrieved February15, 2009 from http://proquest.umi.com/pqdlink?did=953999691&Fmt=7&clientId=79356&RQT=309&VName=PQD.

Pinsonneault. A and Kraemer, K.L. (1993). *Survey Research Methodology in Management Information Systems: An Assessment.* Retrieved 25 July 2007 from Available at: http://www.crito.uci.edu/research-archives/pdf/urb-022.pdf.

Pipkin, D. L. (2000). *Information Security: Protecting the Global Enterprise*. Prentice Hall PTR: Upper Saddle River, New Jersey.

Post, G.V. and Kagan, A. (2007). Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computers and Security*. 26: 229-237. Retrieved January 10, 2009, from ScienceDirect Database.

Post, G.V. and Kievit, Karen-Ann. (1991). Accessibility vs Security: A Look at the Demand for Computer Security. *Computer and Security*. 10(4):331-344.

Post, G.V. and Kievit, Karenn-Ann. (1991). Accessibility vs. security: A look at the demand for computer security. *Computers and Security*. 10(4): 331-344.

Prince, K. (2008). Top 9 Network Security Threats in 2009. *The International Data Group Network.* Retrieved January 2, 2009 from http://www.cgisecurity.net/2008/12/top-9-network-security-threats-in-2009.html.

Qayoumi, M.H. and Woody, C. (2005). Addressing Information Security Risk. *Educause Quarterly*. 28(4). Retrieved February 25, 2009 from http://www.educause.edu/EDUCAUSE+Quarterly/EDUCAUSEQuarterlyMagazineVolum/Ad_dressingInformationSecurityR/157366.

Rajendran, L. and G. Rathinasabapathy (2007). Role of Electronic Surveillance and Security Systems in Academic Libraries. In: *Proceedings of the Conference on Recent Advances in Information Science and Technology (READIT 2007), MALA & IGCAR, Kalpakkam. pp. 111-117.* Retrieved February 11, 2008 from http://library.igcar.gov.in/readit2007/conpro/s4/S4_2.pdf.

Raymond, L. (1990). Organisational Context and Information Systems Success: A Contingency Approach. *Journal of Management Information Systems.* 6(4): 5-20.

Reich, B.H. and Benbasat, I. (1990). An Empirical Investigation of Factors Influencing the Success of Customer Oriented Strategic Systems. *Information Systems Research.* 1(3):325-347.

Reitz, J. M. (2007). Information systems. *ODLIS — Online Dictionary for Library and Information Science.* Retrieved March 25, 2008, from http://lu.com/odlis/search.cfm.

Richards, T. C. (1986). A Historical Perspective of Computer Related Fraud. *SIGSAC Review*. 4(3):15-25.

Ross, R., Katzke, S., Johnson, A., Swanson, M., Stoneburner, G., Rogers, G., and Lee, A. (2007). Recommended Security Controls for Federal Information Systems. NIST Special Publication 800-53, Revision 2. *National Institute of Standards and Technology*. Gaithersburg, Maryland: U.S. Department of Commerce. Retrieved November 25, 2007, from http://www.csrc.nist.gov/publications/nistpubs/800-53.../sp800-53-rev3-final.pdf.

Rossman, G.B. and Wilson, B.L. (1985). Numbers and words: Combining quantitative and qualitative methods in a single large-scale evaluation study. *Evaluation Review*. 8(5): 627-643.

Ryan, S.D. and Bordoloi, B. (1997). Evaluating security threats in mainframe and client/server environments. *Information and Management*. 32(3):137-42.

Ryoo, J., Girard, T., and McConn, C. (2009). An Information Systems Security Readiness Assessment for Municipalities in Rural Pennsylvania. *The Center for Rural Pennsylvania*. p. 1-20. Retrieved March 25, 2001, from www.rural.palegislature.us/Info_Systems_Security09.pdf.

Samy, G.N., Rabiah, A. and Zuraini, I. (2009). Security threats in healthcare information systems: A preliminary study. In: *Fifth International Conference* on Information Assurance and Security. IEEE Computer Society. 18 20 August, 20 09, Xian, China.

Sandhu, R.S. (1993). Lattice-based access control models. *IEEE Computers.* 26(11):9-19.

Saunders, J. H. (2001). A Risk Management Methodology for Information Security: The Analytic Hierarchy Process (AHP). *SANS Institute*.

Scarfone, K., Grance, T., and Masone, K. (2008). *Computer Security Incident Handling Guide, NIST Special Publication 800-61*, Revision 1, March 2008, Gaithersburg, MD. Retrieved May 20, 2009, from http://www.csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf.

Schwartz, M. (2006). *Employees Cause Most Security Breaches, Yet Response Lags.* Retrieved October 19, 2009 from http://www.esj.com/security/article.aspx?EditorialsID=1769.

Seliem, A. A.M., Ashour, A.S., Khalil, O.E.M. and Millar, S.J. (2003). The Relationship of Some Organisational Factors to Information Systems Effectiveness: A Contingency Analysis of Egyptian Data. *Journal of Global Information Management.* 1(1): 40-71.

Shahid, S.M. (2005). Use of RFID technology in libraries: A new approach to circulation, tracking, inventorying, and security of library materials. *Library Philosophy and Practice*. 8 (1). Retrieved March 25, 2008, from http://unllib.unl.edu/LPP/shahid.htm.

Shelly, G. B., Cashman, T. J., and Rosenblatt, H. J. (2006). *Systems analysis and design*. 6th ed. Boston, MA.

Shelly, G.B., Cashman, T.J., and Rosenblatt, H.J. (1998). *Systems Analysis and Design*. Course Technology, Cambridge.

Shen, W.Z. (1999). Attack and protection with Hacker. *Communication of Information Security*. 5(3):86–96.

Siponen, M.T. (2001). An analysis of the recent IS security development approaches: descriptive and prescriptive implications. In G. Dhillon (eds:) *Information Security Management - Global Challenges in the Next Millennium.* Idea Group Publications, Hershey, PA, USA, p. 101-124.

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*. 38(1): 60-81.

Slade, R. (2006). *Dictionary of information security*. Rockland, MA: Syngress.

Smith, S. and Jamieson, R. (2006). Determining key factors in e-government information system security. *Information Systems Management*. 23(2):23–32.

Smith-Thomas, B. and Wand, C.Y. (1995). Implementing Role Based. Clark-Wilson Enforcement Rules in a B1 Outline Transaction Processing System. *Computers and Security.* 14(1):29.

Solomon, M. G. and Chapple, M. (2005). *Information Security Illuminated*. Jones and Bartlett. 228. Jones and Bartlett Publishers.

Stoneburner, G., Goguen, A., Feringa, A. (2002), Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology (NIST), United States Department of Commerce, Washington, DC. Retrieved May 5, 2008 from http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

Straub, D., Boudreau, M.-C., and Gefen, D. (2004). Validation Guidelines for IS Positivist Research. *Communications of AIS*. 13(24):380-427.

Straub, D.W. (1986). Computer Abuse and Computer Security: Update on an Empirical Study. *Security, Audit, and Control Review* 4(2): 21-31.

Straub, D.W. (1990). Effective IS Security: An Empirical Study. *Information Systems Research.* 1(3): 255-276. Retrieved July 15, 2008 from www.cis.gsu.edu/~dstraub/Papers/Resume/Straub1990.pdf.

Straub, D.W. and Welke, R.J. (1998). Coping with Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly.* 22(4):441-469.

Suhazimah, D. (2007). *The antecedents of information security maturity in Malaysian public service organizations*. Ph.D. thesis. (Faculty Business and Administration, University of Malaya, Malaysia).

Sundt, C. (2006). *Information security and the law, Information Security Technical Report*. 11(1): 2-9.

Swanson, M. (2001). *NIST Special Publication 800-26. Security Self-Assessment Guide for Information Technology Systems*. Retrieved December March 25, 2007, from http://csrc.nist.gov/publications/nistpubs/800-26.pdf.

Syed Sajjad, A. (2002). Managing change to enhance Web-based services in the Arabian Gulf libraries. *Online Information Review*. 26(4):265 – 270.

Tarimo, C. N., Bakari, J. K., C. Yngström, L., and Kowalski, S. (2006). A Social-Technical View of ICT Security Issues, Trends, and Challenges: Towards A Culture of ICT Security – The Case of Tanzania. *Proceedings of Information Security South Africa (ISSA), from insight to foresight Conference,* eds. Venter, H. S., Eloff, JHP., Labuschagne, L, Eloff, MM, Sandton, Johannesburg, South Africa, July 05-07, 2006.

Telekom Malaysia Berhad (2011) TM Annoucement: Internet Services Distruption. Retrieved March 31, 2011, from http://www.tm.com.my/about-tm/media-centre/announcements/Pages/INTERNETSERVICESDISRUPTIONEARTHQUAKEJAPAN11MAR11.aspx.

Thiagarajan, V. (2003). Information Security Management BS 7799.2:2002 Audit Check List for SANS. Retrieved March 25, 2008, from www.sans.org/score/checklists/ISO_17799_checklist.pdf.

Thompson, S. T. C. (2006). Helping the hacker? Library information, security, and social engineering. *Information Technology and Libraries*. 25(4):222-225. Retrieved May 5, 2009, from http://www.ala.org/ala/mgrps/divs/lita/publications/ital/252006/number4decembera/thompson.pdf.

Thong, J.Y.L., Yap, C.S. and Raman, K.S. (1996). Top Management Support, External Expertise and Information Systems Implementation in Small Businesses. *Information Systems Research.* 7(2): 248-267.

Tipton, H. F. and Krause, M. (1997). Deterrent controls. *Handbook of Information Security Management.* Retrieved January 15, 2009 from http://books.google.com.my/books?id=MhaqJNSNHGAC&dq=Tipton,+H.+F+Handbook+of+Information+Security+Management.&source=gbs_summary_s&cad=0.

Tittel, E., Chapple, M., and Stewart, J. M. (2003). *CISSP: Certified Information Systems Security Professional study guide.* 3rd. ed. Sybex: Wiley Publishing.

Tong, C.K.S., Fung, K.H., Huang, H.Y.H., and Chan, K.K. (2003). *Implementation of ISO17799 and BS7799 in picture archiving and communication system: local experience in implementation of BS7799 standard.* International Congress Series. 1256(June):311-318.

Trend Micro White Paper. (2009). *Ghosts in the Machine: Today's Invisible Threats*. Retrieved March 25, 2008, from http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/wp03_ghosts_090930us__2_.pdf.

Unisys. (2007). *Unisys Security Index Malaysia: A Synovate Survey.* Retrieved April 2, 2008, from http://www.unisys.com.sg/eprise/main/admin/country/doc/sg/MY_Security_Index_May_FINAL.pdf.

United States Code. (2008). Information Security 44 U.S.C. § 3542. Retrieved November 15, 2009 from http://www.law.cornell.edu/uscode/44/3542.html.

Vaast, E., Boland, R., Davidson E., Pawlowski, S. and Schultze, U. (2006). Investigating the "Knowledge" in Knowledge Management: A Social Representation Perspective. *Communications of the Association for the Information Systems.* 17:314-340.

Vaast, E. (2007). Danger is in the Eye of the Beholders: Social Representations of Information Systems Security in Healthcare. *Journal of Strategic Information Systems*. 16(2):130-152.

Vaus, D. A. (2004). *Analysing Social Science Data: 50 problems in data analysis.* London:Sage Publication.

Vacca, J.R. (2009). *Computer and information security handbook*. Burlington: Morgan Kaufmann Publication. p.632.

Volonino, L. and Robinson, S. R. (2004). Principles and Practice of Information Security: Protecting Computers from Hackers and Lawyers. Pearson Education: Upper Saddle River, p.1.

Von Solms, B. (2000). Information security- the third wave?. *Computers and Security*. 19 615-620. Retrieved November 12, 2008 from http://www.tut.fi/units/tuta/tita/2006-2007/TITA-5300/the_third_wave.pdf.

Waldhart, N.A. (1990). The army secure operating system. *Proceedings of 1990 IEEE Symposium on Research in Security and Privacy.* p.50-60.

Warren, M.J. (2002). Security practice: survey evidence from three countries. *Logistics Information Management*. 15(5/6):347 – 351.

Weber, R. (1988). *EDP Auditing: Conceptual Foundations and Practice*, McGraw Hill: New York, NY.

Weise, J.and Martin, C.R. (2001). Developing a Security Policy. *Sun Blue Prints Online.* Retrieved November 10, 2009 from http://www.sun.com/blueprints/1201/secpolicy.pdf.

Werlinger, R., Hawkey, K., and Beznosov, K. (2009). An Integrated View of Human, Organisational, and Technological Challenges of IT Security Management. *Journal of Information Management & Computer Security.* 17(1):4-19.

Westby, J.R. and Allen, J.H. (2007). *Governing for Enterprise Security (GES) Impmplementaon Guide (CMU/SEI-2007-TN-020)*. Pittsburgh, PA., Software Engineering Institute, Carnegie Mellon University. Retrieved March 15, 2009 from http://www.cert.org/archive/pdf/07tn020.pdf.

White, G.W. and Pearson, S.J. (2001). Controlling corporate e-mail, PC use and computer security. *Information Management and Computer Security*. 9(2):88 – 92.

Whitman, M.E. (2003). Enemy at the gates: threats to information security. *Communication of the ACM*. 46 (8):91–95.

Whitman, M.E. and Mattord, H.J. (2009). *Principles of Information Security*. 3rd edition. Cengage Learning, Inc International. p. 81.

Williams, R. L. (2001). Computer and network security in small libraries: A guide for planning. *Texas State Library & Archives Commission*. Retrieved April 5 2008, from http://www.tsl.state.tx.us/ld/pubs/compsecurity/.

Wold, G. and Shriver, R.F. (1997). Risk Analysis Techniques: The risk analysis process provides the foundation for the entire recovery planning effort. *Disaster Recovery Journal*. Retrieved November 15, 2009 from http://www.drj.com/new2dr/w3_030.htm.

Yang, C. (2002) Security breach. *Actel Security Glossary*. Retrieved June 15, 2008 from http://www.pldworld.com/_actel/html/ref/glossary-security-body.htm.

Yap, C.S., Soh, C.P.P. and Raman, K.S. (1992). Information System Success Factors in Small Business. *Omega.* 20(5):597-609.

Yasin, R. (2002). What is Identity Management?, *Information Security Magazine.* Retrieved July 12, 2007 http://www.infosecuritymag.com/2002/apr/cover_casestudy.shtml.

Yeh, Q. and Chang, A.J. (2007). Threats and countermeasures for information system security: A cross-industry study. *Information & Management.* 44:480-491. Retrieved July 15, 2008 from ScienceDirect Database.

Yong, F. (2008). Managing security and productivity challenges within libraries. In: *International Conference On Libraries (ICOL) : Emerging Trends*, 31 October – 2 November 2007, Universiti Sains Malaysia, Pulau Pinang. (Unpublished). Retrieved January 10, 2009 from http://eprints.ukm.my/136/1/Managing_Security_And_Productivity_Within_Library.pdf

Zimerman, M. (2010). Protect your library's computers. *New Library World*. 111(5/6), 203-212..

Zoughbi, S. (2009). Implementation of Sound Security Practices -Regional Analysis. *UN-ESCWA.* Retrieved June 15, 2010 from http://css.escwa.org.lb/ictd/850/SZoughbi_Sound_Security_Practices.pdf.

Zviran, M. and Chanan, G. (2000). Towards generating a data integrity standard. *Data & Knowledge Engineering.* 32(3):291-313.

Appendices

Appendix A: Sample Questionnaire

Appendix B: List of Publications

Ref. #/QIS/56

Questionnaire on Information Security Management in Malaysian Academic Libraries

January 4, 2010

Dear Respondent,

I am a PhD candidate at the Faculty of Computer Science and Information Technology, University of Malaya. Currently, I am conducting a study on information security management in Malaysian academic libraries. Through your participation, I eventually hope to understand the most common information security incidents experienced by Malaysian academic libraries as well as the types and extent of security measures undertaken by these libraries to protect their information systems (IS).
Enclosed with this letter is a set of questionnaire (Part A, B & C) that asks a variety of questions about your library, your library IS security threats and your library IS security measures implementation.
I hope you will contribute your time to complete this questionnaire and return it to me in the enclosed postage-paid envelope, preferably within two weeks. The information collected in this survey will be used for research purposes only and I assure you that your responses are completely anonymous.

Any questions or concerns about completing the questionnaire can be directed to me at 4uroesnita@gmail.com.

Your cooperation is greatly appreciated.

Sincerely,

Roesnita

Roesnita Ismail
PhD candidate
Faculty of Computer Science and Information Technology
University of Malaya, Kuala Lumpur.

Encl.

	Additional Information:
A)	**Targeted respondent to answer this questionnaire**
	An individual who is responsible for the library information systems (IS) and/or Information Technology (IT) in your library such as follows: - *Head of IT/Systems Department, or* - *IT/Systems Manager, or* - *IT/ Librarian/Systems librarian, or* - *IT//Systems Executive, or* - *IT//Systems Officer, or* - *Individual who is responsible for the IT and systems in your library.*
B)	**Definitions of key terminologies**
	▪ **Information Systems:** 'It refers to the entire infrastructure, organisation, personnel and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information'. ▪ **Information Systems (IS) Security:** 'The protection of information systems against unauthorised access to or modification of information, whether in storage, processing, or transit, and against the denial-of service to authorised users or the provision of service to unauthorised users, including those measures necessary to detect, document and counter such threats'. ▪ **Threat:** It represents any type of action, circumstance or event that may have some negative impact to information systems (IS). ▪ **Countermeasure:** Include all devices, techniques, policies, procedures, actions or processes implemented to prevent the information systems (IS) threats. ▪ **Oganisational security measures:** 'Include the security policy; procedures and control; non-technological tools and methods; and creation and maintenance of security awareness to guard the library information systems integrity, confidentiality, and availability'. ▪ **Technological security measures:** 'Include the technical mechanisms that are put in place to protect, control and monitor information access, or prevent unauthorised access to data that is transmitted over a library systems'.

Part A: Questions about your library and yourself.
Please tick **(√)** whichever appropriate

1) Please indicate your library ownership:
   [ ] Government
   [ ] Public
   [ ] Private
   [ ] Non-profit

2) Total numbers of staff in your library:
   [ ] Less than 10
   [ ] Between 10 and 50
   [ ] Between 51 and 100
   [ ] Between 101 and 190
   [ ] More than 191

3) Numbers of PC/work station with Internet connection for staff in your library:
   [ ] Less than 10
   [ ] Between 10 and 50
   [ ] Between 51 and 100
   [ ] Between 101 and 190
   [ ] More than 191

4) Estimate numbers of total library patrons:
   [ ] Less than 500
   [ ] Between 500 and 1000
   [ ] Between 1001 and 5000
   [ ] More than 5 000

5) Numbers of PC/work station with Internet connection for patrons in your library:
   [ ] Less than 100
   [ ] Between 101 and 200
   [ ] Between 201 and 300
   [ ] More than 300

6) Does your library have a wireless connection to the Internet?
   [ ] Yes
   [ ] No
   [ ] Currently piloting
   [ ] Do not know

7) Operating system used in your library.
   You may tick (√) more than one answers whichever appropriate.
   [ ] Windows
   [ ] Linux
   [ ] Unix Variants
   [ ] Novell
   [ ] Mac OS X
   [ ] Other: Please specify:
   _____

8) Please indicate information systems used in your library. You may tick (√) more than one answers whichever appropriate.
   [ ] E- books and E-journals
   [ ] Integrated Library systems (ILS)
   [ ] Online databases
   [ ] Web-based resources
   [ ] Other: Please specify:
   _____

9) Percentage of information systems security budget from the library general budget.
   [ ] Less than 1%
   [ ] Between 1% to 3%
   [ ] Between 4% to 5%
   [ ] More than 5%

9) Does your library have dedicated staff assigned for IS security related job?

   [ ] Yes
   [ ] No
   [ ] Not sure

11) How long has your library been involved in the ICT or computerization implementation?
   [ ] Less than 5 years
   [ ] 5 years to 10 years
   [ ] 10 years to 15 years
   [ ] 15 years to 19 years
   [ ] More than 19 years

12) Which statement best describes the role of information systems in your library?
[ ] Information systems are critical to our library.
[ ] Information systems serve an important role, but are not critical to our library.
[ ] Information systems are helpful, but do not serve an important role in our library.
[ ] Information systems are not important to our library.
[ ] Not sure

13) Your highest academic qualification:
[ ] Master.
(Please specify: ……....)
[ ] Bachelor
(Please specify:……..)
[ ] Diploma
(Please specify:……..)
[ ] Other:
(Please specify:……..)

14) Please indicate your current designated post in your library:

……
……

15) Are you responsible for information security and information systems (IS) security in your library?
[ ] Yes
[ ] No
(If No, please specify who is responsible for information security and information systems (IS) security in your library:
……
……
…….....

16) How many information security seminar, conferences or knowledge sharing sessions have you attended in the past 24 months?
[ ] None
[ ] 1
[ ] 2
[ ] 3
[ ] 4 or more

PART B: The following list is the most common Information Systems (IS) security incidents experienced by organisations. With regard to question 17, please tick **(√)** in the box to indicate frequency of occurrence in your library for the past six (6) months.

17.	**Presence of security threats in my library.**	**Frequency of Occurrence for the Past 6 Months**				
		Don't know	Never	Very rarely	Sometimes	Always
	Hardware Security Threats	**0**	**1**	**2**	**3**	**4**
Example:	Electromagnetic interference			√		
17.1	Electromagnetic interference					
17.2	Failure of communication equipments					
17.3	Hardware/ equipments failure					
17.4	Installation/ use of unauthorised hardware					
17.5	Maintenance errors					
17.6	Malware and malicious code (e.g. virus, worm, trojan horse, logic/time bombs, trapdoor) e.g. making it impossible to boot the computer.					
17.7	Theft, physical sabotage, vandalism of ICT hardware equipments					
	Software Security Threats	**0**	**1**	**2**	**3**	**4**
17.8	Abuse of computer access control					
17.9	Adware and spyware					
17.10	Corruption by system, system errors, or failure of system software					
17.11	Cyber-terrorism					
17.12	Hacking/Intrusion/unauthorised access to system resources					
17.13	Installation/use of unauthorised programmes or software					
17.14	Maintenance errors					
17.15	Malware and malicious code (e.g. virus, worm, Trojan horse, logic/time bombs, trapdoor) e.g. program crashes, repeated error messages or periodically reboot your system.					
17.16	Password attacks/sniffing/stealing					
17.17	Software piracy					
17.18	Unauthorised changes to software settings					
17.19	Use of library Internet for illegal or illicit communications or activities (e.g. surfing for pornography)					
17.20	User abuse/fraud					
17.21	Weak passwords					

17.	Presence of security threats in my library.	Frequency of Occurrence for the Past 6 Months				
		Don't know	Never	Very rarely	Sometimes	Always
	Network Security Threats	**0**	**1**	**2**	**3**	**4**
17.22	Denial of service attacks (DoS)					
17.23	Eavesdroping/ wiretapping					
17.24	E-mail attacks /spams/ fraud					
17.25	Hacking/ Intrusion/ unauthorised access					
17.26	IP spoofing attacks					
17.27	Malware and malicious code (e.g. virus, worm, Trojan horse, logic/time bombs, trapdoor) e.g. losses associated with the network downtime or lowered network speed.					
17.28	Misrouting/re-routing of messages					
17.29	Packing sniffs					
17.30	Password attacks/sniffing/stealing					
17.31	Probes and scans or unauthorised access to computers, data, services and applications					
17.32	Session hijacking					
17.33	Transmission errors					
17.34	Weak password					
17.35	Website defacement					
17.36	Wireless network breach					
17.37	Zombie networks					
	Data Security Threats	**0**	**1**	**2**	**3**	**4**
17.38	Data diddling (Changing data with malicious intent before or during input into the system)					
17.39	Data loss due to wrong procedures of updating/storage/backup etc.					
17.40	Data manipulation					
17.41	Delay in updating/dissemination					
17.42	Destruction due to natural disaster etc.					
17.43	Exposure of patrons sensitive data through web attack					
17.44	Impersonation/ social engineering					
17.45	Loss of patron data/privacy ideas					
17.46	Malware and Malicious code (e.g. virus, worm, Trojan horse, logic/time bombs and trapdoor) e.g. destroy your data or wipe your hard drives clean					
17.47	Masquerading of user identity					
17.48	Password attacks/sniffing/stealing					
17.49	Phishing/ pharming					
17.50	Theft of proprietary data					
17.51	Unauthorised access					
17.52	Unauthorised data copying					
17.53	Unauthorised transfer of data					
17.54	Unauthorised/accidental disclosure/modifications/alteration of data					

17.	Presence of security threats in my library.	Frequency of Occurrence for the Past 6 Months				
		Don't know	Never	Very rarely	Sometimes	Always
	Physical facilities & Environmental Threats	**0**	**1**	**2**	**3**	**4**
17.55	Hazardous material accident					
17.56	Intrusion/ unauthorised access into library building					
17.57	Leaking					
17.58	Natural calamity (e.g. fire, flood, storm, earthquakes or lightning)					
17.59	Power supply failure (e.g. electricity, air-conditioning, water utility)					
17.60	Theft, buglary, sabotage, vandalism or physical intrusions					
	Other Threats	**0**	**1**	**2**	**3**	**4**
17.61	Employee misconduct					
17.62	Human errors (data entry errors or carelessness)					
17.63	Online extortion					
17.64	Social engineering					
17.65	Unfaithful patrons					
17.66	Unfaithful staff					

18) In your opinion, the most common IS security threats sources in your library come from (only ONE answer, please):

[ ] Hardware and software failures (e.g. power failure, equipment failure, network failure or system malfunction)

[ ] Natural or environmental threats (e.g. fire, flood or earthquake)

[ ] People or human threats (e.g. intentional or unintentional acts by library staff or library patrons)

[ ] Others (Please pecify:……..)

[ ] Unknown

PART C: 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.

19.	**Presence of technological security in my library.**	Not implemented	Only some part has been implemented	Implemented but has not been reviewed	Implemented and reviewed on regular basis	Fully implemented and recognised as good example for other libraries
	Hardware security	**1**	**2**	**3**	**4**	**5**
e.g.	Periodical remote mirroring or file mirroring to back up disk drives.		√			
19.1	CCTV, visual camera, magnetic detection system and electronic anti theft system at strategic places, public computer areas and server areas.					
19.2	Emergency power sources and alternative communication lines. (e.g. use of alternative telephone lines or cables and generators)					
19.3	Locks, security cables, locked cable trays, metal cages or anchoring devices to improve the security of hardware equipments.					
19.4	Periodical remote mirroring or file mirroring to back up disk drives.					
	Software Security	**1**	**2**	**3**	**4**	**5**
19.5	Anti spyware software to detect and remove any spyware threats.					
19.6	Anti-phishing solutions to prevent phishing attacks.					
19.7	Cleanup software to erase files or settings left behind by a user.					
19.8	Desktop security software at application level and operating level to monitor, restrict usage or disable certain features of the workstations.					
19.9	Distribution agents to automate the process of installing an application or updates to workstations on a network.					
19.10	ID management software to automate administrative tasks such as resetting user passwords and enabling users to reset their own passwords.					
19.11	Menu replacement software to replace the standard windows desktop interfaces and provide control on timeouts, logging and browsing activities.					
19.12	Multi user operating systems and application software to allow concurrent access by multiple users of a computer.					
19.13	Periodical automatic debugging and tests to remove any defects from newly developed software or hardware components.					

19.	**Presence of technological security in my library.**	Not implemented	Only some part has been implemented	Implemented but has not been reviewed	Implemented and reviewed on regular basis	Fully implemented and recognised as good example for other libraries
	Software security	**1**	**2**	**3**	**4**	**5**
19.14	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.					
19.15	Single sign on system for user authentication and authorisation to access all computers and systems without the need to enter multiple passwords.					
19.16	Spam filtering software to automatically detect unwanted spam emails from getting into a user's inbox.					
19.17	Timer software to control the amount of time a patron can use a workstation.					
19.18	User entrance log to record and monitor user logs. These logs are regularly analysed by a library staff.					
19.19	Web filtering software to prevent access to inappropriate materials or sites.					
	Workstation Security	**1**	**2**	**3**	**4**	**5**
19.20	All office productivity software and browsers for the workstations/laptops are configured to receive updates in a timely manner.					
19.21	An application firewall is used for mobile laptops that connect to the library external LANs.					
19.22	The computer's BIOS are secured in order to create a secure public access computer.					
19.17	User identification and authentication are required before logging into the library's workstations, laptops screensavers, library network or campus network.					
19.24	Virus protection programs, configuration settings and security software programs are installed for web browsers and email programs.					

19.	Presence of technological security in my library.	Not implemented	Only some part has been implemented	Implemented but has not been reviewed	Implemented and reviewed on regular basis	Fully implemented and recognised as good example for other libraries
	Network Security	**1**	**2**	**3**	**4**	**5**
19.25	Antivirus software and desktop security software to receive regular updates to protect the internal network from any security breaches.					
19.26	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)					
19.27	Firewall to protect the internal network from external threats.					
19.28	Firewall with virtual private network (VPN) capabilities is installed for remote and wireless access connections.					
19.29	Limitation of connection time is performed via configuration routines to control and restrict access for the library's high-risk applications or databases.					
19.30	Public and staff's local area networks (LANs) are physically separated by means of separate cabling for each network to provide alternative circuit.					
19.31	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.					
19.32	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**.					
19.33	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))					
	Server Security	**1**	**2**	**3**	**4**	**5**
19.34	Anti-virus software on servers and anti-virus virus definition files are kept up-to-date.					
19.35	Authentication systems to prevent unauthorised access to the library's server.					
19.36	Fault tolerance is implemented to make sure if one system fails, then there is a backup system that immediately takes over.					
19.37	Firewalls to protect the library network from unwarranted intrusion.					

19.	**Presence of technological security in my library.**	Not implemented	Only some part has been implemented	Implemented but has not been reviewed	Implemented and reviewed on regular basis	Fully implemented and recognised as good example for other libraries
	Server Security	**1**	**2**	**3**	**4**	**5**
19.38	Intrusion detection software and host auditing software are installed to monitor the servers or computers for signs of intrusion.					
19.39	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.					
19.40	Server logs are reviewed periodically by using a log file monitor utility to monitor any signs of intrusion or security violations.					
19.41	The file system in a server is restricted access to the directory structure using file or directory permissions.					
19.42	The library servers' operating systems (OS) and applications are hardened to protect from any vulnerabilities.					
19.43	The server is placed in a secure location, such as in a lockable cage, a locked room and place it with environmental controls.					
	Data Security	**1**	**2**	**3**	**4**	**5**
19.44	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.).					
19.45	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)					
19.46	Disposable of unused media and sensitive media are properly managed to maintain an audit trail.					
19.47	Enforced path is created between a user terminal and other library services that the user is authorised to reduce the risk of unauthorised access.					
19.48	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)					

19.	**Presence of technological security in my library.**	Not implemented	Only some part has been implemented	Implemented but has not been reviewed	Implemented and reviewed on regular basis	Fully implemented and recognised as good example for other libraries
	Data Security	**1**	**2**	**3**	**4**	**5**
19.49	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)					
19.50	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).					
19.51	RFID tags to manage and secure the library collection as well as to track attendance and prevent unauthorised access into the library building.					
19.52	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).					
19.53	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.					
19.54	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.					
19.55	Llibrary's vital 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).					
19.56	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).					

19.	**Presence of technological security in my library.**	Not implemented	Only some part has been implemented	Implemented but has not been reviewed	Implemented and reviewed on regular basis	Fully implemented and recognised as good example for other libraries
	Data security	**1**	**2**	**3**	**4**	**5**
19.57	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).					
19.58	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).					
	Physical and environmental security	**1**	**2**	**3**	**4**	**5**
19.59	Air conditionings to stabilise the air temperature and humidity within the library building.					
19.60	Earthquake early warning system to provide an emergency warning to the library staff and patrons prior to damaging ground shaking.					
19.61	Flood detector to sense the presence of water to provide an early warning of developing floods in a library.					
19.62	Lightning protectors and surge protectors to protect any valuable machines or equipments from lighting strikes, voltage spikes and surges.					
19.63	Security guards to monitor people entering and leaving the library buildings and sites.					
19.64	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.					
19.65	Use of magnetic stripe swipe cards, electronic lock, proximity cards, bar code card or biometrics to secure and control access to restricted library areas.					
19.66	Warning signs, fencing, vehicle height-restrictors, site lightings and trenches around the library areas to provide initial layer of security for a library building.					
19.67	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.					

20.	**Presence of information security policy in my library.**	Not implemented	Only some part has been implemented	Implemented but has not been reviewed	Implemented and reviewed on regular basis	Fully implemented and recognised as good example for other libraries
		1	**2**	**3**	**4**	**5**
20.1	Back ups and off-site storage policies for your library data, media or materials that contain sensitive information.					
20.2	Data classification, retention and destruction policies for your library data, media or materials that contain sensitive information.					
20.3	Identity management policies for library Information Systems user registration and password management.					
20.4	Job responsibility policy for individual employee responsibilities related to the library IS security practices.					
20.5	Policies on access control, authentication and authorisation practices for using the library Information Systems.					
20.6	Policies on protection of library IS assets to protect your library's hardware, software, data and people.					
20.7	Secure disposal policies to dispose library data, media or materials that contain sensitive information.					
20.8	Polices on reporting, notification and response of Information Systems security events to affected parties such as individuals, law enforcement, campus or parent organisations.					
20.9	Policies on acceptable use of wireless devices in your library such as laptops and hand phones.					
20.10	Policies on acceptable use of workstations, e-mails, databases, intranet and Internet in your library.					
20.11	Policies on managing privacy and confidentiality issues, including breaches of personal information.					
20.12	Policies on sharing, storing and transmitting of library data via ISPs, external networks or contractors' systems.					

21.	**Prsence of procedures and controls in my library.**	Not implemented	Only some part has been implemented	Implemented but has not been reviewed	Implemented and reviewed on regular basis	Fully iImplemented and recognised as good example for other libraries
		1	**2**	**3**	**4**	**5**
21.1	Controls and disciplinary procedures if a library staff or patrons breach the IS security polices or rules. (e.g. verbal warning, written warning, suspension and dismissal).					
21.2	Procedures for handling library sensitive data and personal data of library patrons to prevent errors, unauthorised disclosure or misuse by those who handle it.					
21.3	Procedures for non-disclose agreement or confidentiality agreement to all library staff and patrons to protect any type of confidential and proprietary information.					
21.4	Procedures for update and review existing information security policies.					
21.5	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.					
21.6	Procedures that list all requirements with regard to outsourcing any library Information Systems service or activities.					
22.	**Presence of administrative tools and methods in my library.**	**1**	**2**	**3**	**4**	**5**
22.1	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).					
22.2	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).					
22.3	Procedures on handling, reporting, notification and response of IS security events to affected parties such as individuals, law enforcement, campus or parent organisation.					

22.	**Presence of administrative tools and methods in my library.**	Not implemented	Only some part has been implemented	Implemented but has not been reviewed	Implemented and reviewed on regular basis	Fully implemented and recognised as good example for other libraries
		1	**2**	**3**	**4**	**5**
22.4	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)					
22.5	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.					
23.	**Presence of awareness creation in my library.**	**1**	**2**	**3**	**4**	**5**
23.1	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.					
23.2	All staff and patrons at various levels receive appropriate information security trainings and education.					
23.3	All staff and patrons at various levels receive regular updates on your library Information Systems' policies and procedures.					
23.4	Information security awareness trainings have become mandatory to all staff and patrons at various levels.					
23.5	Risk assessment approach exists and follows a defined process that is documented.					
23.6	Staff and patrons at various levels are trained to monitor and handle the library's Information Systems on their own.					
23.7	There are balanced set of key performance indicators (KPIs) and metrics used to provide the real insight into the effectiveness of security awareness programs.					
23.8	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).					
23.9	Threats that could harm and adversely affect critical operations of your library Information Systems' security are identified and up dated regularly.					
23.10	Vulnerabilities in your library information systems and related processes are identified and up dated regularly.					

-End of Questionnaire-

……..Thank You……

List of publications:

PAPER I:

Roesnita, I. and Zainab, A.N. (2010). A framework for assessing information system (IS) security practices in Libraries. In: *Towards Greater Information Accessibility: Proceedings of the 3rd International Conference on Libraries, Information and Society (ICOLIS 2010) 9-10 November 2010, Petaling Jaya, Malaysia.* Editors, A.Abrizah et al. Petaling Jaya: Library & Information Unit, Faculty of Computer Science & Information Technology, University of Malaya, 2010: 273-287. (LISI Monographic Series, no.1). ISBN:9789675148767.

PAPER II:

Roesnita, I. and Zainab, A.N. (2011). Information systems security in special and public libraries: assessment of status. *Malaysian Journal of library & Information Science*, 16(2): 45-62. ISI, SSCI, Scopus. Tier 4 (JCR2010). (*ISI/SCOPUS Cited Publication*)

PAPER III:

Roesnita, I. and Zainab, A.N. (2013). Assessing the Status of Library Information Systems Security. Accepted paper, *Journal of Librarianship and Information Science (JOLIS),*(UK). (*ISI-Cited Publication*).