Security for Libraries in the Digital Networked Environment

Manoj Kumar K Haneefa K M

Abstract

Libraries are using Information and Communication Technologies (ICT) for their operations and services by making huge investments and spending vast amounts of staff time for the selection, acquisition, retrieval, and dissemination of digital information. But the proliferation of computers, widespread acceptance of computer networks, explosive growth of Internet, increased reliance on electronic databases and the move from dedicated mainframe environments to client-server environments make libraries vulnerable to security threats. The moment user connects the computer to a Network or Internet, is the moment that the security of data has been compromised. Even the most secure systems, shepherded by the most intelligent and able system administrators, and employing the most up-to-date, tested software available are at risk every day. It is very essential to take all measures to protect the ICT infrastructure from security threats. However, libraries are lagging behind in realizing the need to protect their ICT resources and services from misuse, damage, theft, sabotage, mistake, etc. This paper deals with the issues related to the security of libraries in the present digital networked environment and makes recommendations for protecting ICT resources and services. The paper discusses security risks, strategies for security, security policy, personnel security, physical security, software security, network security, Internet security, access control, protection against computer viruses, protection of public terminals and backup information. This paper also discusses the need for professional assignments for library security and the importance of security training for library professionals.

Keywords : Security Risks, Security Policy, Internet Security, Access Control, Network Security

0. Introduction

With the advent of the Information and Communication Technology(ICT), the paradigm for libraries has dramatically changed due to the penetration of internet, communication technologies and the consequent elimination of the constraints based on the geographical boundaries. The conventional library system is undergoing rapid changes; it has transformed from secured physical location to less secured public domain systems. As the application of Information and Communication Technologies (ICT) in libraries is widely accepted, Libraries are using these ICT facilities for their operations and services by making huge investments and spending large amounts of staff time for the selection, acquisition, retrieval, organization and dissemination of digital information. But in the absence of sufficient security ICT may not be used to with its full potentials. The proliferation of computers, widespread acceptance of computer networks, explosive growth of Internet, increased reliance on electronic databases and the move from dedicated mainframe environments to client-server environments make libraries vulnerable to the security threats. It is very essential to take all measures to protect the ICT infrastructure of libraries. However, libraries are lagging behind in realizing the need to protect their ICT resources and services from misuse, damage, theft, sabotage, mistake, etc.

Information is the most valuable resource of libraries. This information should be stored in such a way that its integrity and availability is maintained. ICT allow libraries to store, preserve, index, retrieve and

disseminate information more easily and quickly. But it gives a lot of scope for misuse and abuse of electronic information. There are risks of loss from unauthorized access, use, modification or destruction of information, which may be caused accidentally or intentionally. If it is damaged or lost due to misuse, mistake, theft, sabotage, the very purpose of these resources is not achieved.

Digital networked environment of a library may include hardware, library management software, computer programs, electronic databases, data, information, etc. Now libraries are web accessible and increasingly handling web accessible information. Threats to these resources may arise from the failures of computer and communication hardware or software, malfunctions caused by bugs and viruses, overload or other operational or quality problems. Misuse or abuse of digital information may arise from the unauthorized access for the purpose of mischief, vandalism, sabotage, fraud or theft, etc. Digital resources of a library should be stored, retrieved and disseminated in an authorized manner and should be disclosed to authorized users only. It should be protected from threats to gain its availability, integrity and confidentiality. ICT infrastructure should be protected from physical threats. System and application software should be protected from non-physical threats. Computer networks should be protected from unauthorized access, interruption and manipulation. Access to digital information should be controlled through authorization.

1. Security Risks

The first task is to determine the type and level of security risks associated with the library. The assets to be protected should be determined. Usually more insidious threat to security comes from internal sources. The explosive growth of Internet had increased the security risks from external sources also. E-mail is one of the most used Internet service or tool, but E-mail became the most dangerous medium for security threats by spreading computer viruses through attachments. Downloading of programs and files using www or ftp is also threatening dangerously. In order to evaluate the security risks associated with the network of a centre, proper security audit methodology should be adopted.

In a security audit, a company's IT infrastructure and associated process is tested for reactions to known attacks. Those reactions are then analyzed to identify possible security weaknesses. These weaknesses are measured and prioritized so appropriate controls can be deployed

The assessment will be carried out in following steps

1. Data collection
2. Assessment of Existing Systems & Processes
   - ✍ Vulnerability assessment
   - ✍ Threat assessment
   - ✍ Security Process assessment
3. Information security policy document
4. Risk analysis & management
5. Recommendations

The information gathering for the purpose of this analysis should be done by the following methods by a security audit team.

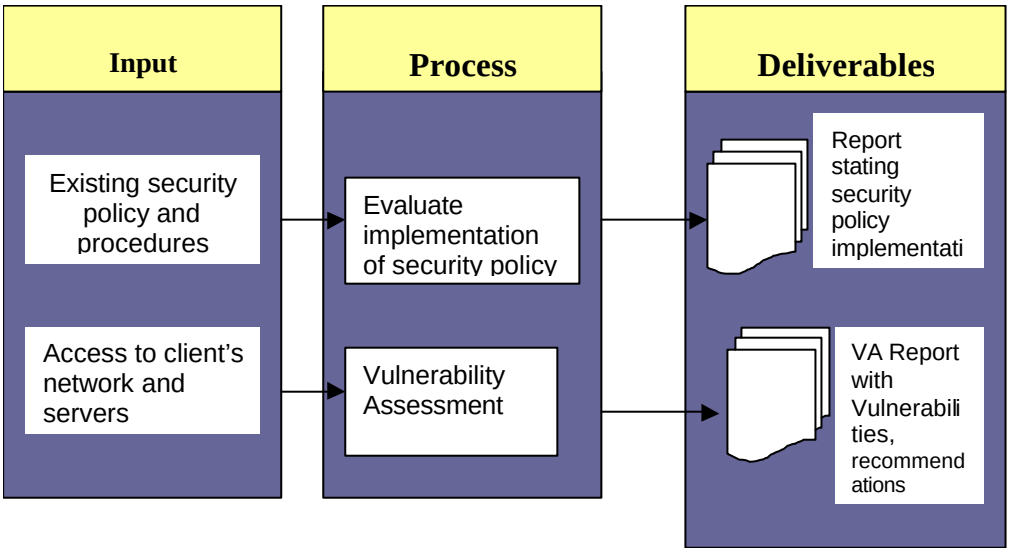
1.1 Questionnaires

A Security audit team will conduct interviews or administer detailed questionnaires that will require the client to list key business processes and assets in the order of criticality they perceive and link them to the business outputs. The team would ask the department heads to detail the departmental, interdepartmental and inter organizational dependencies of these processes and assets

1.2 Consultative discussions with the IT Team of Customer

The team will review the IT related policy documents that can provide good information about the security controls used and planned for the IT system. An organization's asset criticality assessment provides information regarding system and data criticality and sensitivity.

Assessment of Existing Systems & Processes



As part of this exercise, the task is carried out to evaluate the current operational posture of the Perimeter Architecture and servers of the organization in order to check various servers against their standard functional and non-functional requirements

2. Security Policies and Procedures

It is very important to establish well-formulated policies and procedures to protect ICT resources and access tools from security threats. A security policy defines the resources and services to be protected, discusses the technologies to be used for protecting the resources and explains how these tools should be deployed. The policy should include the purpose, scope, rules, standards and specific activities. It should cover the use of ICT resources, marking of sensitive information, movement of computing resources, disposal of sensitive wastes and security incident reporting. Enforcement of these policies is very essential to their effectiveness.

3. Personal Security

Personal security consists of management constraints and operational procedures to provide an acceptable level of protection for ICT resources. It includes procedures established to ensure that all personnel who have access to electronic resources have the required authorization and appropriate security clearance. It also includes personnel-oriented techniques for controlling people's behavior to ensure the confidentiality, integrity, and availability of digital resources.

4. Physical Security

Physical threats to ICT resources may come from extreme environmental events or from adverse physical conditions or from purposeful activity. Extreme environmental events include earthquake, fire, flood, lightning, excessive heat, humidity, etc. The digital networked environment of a library is susceptible to rough treatment and inexperienced users as well as knowledgeable vandals and thieves. Hardware can be stolen, damaged or destroyed. Peripherals can be moved, stressed, overused or damaged. Threat assessment should be carried out in a proper manner.

During this stage it is mandatory to explore threats to the assets that have been identified and will arrive at the likelihood of occurrence of adverse events due to these threats. For identification of threats threat analyse team should use multiple sources for enumeration of relevant threats. The sources that will be consulted for threat exploration must include the client representatives involved with the IT dept and threat database with details regarding post identification of threats (who and what causes the threat) and threat agents (who and what elements of the organization cause the threat). Most of the physical security threats are based on the following factors. Threat frequency: how often the threat might occur, according to experience, statistics. Threat Source Motivation and Skills: the motivation, the capabilities perceived and necessary, resources available for attacker etc. Geographical factors: proximity to chemical factories, areas of extreme weather conditions etc.,

Many security threats can be avoided by protecting the ICT infrastructure. The library should be fireproof with fire alarms, smoke detectors, extinguishers etc. It should have intrusion detectors and guards and should use surge suppressors or electronic power filters for all devices in area of power fluctuations. Secure computer/server room is a very important component of a good security program. Smoke and water detectors are essential features of a good computer room. ICT infrastructure should not expose to extreme cold or warm temperature and should be kept in an air-conditioned environment. It is a good practice to keep significant resources separate from general access equipments. All electronic media for storing digital information such as diskettes, CDs, DVDs, tape, etc. should be secure. Library professionals should clearly understand who to contact if urgent equipment repairs are needed and how to contact them.

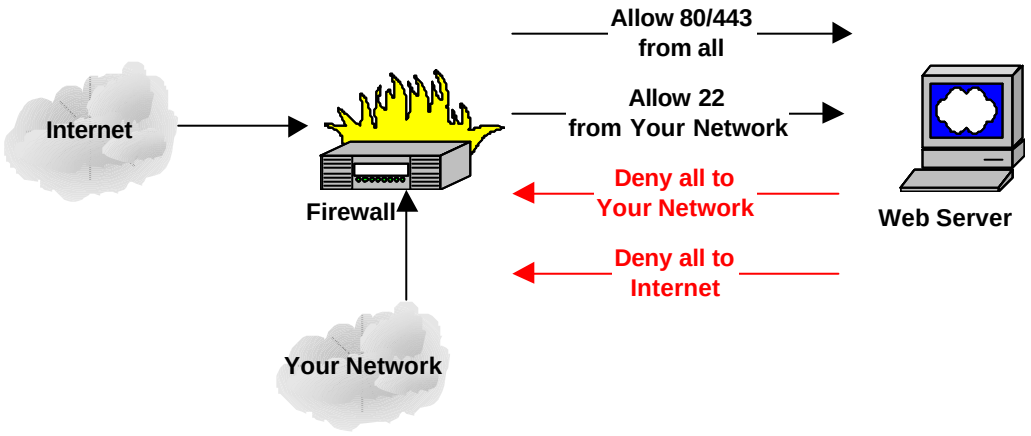
5. Software Security

Software security is very important for the smooth functioning of ICT resources and services. Software security threat includes the unauthorized access for breaking the nonpublic areas of the automated information system and viewing private records, changing files, or erasing records. Unauthorized access also includes introducing viruses to the system or using the system as a base for further unauthorized activities on any other system. Poorly programmed or configured software is always prone to hacking or cracking. Application software is usually very similar and therefore become well known to an intruder. Default locations for key files are often accepted so that an intruder can easily find the locations and tamper with them. The homogeneity of services and programming for different software reduces the time required for a person to find and alter key areas on the system.

Software should have adequate security measures and it should be protected from computer viruses. Library should be able to get local support from the software company and should be able to access a secure master copy in case the copy in use is corrupted or lost. It can be avoided by taking backup copies of major software. All software and new files should be regularly checked by reputable anti-virus software. The system administrator should keep a software toolkit for troubleshooting.

6. Network Security

The increased reliance on computer networks has made security a major issue. ICT infrastructure and access tools should be protected from unauthorized access, interruption and manipulation. Libraries are using Local Area Networks (LAN) to share resources, peripheral devices such as printers and scanners, to store or archive files and to exchange files through e-mail, ftp, telnet, etc. Most libraries use CD-ROM networks using CD-Net server or CD-ROM tower for sharing electronic databases. Once computers are connected to a network, they become vulnerable. Public access networked computers like OPAC can be used for other purposes if adequate security measures are not implemented. As libraries are forming library networks and library consortia, it is very important to verify the contents and origin of digital resources. The library networks and consortia should be protected from unauthorized access by various techniques such as encryption, remote access regulations, etc. Sensitive information should be encrypted, authenticated by digital signature, time stamps, sequence numbers and digital certificates. Libraries should ensure security by setting devices like routers, firewalls, proxy servers, etc. A firewall is usually a combination of hardware and software which will inspect network traffic, and allow or deny the flow of traffic based on some sort of rule set.



Firewalls filter the traffic exchanged between networks, enforcing each network's access control policy. Often, a firewall defends an inside "trusted" network from attack by "untrusted" outsiders. Firewalls ensure that only authorized traffic passes into and out of each connected network. To avoid compromise, the firewall itself must be hardened against attack. To enable security policy design and verification, a firewall must also provide strong monitoring and logging.

7. Internet Security

Library networks connected to Internet is the greatest risk to the digital environment of libraries. Internet is a virtual library, which revolutionized the ways of accessing, organizing, managing, retrieving and dissemination information. It provides different types of tools/services/utilities for accessing electronic resources all over the world. Information is disseminated openly over the Internet. In many cases the parent organizations provide Internet connectivity to their libraries. Once connected to the Internet, libraries become vulnerable to outside attempt to break into the library systems. It can facilitate undesired access to internal systems, unless systems are appropriately designed and controlled. The open architecture of the Internet also makes it easy for system attacks to be launched against systems from anywhere in the world. Library Internet systems can even be accessed and then used to launch attacks against other systems. Confidential information that sends over the Internet could be viewed, intercepted, or stolen. Any information accessed, stored, retrieved or disseminated on a web server may be susceptible to compromise if proper security measures are not taken. If proper access controls are not maintained data integrity could also be compromised. Web servers and internal networks can be secured automatically by using software programs. These software are effective to check unauthorized access to the system. It is the responsibility of library to ensure that all data is maintained in its original or intended form.

8. Access Control

Only authorized users should have access to ICT resources. Usernames and passwords are the most common way of authenticating users and monitoring their access. Most of the library management software provides several levels of password access for different modules. A password should not be easy to guess and it should not be a nickname, common word, a film title, or a character in a film or in a book, birth date or popular work. The best passwords are at least eight characters in length and a mix of uppercase and lowercase characters, numbers, and special characters. It should be changed regularly. All vendor-supplied passwords should be changed. Usernames and passwords may be deactivated when they are not required. Library should have additional security measure for public access workstations. It should be monitored through passwords. It is a good practice to remove, hide or rename dangerous or unnecessary programs from such workstations. User privileges on public access workstations should be limited.

9. Protection Against Computer Viruses

Library professionals and users should work in accordance with safe computing practices to minimize the risks associated with computer viruses. A computer virus is a program, which disrupts the normal operations of a computer, leaving unwanted messages, erasing data, or scrambling a system's configuration. There are two major types of computer viruses, file infectors and boot sector infectors. File infectors are attached to executable programs. Boot sector infectors are restricted to diskettes, hard drives, and other storage media. These media contain a boot sector that holds specific information about the formatting of the storage medium and data stored there. When the boot sector program is read and executed, the virus goes into memory and infects the hard drive. A third type of virus, the hybrid, infects both sectors and files. An important feature of any virus is that it replicates itself, usually by attaching itself to program files. To prevent the spread of viruses, library staff should be made aware of the potential sources of infection. The best defense against viruses is running anti-virus programs. Computer system should have up-to-date anti-virus software that checks for virus and repair them. A good anti-virus program scans a system for files that match its database of known viruses, and will also watch for the generic symptoms of virus infection. It is a good idea to scan for viruses after transferring a file into a system. Scanning should take place before the transferred file is executed or used. All hardware and software should be scanned at periodic intervals. The anti-virus software should be updated regularly to ensure its effectiveness. If the anti-virus software detects a virus from an incoming file, inform the people who introduced that file so they can ensure it does not happen again.

10. OPAC

The Online Public Access Catalogue (OPAC) of library should be protected from misuse and abuse. It can be used for unauthorized access to the digital resources of the library. Physical risk of theft or damage of the public terminal, and risk of unauthorized access to resources outside the library are the major security issues associated with OPAC. It is very important to consider any accessible item to be subject of tampering, theft, damage, sabotage, etc.

11. Backup Information

Backing up electronic information, software and other important electronic documentation is a reliable security technique. An accident or a severe environmental condition may destroy these resources. Errors and omissions may occur during accessing, creating, processing, storing, managing, retrieving and transmitting data and information. If the information is destroyed or corrupted, there must be copies of the information that can be restored to the system. So it is very essential that backup copies should be readily available. Regular backups must be performed to ensure that no data are lost in the event of equipment failure. If files have not been backed up, the library may incur significant expense in time and money in recreating them. Backup information should have the same level of protection as the active files of this information. It should also be kept in a secure location physically separate to the one in which the computer system is located. It should not be kept near any magnetic fields, extreme heat or cold and should have adequate protection against fire and other physical hazards. Backup logs should be examined on a daily basis to check that backup has been completed satisfactorily. There should be written procedures outlining all aspects of backup procedures. Generally the system administrator is responsible for backups. It is very important that in addition to the system administrator one or two other professionals should know how to backup and access backed up information.

12. Professional Assignments and Security Training

All library professionals should be aware of their responsibility in relation to security. All major information related procedures should be documented so that important procedures can be followed when concerned library professionals are not available. More than one staff member should know important procedures. Library computer system should be assigned to a system administrator who is responsible for the maintenance and security of the system. Maintenance of digital information is very essential in order to avoid inevitable decay due to interaction with the environment. To be diligent about the security of the systems, library personnel with specific security related job descriptions are a necessity.

Libraries should give training to library professionals in security. Security awareness and education for library professionals and users are critical to good security practice. It is a preventive measure that helps users and library professionals to understand the benefits of security. Technical training in the form of emergency fire drills for library personnel can ensure that proper action will be taken to prevent such events from escalating into disasters. Security related magazines, mailing lists and newsgroups should be subscribed for more information, suggestions and warnings about security. A Network Security Administrator should be able to do the following jobs after proper training.

- ✍ Assimilate information gathered on the network and classify the criticality of the information. Reading documents and e-mails as they flow in the network.
- ✍ Sniff the network to capture network traffic. Put agents on the network to scrutinize and store all the network traffic logs.
- ✍ Assimilate clear text passwords. Collect passwords that can easily be read by any user on the network

- Deploy Snooping Agents – placing agents on network. Test and record current state of affairs inside the network through automated processes controlled by agents to analyze network devices and services offered;
- Identifying security lapses on the network based on the findings. Define the factor of risk associated with each lapse
- Identify open ports
- Identify various services running on the workstation
- Map the above services to the application used and user requirements
- Identify unnecessary services
- Search and identify configuration errors, which form potential Vulnerability
- Identify the patch level on various applications
- Run vulnerability assessment tools on the servers to find the Vulnerability
- Conduct manual vulnerability research
- Evaluate the vulnerability based on the potential of exploitation and impact

Based on these above findings, the Administrator should be able to give proper recommendation for Redesigning the Security Architecture, Redesign the Information security policies.

13. Conclusion

Digital networked environment of libraries should have adequate security. Security relates to the techniques, policies and strategies used to protect the availability, confidentiality and integrity of electronic information. Security includes personal security, physical security, software security, network security, Internet security, etc. Libraries need to have policies and protection measures in order to protect their ICT resources. Libraries should also have well-established backup policies. Public terminals like OPAC should be protected from the internal system with adequate security measures. Libraries should take necessary steps to safeguard their digital resources and access tools from various threats like damage, misuse, mistake, theft, sabotage, etc. Library professionals must be assigned security related tasks. Due to the explosive growth of Internet with various tools, which provide unprecedented access to digital information and resources ongoing diligence is required to keep the digital networked environment of library secure.

14. References

1. Brandt, D Scott. (1998) Insecurity on the net. Computer in Libraries : 34-37.
2. Breeding, Marshall., 1997 Designing secure library networks. Library Hi Tech 57-58 (15:1-2) : 11-20
3. Camp, Jean. (1999) Web security and privacy: an American perspective. The Information Society, 15 : 249-256.
4. Gladney, Henry M. (1997) Safeguarding digital library contents and users. D-Lib Magazine <http://www.dlib.org/dlib/june97/ibm/06gladney.html.> (Accessed on 22 th December 2000).
5. Lavagnino, Merri Beth. (1997) System security in the networked library. Library Hi Tech 57-58 (15:1-2) : 9-10.

6. Morgan, Eric Lease. (1998) Access control in libraries. Computer in Libraries : 38-39.

7. Rasmussen, Audrey. (2002) Desperately seeking security. Information Technology 11(3) : 14-23.

8. Schuyler, Michoel. (2002) A serious look at system security. Computers in Libraries : 36-39.

9. Vince, Judith. (1996) Information security- protecting your assets. Aslib Proceedings 48 (4) : 109-115.

About Authors

Mr. Manoj Kumar K working with INFLIBNET Centre as Scientist-D (Computer Science) after having more than 10 years of wide experience in the entire gamut of Information Technology which include 5 and half years of service in Indian Institute of Management, Kozhikode(IIMK) as an Officer in Computer Centre. Involved in setting up of state-of-the-art IT infrastructure in IIMK from scratch, which comprise of a multi layered architecture with File servers, Database servers, Web server, FTP server, Email server and other high-end servers/computers. He holds BSc from University of Calicut and MCA from Government Engineering College, Thiruvananthapuram. He has worked in Coal India Ltd, Ranchi, Bihar as Technical Secretary to Director(Finance) and CEDTI, Calicut as Asst Engineer. He has involved in setting up wireless LAN based on WiFi in e-journals lab and he is looking after training programmes such as DSpace workshop, Network Administration etc. for different kind of professionals including Librarians at INFLIBNET Centre. He has contributed number of papers in seminars and conferences.
Email : manoj@inflibnet.ac.in

Mr. Mohamed Haneefa K is Senior Research Fellow in DLISc at Calicut University, India. He holds BSc, MLISc, PGDCA and awarded JRF from UGC in 1999. He worked with NIT Calicut, IISR Calicut and Calicut University. He has published few research papers in professional journals and participated in many national and international conferences. His current research interests include application of ICT in libraries, library consortia and digital library.
E-mail: haneefcalicut@yahoo.com