Issues in Information Security

(Digital Library Environment)

S. Hema Siselee, V. Soundhariya
Department of CSE,
Parisutham Institute of technology and science
Thanjavur

***Abstract*:- As organizations increase their reliance on, possibly distributed, information systems for daily business, they become more vulnerable to security breaches even as they gain productivity and efficiency advantages. Security in digital libraries is an issue of the most important, and should be considered carefully in creating policies and strategic plans of institutions wanting to set up a digital library. This paper focused on the four main streams that concerns security in the digital environment, namely: infrastructure, digital content, users and standards and legal issues. This literature review also built upon previous literature reviews, and is one of the few of its kind in the topic.**

I. INTRODUCTION

Society has been increasingly dependent on information technology for several years now. In this Information Age, millions of users access and exchange billions of objects of information content in complex work flow processes (e.g., commerce, learning, health care). The research community uses computer systems to perform research and to disseminate findings. Information sharing has been made easier and less expensive by Internet technologies and global networking infrastructures, but availability of such information systems comes at the expenses of higher risks. In the long run, information is not preserved, websites tend to disappear frequently and digital media become obsolete easily and there can be an abuse in the privacy of information. Moreover, the integrity of the systems could be compromised. Access control is often described as rules regulating how participants are allowed to access object and could also be viewed as information flow control because every access results in flow of information between entities (either or both participant and object. The integrity and availability of all these systems have to be protected against a number of threats. Hackers, rival corporations, terrorists and even foreign governments have the motive and capability to carry out sophisticated attacks against computer unless an attack is successful or a system is compromised, security in general, intrusion detection in particular, is rarely noticed by management. When security fails and the notification is too late, only would managers consider viewing the security issue as visible as their organizational needs.

II. METHODOLOGY

The search strategy that was employed for this literature review involved searching printed and online materials. Several keywords used to search catalogues and databases include “digital libraries AND security”, “security in digital libraries”, “information security in digital libraries”, “threats information security”, “wireless security”, “database security”, “system security ontology library”, “security AND libraries”, “security in libraries”, “privacy in libraries”, “information security”, “digital content security”, “information security AND legal aspects”, “information security standards”, “information security AND digital library”, “data protection law” A very broad spectrum of articles that deals with the whole concept of security came out; so we decided to limit the articles to those that pertains to the four main streams that concerns security in the digital environment:

1) **Infrastructure** - This section focused on the importance of security applied in any system infrastructure that covers securing hardware and software, ensuring network security, and looking into Web vulnerabilities that can distract the smooth flow of communication and transfer of information in a wired or wireless environment.

2) **Digital content** - This section discussed how important it is to also ensure that digital content are secured in a digital environment and describes some of the steps that can be undertaken in order to recover important data and attain the real purpose of preservation.

3) **User information security** - This section illustrated some issues pertaining to the terms of security of systems, maintaining the confidentiality of users within a digital library environment i.e. their private information are kept in a trustworthy manner and is not used without their knowledge.

4) **Standards and legal issues** - This section provided an overview of the development of the different existing standards in ensuring security of any system which can serve as basis for formulation of polices and guide in setting up a system in digital environment.

III. SECURING THE HARDWARE

A hardware security module (HSM) is a physical computing device that safeguards and manages digital keys for strong authentication and provides cryptoprocessing. These modules traditionally come in the form of a plug-in card or an external device that attaches directly to a computer or network server. Hardware security is the security of such equipment as computers, printers, monitors etc which libraries find indispensible in their day today functions especially in this digital. There is need to keep such hardware in secure rooms

under physical lock and key and an inventory system should be implemented for easy tracking. Control deters theft of property, unauthorized access to servers thereby preventing tampering with server settings, corrupting data, or gaining access to programs and confidential information. In order to maintain hardware security, it is important to implement strong physical security measures.

IV. NETWORK SECURITY

Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. In a digital library "...resources are accessed via the Internet and networks are playing a vital role in connecting these information sources". "In the digital age availability of secure, efficient and cost effective networks of access, would be the core competency of the libraries". It would be vital for libraries to secure networks so that the integrity of data can be maintained. Network equipment include hubs, routers switches and cabling. For the hardware that supports the network it is necessary to implement security measures that correspond to all other sensitive hardware equipment. Computer networks now exist as wired and/or wireless networks and security measures in these environments are different. Libraries tend to use wired networks for machines which are fixed in their premises. Wireless networks are used for connecting users who might be having their own mobile gadgets to connect to the network. Unlike in the wired network, security in a wireless network is more of concern because network transmissions are available to anyone within the transmitter with the appropriate antenna, physical access controls like doors and locks do not help. Due to the increase on the use of mobile gadgets, digital libraries are increasingly being accessed via wireless networks. That implies the need to consider investment in wireless network security if the integrity of information resources is to be maintained.

V. DATABASE SECURITY

Database security refers to the collective measures used to protect and secure a database or database management software from illegitimate use and malicious threats and attacks. It is a broad term that includes a multitude of processes, tools and methodologies that ensure security within a database environment. Databases are very critical parts of the library information system as the key hosts of metadata, and other administrative information. Databases employ security systems as those of operating systems but users are assigned certain types of groups called roles. For example the head librarian and the library clerk have different roles in the system and that controls what each user can view or edit in the database. Database security can be maintained discretely or can be integrated with operating systems. That implies that users will require only one logon into the system. Database security mechanisms are effective if they are used in conjunction with proper security mechanisms implemented at the front end application like dynamic web pages. Databases have the capability to offer access to resources as defined by roles and profiles and should be based on the respective functions. A database should also have tracking features that can track when the database was accessed by whom and what changes took place. For instance: it must be possible to trace who added an article to the collection and when. Data transmission should be secured using protocols such as Secure Socket Later (SSL) or Secure Shell (SSH). which is historically associated with web pages accessed via the secure hypertext transfer protocol even though it can be used to encapsulate any protocol? Judges that SSL is best for protecting transaction based protocols such as web traffic and mail transactions. SSH is a secure replacement for commands such as rlogin, rcmd, and rshel. SSH also uses public key cryptography like SSL but does not rely on trusted authority to issue the public/private key pairs.

VI. LIBRARY PRIVACY PLANS AND POLICIES

In order to maintain user trust, libraries should take measures to protect their patron's confidential data. Indicates that this can be done in the form of a privacy plan, which should be built on a combination of 'principle' and 'experience'. Different authors offer recommendations for libraries regarding privacy plans. Newby proposes a set of recommendations:

1. Maintain a comprehensive list of data that may be collected and the circumstances
2. For each type of data, what risks of misuse exist?
3. Specify a policy for the collection of data and possible misuses.
4. Identify personnel responsible for ensuring the policies are followed, and for remediation as needed.

So these recommendations consist of listing sensitive data and the risks, devising a data collection policy and the training of personnel. Discusses a number of policies to limit privacy risks, that are related to Newby's third recommendation above. First of all, libraries should use anonymity in reference software as much as possible. A second step is the limitation of collection of personal information to what is needed for a specific transaction. A third step mentioned by Neuhaus is the restriction of the number of persons who have access to certain records. The fourth recommendation point of Newby handles about the personnel of a library. Privacy policies are also influenced by national regulations. It is possible to base these principles on general principles, for example the International Safe Harbor privacy principles It might be valuable for libraries to consider using privacy principles in their organization, as Sturges' concludes: "The knowledge, plans and procedures to deliver data protection and confidentiality in practice are not present in libraries generally". This problem can lead to legal issues, so adjusting security practices to national and international standards might be a good idea for libraries. This is discussed in the next section.

VII. CONCLUSION

This paper has reviewed the literature on information security which librarians have to consider in setting up and managing digital libraries. The literature revealed that maintaining a secure infrastructure is necessary, however it implies costs. Finally, given the proliferation of digital libraries and the influence that they are increasingly having in research and learning, it is imperative that libraries consider taking security issues seriously in order to ensure that their resources and user privacy are secured. To ensure that there is an adequate level of information security, different standards and benchmarks must be used. Our literature review has discussed various ISO and non-ISO standards, which could be used by libraries to review their security policies.

VIII. REFERENCES

[1] Abrams, S.L. (2005). Establishing a global digital format registry. Library Trends, 54(1), 125-143. doi:10.1353/lib.2006.0001.
[2] Al-Suqri M. and Afzal W. (2007). Digital age: Challenges for libraries. Information , Society and Justice. 1(1), 43-48. doi: 10.3734/isj.2007.1105.
[3] American Library Association (2008). Code of ethics of the American Library Association. Retrieved on 14th April 2011 from http://www.ala.org/advocacy/proethics/codeofethics/codeethis
[4] Balas, J. (2005). Close the gate, lock the windows, bolt the doors: Securing library computers.
[5] Computers in Libraries, (March), Strategies.
[6] Retrieved on 15th April 2011 from http://28-31.
[7] Beagrie, N., Semple, N., Williams, P. and Wright, R. (2008). Digital preservation policies part 1:
[8] Final report October 2008.
[9] www.jisc.hosting.eduserv.org.uk/media/documents/programmes/preservation/jiscpolicy_
[10] p1finalreport.pdf.
[11] Birnbaum, J.S. (2004). Cyber security considerations for digital libraries in an era of pervasive
[12] computing. In Proceedings ACM/IEEE Conference on Digital Libraries (JCDL'04) (pp.169-169)
[13] New York: ACM.
[14] Bowers, S. (2006). Privacy and library records. The Journal of Academic Librarianship, 32(4), 377-383.
[15] BSI - The British Standards Institute and British Standards Publications (2010). The British Standards
[16] Institute and British Standards Publications. Retrieved on 5th May 2011 from http://www.standardsuk.com/bsi/.