Information (ICT) security and Libraries

Yasmeen Zia[1*], Seema Tehseen[2], Rajesh Kathane[3]

[1-3]Librarian, [1]Government College Ghoradongri, Betul, [2]Bhoj College, Bhopal, [3]L.N Medical Collage & Research Centre Bhopal, Madhya Pradesh, India

***Corresponding Author: Yasmeen Zia**
Email: yasmin.library@gmail.com

Abstract
The paper provides to brief introduction of the term 'Information Communication Technology Security with special reference of libraries and information centres". The paper also discusses important facts for better information security in a system or organization like libraries. The library is a centre for a acquisition and dissemination of information to its user so that this is a really important to all the library professionals to take preventive steps like policy and guidelines to safe and secure the acquire e-resources and content. Many of the information professionals observe that new technological development in the form of computers, telecommunications, electronics and Internet have been adopted in libraries to serve the researchers & academics. In the present digital world where Information Technology has become an essential part of the libraries. However libraries continue to increase their use of IT, the security risk increasing more rapidly. Misuse by professionals, students, users, viruses, hackers and other abuse have created need for various ways and methods implementing in Information Security.
In this paper, I have tried to highlight on Information about Information Security Management for organizations and socio-ethical issues related to it. Also, methodology for assessing information Security in networked libraries is also discussed.

Keywords: Information security, Socio-ethical, Information Communication Technology, Library.

Introduction
Library has always been striving hard to meet the expectations of its users however, there has been a long felt need to bring clarity and uniformity in procedure and practices of the library to improve its efficiency, utility and services. It identifies, evaluates, procures, processes and then makes these learning resources available to the faculty and students for their teaching and research. Because of the conveniences like multi user access and anywhere, anytime access, there is a considerable demand for online databases, e- journals and e-books. Libraries and Information centers tried to provide excellent access infrastructure like high internet bandwidth, Wi-fi connectivity in the campus for its user. But in theses information era its essential part to secure online e-content and distribute its in coherent way.

The goal of information security is mainly to detect and prevent the unauthorized acts of computer users (Gollmann,1999) and the broad objectives of a computer security policy are to ensure the data confidentialty,Smith,1989).[4] Information security issues cover information security policy, risk analysis, risk management, and disaster recovery (Von Solms et.al., 1994).[6]

Term information security is defined as all aspects related to achieving and maintaining confidentiality, integrity, availability, audit ability (accountability), authenticity and reliability. Information security therefore aims at providing confidentiality, integrity, availability, accountability, authenticity and reliability, which are referred to as information security concerns.[2]

Purpose and Scope
The purpose of implement of the information security is to:

1. establish administrative, technical, and physical safeguards to protect e-resources subscribed by the library
2. Contents that is owned, licensed, stored or maintained by the institute, whether such information is contained in paper, electronic records, or in any other form, and is designed to ensure the security and confidentially of Personal Information.
   The information security program is also designed to protect information of the institute deems sensitive in nature.
3. Establish the direction on and commitment to Information Security and ensure it is communicated, applied, and complied with throughout the organization.
4. To protect information assets from loss or misuse, and to mitigate the risk of financial, productivity, and reputation

Fig. 1: Need of Information Security

Flynn (2001)[7] proposed a model which covers:
1. E-risk management policy
2. Computer security policy
3. Cyber insurance policy
4. E-mail policy
5. Internet policy
6. Software policy

Information Security Management (ISM)[3]
In the development of a framework for the implementation of ISM in an organization, it is important to first consider the elements of the preparation phase of the process. The various stages of the framework are (Vermeulen and Solms, 2002)[5]
1. Preparatory Stage
2. Implementation Stage
3. Maintenance Stage

Table 1: Showing Information Security Management (ISM) Framework

Top Management Commitment		
Organisational Aspects	Security requirement	Vision & Strategy Keeping security in view
	Information security policy	
	Risk management	
	Follow up	
Standards set for information security		

(Source- Vermeulen & Solms, 2002)

Preparatory stage consist of top management, information security standards, organizational aspects of information security and security vision and strategy.[1]

In Implementation stage developing sets of safeguards and procedures included.

The Maintenance s is represented by a follow-up element.[3]

Socio-Ethical information Security awareness of Information Security-

It is vital, therefore, to have certain socio-ethical information security controls in place. These controls may include privacy, property and obligation.[8] Socio-ethical information security awareness must be incorporated with the security policy of the institutions.

Information Security in Networks
1. **Authenticate connections**: Automatic equipment identification shall be used to authenticate connections from equipment if it is important that the communications can only be initiated from a specific location or equipment.
2. **Diagnostic and configuration ports:** Physical and logical access to diagnostic and configuration ports shall be controlled.
3. Groups of information services, users and information systems should be segregated on networks. For shared networks, especially those extending across institute boundaries, the capability of users to connect to the network should be restricted to institute service purposes on a need-to-know basis.
4. Routing controls should be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the applications.
5. Access to operating systems should be controlled by a secure log-on procedure. All users should have a unique user ID for their personal use only and a suitable authentication technique used to authenticate users.
6. Sensitive systems should have a dedicated (isolated) computing environment.
7. A formal policy, operational plans and procedures should be developed and implemented for tele-working activities and appropriate security measures adopted to protect against the risks of using mobile computing and communication facilities.

Information Security and Libraries
The library and information security means provide a safe and secure facility for library employees, library resources, equipment and library patrons, specially against their theft and mutilation.[9] Libraries need to have policies, protection measures and trained staff in place in order to safeguard their investments.[10]In today's environment, it is necessary to take precaution to avoid theft, hacking, virus and stealing the resources, equipment, etc. Therefore Library and information security is necessary in all aspects such as Organization Security, physical security and Technological Security.

Types of security measures in Libraries
Library and information security can be measured in three parts
1. Organizational Security
2. Physical Security
3. Technological Security

1. **Organizational Security –**The organizational security comprises of four main factors they are as follows

The existence of library and information security policies, the emplacement of procedures and control, the formation of adequate administrative tools and methods and awareness creation in staff to perform their job.[11] Some of the tools that can be used to protect library systems, including: firewalls, antivirus software, alarms, network analysis tools, and encryption.[12] Suggested useful advice in the forms of steps that libraries can take to protect themselves, including: avoiding being an attractive target, keeping software up to date, backing up valuable data, setting traps to catch hackers, and monitor systems for unusual activity.

2. **Physical Security** –Physical security includes Architectural Considerations, security staff and Hardware Security.
3. **Technological Security** – "Technological security mechanisms are used to safeguard the library and information integrity, confidentially, availability. These include the mechanisms that are put in place to protect,

control and monitor library and information access as well as prevent unauthorized access to data that is transmitted over a library System. The assumption is that a technological foundation must always be in place in any library environment treated as of the main defensive system. The technological security foundation refers to the security of hardware, software, workstations, networks, servers, data and its physical facilities and environment in libraries."[11]

Conclusion

Recent development in information technology that has made possible to share information with libraries as well as the users. Many of the new arrangements mean that information which was previously restricted to internal staff is now shared by others who may or may not properly guard it. Thus there is an urgent need for the organizations to see their information security as a lifecycle where they assess, design, implement, manage and continuously reassess their infrastructure.[13]Libraries have to be much secured regarding their technological, physical, and organizational security to serve their patrons in proving every possible service. In the light of changing user expectations, libraries have been expanding their services by prodiging user –centered services services where security majors should be given top priority.

Source of Funding

None.

Conflict of Interest

None.

References

1. A paper submitted to University of Hertfordshire.
2. Information management & computer security. 2006;9(1).
3. Information management & computer security. 2006;10(3).
4. Information management & computer security. 2006;11(5).
5. Vermeulen C, Von Solms R, "The information security management toolbox –taking the pain out of security management ", *Inf Manag Computer Sec* 2002;10(3):119-25.
6. Von Solms R, VanHaar H, VonSolms S.H, Caelli W.J (1994),"A framework for information security evaluation", *Inf Manag* 1994;2(3):143-53.
7. Internet source www.isedj.org
8. Internet source www.scissec.scic.ecu.edu.au
9. Internet source www.librisdesign.org
10. Internet source www.petascale.org
11. Internet source www.myjurnal.my
12. Internet source www.gep.doalog.com
13. Internet source www.naturesoft.com
14. Gerber M, VonSolms R, Overbeek P. "Formalizing information security requirements", *Inf Manag Computer Secur* 2001;9(1):32-7.
15. Golmann D," Computer Security ", John Wiley & Sons, New York, NY
16. Goswami S. Networking and security measures. *DESIDOC Bull Inf Technol* 2004;24(2):9-16.
17. Highland H.J,"A view of information security tomorrow ",Computer security – Proceedings of the IFIP TCII Ninth International Conference on Information Security, Elsievier Publishers B.V.,Amsterdom,1993:243-8.
18. Ismail R & Zainab A N. Assessing the status of Library Information System Security. *J Libr Inf Sci* 2013;45(3):232-47.
19. Latuszek T. Library Security.(2000). A growing Awareness. *Libr Archival Secur.* 2000;15(2):3-7.
20. Gupta M. Library & Information Security Measures. *IASLIC Bull* 2015;60(4):223-42.
21. Roberts G. Network Security is manageable, *Computers in libr* 2006;26(1)28-30.
22. Schulz,E.E., Proctor,R.W., Lien,M.C(2001),"Usability & Security :an appraisal of usability issues in information security methods" *Computers Secur* 2001;20(18):620-34.
23. Siponen T. "A Conceptual foundation for organizational information security awareness", Inf Manag Computer Secur 2000;8(1):32-41
24. Smith M(1989),"Computer Security – threats,vulnerabilities & countermeasures", *Inf Age* 1989;11(4):205-10.
25. Trompeter C.M, Eloff A J. "Framework for the Implementation of Socio ethical Controls in information security", *Computers Secur* Vol 2001;20(5):384-91.
26. Von Solms b. "Information Security – The Third Wave" *Computers Secur* 2000;19(17):615-20.
27. Von S R. "Information Security Management: Why standards are important ",Infromation Management & Computer Security, 2000;7(3):50-5.
28. Zhdanov D. Information security in organizations: drivers, policies &compliance incentives. University of Minnesota,Ph.D Thesis. 2007;44-74.

How to cite: Zia Y, Tehseen S, Kathane R. Information (ICT) security and Libraries. *IP Indian J Libr Sci Inf Techno* 2020;5(1):43-5.