Network Security Policy: A key to successful Network Management

By

Shweta Pandya

Librarian

GLS Institute of Business Management & Computer Technology

Ahmedabad.

E-mail: shwetapandya@yahoo.com

Bhaumik Shroff

Lecturer

GLS Institute of Computer Application

Ahmedabad

E-mail: shroffbhaumik@rediffmail.com

ABSTRACT

21st century is marked by spectacular and unprecedented developments in the field of telecommunication. The popularity of this field is gaining momentum, as it is faster, cost-effective and more efficient in resource sharing than any other communication media. Networks are the basis of telecommunication technology. The paper flashes on various aspects of network security and requirement of having sound security policy. The topic of network security policy is dealt with in detail, which is followed by the findings of the survey carried out by the authors. Some suggestions for developing security policy are given with the objective of helping the Library and Information Science professionals.

KEYWORDS: Network Security, System Architecture, Security Policy

0. INTRODUCTION

Though not the only source of loss and disruption, the misuse of computers and related IT equipments is a growing problem for the world costing a great deal of time and money. In fiscal 2001, India spent $13.02 billion

on its armed forces to keep the nation safe. In contrast, according to the US research outfit Computer Economics, the worldwide economic impact of malicious code attacks in 2001 was $13.2 billion!!![1] This gives an idea that increased reliance on IT and the growing adoption of the Internet as global network has made organizations vulnerable to the misuse or abuse of technology to a great extent. Research from IDC (Internet Data Center, Framingham, Mass.) expects the security services market to more than triple by 2005, with an average annual growth rate of 25 percent. [2] Such increased dependence of organizations in general and Library and Information Centers in particular on networks and other IT systems has led to a heightened awareness of the need to protect data, information and other network resources from disclosure to guarantee the authenticity of information and to protect systems from network-based attacks.

1. NETWORK SECURITY

Computer networks now play an important part in our everyday lives. This technological development has without doubt produced substantial benefits for all. However, alongside these benefits lies the disadvantage that computers and computer systems are vulnerable to all manner of misuse and the consequences of such misuse are very serious. Undoubtedly as IT products and systems become more common and easily accessible, they attract the unwelcome attention of the hackers, the terrorists and many other miscreants. The Librarians need not feel immune from such threats either! Indeed there is a very big danger in maintaining an attitude of “it can’t happen here”, because it displays too relaxed an attitude to security.

The terms network security and information security refer to information and services available on a network that cannot be accessed by unauthorized users. Security implies safety, including assurance of data integrity, freedom from unauthorized access of computational resources, freedom from snooping or wiretapping and freedom from disruption of service.

Providing security requires protecting both physical and abstract resources. Physical resources include computer resources and in a networked environment, it extends to cables, bridges, and routers etc that comprise the network infrastructure. Therefore, security threats are greater in the networked environment compared to a standalone computer system.

Protecting an abstract resource like information is usually more difficult than providing physical security and it encompasses many aspects of protection as explained below:

Data Integrity: A secure system must protect information from unauthorized alteration and destruction.

Data availability: The system must guarantee that outsiders cannot prevent legitimate access to information. For example, any outsider should not succeed in blocking Library and Information Centers’ users from accessing a website of that organization.

Confidentiality: The system must prevent outsiders from making copies of data as it passes across a network or understanding the contents if copies are made.

Authorization: Security for information usually needs to be more restrictive compared to physical security. For

instance, Library users should not have access to information other than Online Public Access Catalogue (OPAC) or a person working at circulation desk should not be able to modify the acquisition files or catalogue entries and the rights to modify such things should be with respective departments or in case of small libraries they should be with the librarian.

Authentication: The system must allow two communicating entities to validate each other's identity. An unauthorized outsider should not be able to insert counterfeit information into the system.

Replay avoidance: The system must prevent outsiders from capturing copies of information and using them later and must also prevent a retransmitted copy of the same information from being accepted.

The commonly identified potential threats to network security are internal attack, organizational attack, accidental security breach, automated computer attack, professional hackers, virus attack, etc. To protect the information from all these threats, having a sound information security becomes basic necessity especially for Library and Information Centers, as they are all the time dealing with information and which is the sole reason for their existence. No matter how secure the system is, it will have some weakness or the other. Therefore, it would be wise to have good security now than perfect security never. Security and usability are inversely proportional. As one adds more and more security features into a system, the more complex it gets and consequently, it becomes more restrictive and difficult to use. It is also true that security is only as strong as the weakest link. Studies reveal some common network security lapses as follows:

· It is observed that security threats and risks are generally not analyzed before implementing a network security.

· Most of network security policies lack in robustness.

· Poor implementation of physical security opens gate for easy physical access to data centers and critical IT assets of the Library and Information Centers.

· Weak passwords of user accounts can be guessed and cracked easily.

· Misconfigured servers and improper installations of operating systems and applications usually fail to prevent hacking.

· Lack of availability of data footprints is seen usually due to improper methodology in taking data backup.

· There is a lack of regular security audit of IT infrastructure and operations.

· Antivirus software is not periodically updated.

· Library and Information Centers usually do not conduct network security awareness programs for their employees as well as users.

2. NETWORK SECURITY POLICY

Policies are essential to any organization in order to ensure that daily decisions and actions are consistent with the organization's objectives, strategies and values. A policy is the statement or general understanding, which provides guidance in decision making to members of that organization in respect to any course of action. Having a

well-defined network security policy, which contains various policy statements to tackle network security issues, can alone ensure an effective system. The policy should outline the need and importance of the network security and explain what is allowed and what is not allowed. Security policies do not come in generic flavors. Once the needs are determined, the Library and Information Centers can start building on security policies that fit the specifics of that Library and Information Center. Security policies must address six foundational concepts ensuring confidentiality, integrity, availability, authorization, authentication, and reply avoidance to unauthorized user. With these in mind, it is logical to include other related matters in which user education is needed. Security policies can also focus on areas that may not seem to affect these security concepts directly, but are very important for the overall health of the organization. These include 'acceptable use' policies for the equipment, data, e-mail, Internet and others as needed. An organization wide security policy can be developed in four phases.[3]

2.1 Develop baseline system architecture

The first phase is of gathering information and developing understanding of the system architecture, which includes information regarding hardware, operating systems, database management systems, applications, network type or architecture and connectivity. The result is a complete diagram of the system at the functional level and description of all major functions of hardware and software resources. This information is critical in developing a security policy that can be integrated and implemented.

2.2 Review existing policies and procedures

To understand the requirements, examination of any existing security relevant polices, procedures and guidelines become essential. An existing document can become the starting point for the organization wide network security policy.

2.3 Assess protection requirement

Performing an accurate risk analysis is a vital step in securing networks. An automated risk assessment tools can be used to collect information regarding physical, administrative and technical security. This information can be used to evaluate and classify data types, storage location and transfer/access requirement. This process requires extensive interviews and analysis to determine what data resides where and who needs access to it.

2.4 Develop the document

The policy document must take into account all the data and issues, which have been collected and analyzed. A good security policy document should have a minimum of eight important topics to be addressed when it is laid down. They are purpose, related documents, cancellation, background, scope, policy statement, responsibility and action.

For policy to be enforceable, it needs to be

- Consistent with other Library and Information Centers' policies.
- Accepted by the network support staff as well as the appropriate levels of management.
- Enforceable using existing network equipments and procedures.
- Compliant with local, state and central laws.

3. GOOD NETWORK SECURITY POLICY

A network security policy is considered good if it fulfils certain criteria. It should:

Be readily accessible to all members of the organization.

Define a clear set of security goals.

Accurately define each issue discussed in the policy.

Clearly show the organization's position on each issue.

Describe the justification of the policy regarding each issue.

Include the organization's stance on issues not specifically defined.

Define under what circumstances the issues are applicable.

Define the user's expected level of privacy.

Spell out the consequences of noncompliance with the described policy.

Provide contact information for further details or clarification regarding the described issue.

State the roles and responsibilities of organizational members with regards to the described issue.

Thus, network security policy to be good should be clear, precise, flexible and transparent.

4. AWARENESS ABOUT NETWORK SECURITY POLICY AMONG THE LIBRARIANS AND OTHER INFORMATION PROFESSIONALS: A SURVEY

The threats to networked environment have now-a-days become more serious. Today's security challenge is to share information with the right people without also sharing it with the wrong people. As the time-honoured saying advises, prevention is always better than cure and having a sound network security policy is the first and most important step in preventing the computer and information misuse. Therefore, a sincere attempt is made to explore the awareness about this aspect among the library and information professionals and a survey was carried out, sample of which consisted of the librarians and information professionals of computerized libraries and information centers of Ahmedabad and Gandhinagar.

Keeping in mind the time availability and literacy level of the respondents, a questionnaire method was used to gather relevant data. Questionnaire was sent to 17 (seventeen) various libraries and information centers through post and e-mails and responses were received from all the centers.

5. DATA ANALYSIS AND FINDINGS

Data analysis has revealed some very striking facts regarding the awareness about network security policy in libraries and information centers. Some important ones are presented below.

· All esteemed respondents are familiar with the networked environment and 94 percent of them are working in LAN (Local Area Network) environment.

· All respondents firmly believe that security of information network is essential. But, it is quite surprising to note that very few have really taken appropriate actions to secure their servers and networks. Techniques used by respondents vary from very elementary and common devices like login with password, installation of antivirus software and restriction on use of personal FDs and CDs etc (41 % response), to the sophisticated and latest ones like Firewall, Proxy servers, TCPwrapper and DMZ security devices (47 % response).

· 29 percent respondents are still not aware about the concept of Network Security Policy and as many as 65 percent do not have a Network Security Policy for their Library or Information Center. However, all of them have shown interest in having it in the future.

· Major features of Network Security Policy are mentioned by those who already have such policy. They are, changing server administration password periodically, limiting access to different users, demand based traffic dimension to internal servers, restricted service access at various levels like server / router / firewall and providing limited ports open for external networks etc.

· Those who have Network Security Policy, implement it with the help of DMZ (demilitarized zone) and SSL (Secure Sockets Layer).

· Though 94 percent of the respondents are working in networked environment, 29 percent of them still do not have a qualified professional for administering their networks.

· Again, very few respondents are aware about the characteristics of a good network security policy. Some characteristics mentioned by respondents and relevant to the concept are flexibility, transparency, relevance, inclusion of physical as well as information security, clear specifications for audit, clear declaration of responsibility and continuous monitoring.

· 88 percent respondents believe that network security policy should be reviewed at regular interval. However, only 40 percent of them actually review it regularly.

· Keeping a network security policy document is very helpful in getting proper guidance as and when required. But it is rather strange that only 23 percent respondents document their network security policy.

· Only two respondents face difficulty in implementing the network security policy, especially in LAN management and creating awareness among the users. An attempt is made to overcome it by introducing user awareness programmes and updating knowledge and skills of the staff through proper training.

· It is clear from the responses that only two automated Libraries and Information Centers of Ahmedabad and Gandhinagar take help from network security providers. One of the major reasons for low response on this aspect could be that more than 40 percent of them are not even familiar with the network security providers. Days are not far when network security providers will become very popular and helpful to Library and Information professionals. Industries and business units have already started relying on network security providers for the solutions of their network related problems.

6. SUGGESTIONS

Whilst total security is unattainable and probably unworkable in service organizations, all possible steps should be taken to prevent or deter misuse and reduce the security risks. To have a sound security of network and a robust network security policy, a few suggestions in the light of the findings of the study are offered below. Library and information professionals:

· Should perform risk analysis regularly, use intrusion detection tools, analyses logs, be conscious of security breaches and take appropriate action because security is as strong as the weakest link.

· Should deploy security solutions depending on the risks involved.

· Should not depend on a single defense but should use multi-layered security.

· Should restrict network access by using firewall, prevent listener access, encrypt network traffic, make the operating system restrictive etc.

· Should install only the products that are of use.

· Should create an organization wide network security policy.

· Should clearly define goals, organization’s position on each issue and expected level of privacy and responsibilities in network security policy.

· Should perform periodic network security audits and take action on audit results.

· Should arrange user awareness programs regularly for internal as well as external users.

· Should keep an up to date document of the policy.

· Should have a well-defined disaster recovery plan ready.

· Should make the network security policy easily accessible to all members of the Library and Information Centers.

7. CONCLUSION

It is observed that not only automation and frequency of attacks are increasing but also attacking tools are becoming more sophisticated and attackers are discovering vulnerabilities more quickly. No system is foolproof and therefore, security should be proactive in which libraries and information centers must stay several steps

ahead of threatening forces. It is very hard to predict where future threats will come from! What separates secure environments from those most vulnerable is not the amount of money spent on security, it is the way in which that money is spent. The most sensible and cost-effective approach is to build an overarching security policy that involves people, processes and technology in a way that is well integrated with the overall objectives of the organization. Network security policy is thus, an essential element in the management of networks in the libraries and information centers and many potentially damaging situations can be avoided or alleviated by effective forward planning and good network security policies.

REFERENCES

Rana, Arjun S. “Security: A New Business Process”, *Network Computing*, 4,6, (June 2002), 14.

Grow, Kristine. “A Measure of Security”, *Exec*, 24,3, (2002), 7.

Raghudharan, Rakesh. “Corporate Security Policy Design”, *Network Magazine*, 2,3 (October 2001), 32-33.

Appendix I

Questionnaire

Name of the Library _____

Name of the Parent Organization _____

Address _____

_____

Contact No _____ (O) _____ (R) _____(M)

E-mail _____

Total number of books in the library _____

Number of periodicals subscribed to for the year 2002-03 _____

Other Resources _____

_____

Number of staff: Technical _____ Non-technical _____

Total number of users _____

Major Categories of users (1)

(2)

(3)

(4)

(5)

Please ticks mark the relevant choices.

(1) Are you familiar with networked library environment?

☐ ☐Yes No

(2) Do you work in networked environment?

☐ ☐ Yes No

If yes, what type of network environment you have been working with?

☐☐ ☐ LAN WAN MAN

(3) Is security of information network necessary?

☐ ☐Yes No

(4) What do you do to secure your networks?

(5) What do you do to secure your server?

(6) Are you aware about the concept of Network Security Policy?

☐ ☐ Yes No

(7) Do you have a Network Security Policy?

☐ ☐ Yes No

If yes, please mention the major features of your Network Security Policy.

If no, do you intend to have Network Security Policy in future?

☐ ☐ Yes No

(8) How do you implement your Network Security Policy?

(9) Please give the designation and qualifications of a person responsible for network administration in your organization?

(10) According to you, what should be the characteristics of a good Network Security Policy?

(11) Do you think, Network Security Policy should be reviewed and modified periodically?

☐ ☐ Yes No

(12) Do you regularly review your Network Security Policy?

☐ ☐ Yes No

(13) Do you keep Network Security Policy document?

☐ ☐ Yes No

(14) Do you find difficulties in enforcing Network Security Policy?

☐ Yes ☐ No

If yes, please specify them.

(15) What steps have you taken / are taking to overcome these difficulties?

(16) Are you familiar with Network Security Providers?

☐ Yes ☐ No

(17) Do you take help of any Network Security Providers?

☐ Yes ☐ No

If yes, please specify the name and contact details of your Network Security Provider.

You may please provide any other relevant information on the subject.

BRIEF BIOGRAPHY OF AUTHORS

Shweta Pandya is the Librarian of GLS Institute of Business Management and Computer Technology, Ahmedabad. She has B L I Sc and M L I Sc. M S University Baroda. She has two best paper presentation awards including ILA-A G Motiwale Award for Young LIS Professionals – 2001. She is also having a professional experience at the British Library Ahmedabad. She is currently pursuing studies in MBA.

Bhaumik Shroff **(MCA) is a Lecturer at GLS Institute of Computer Application, Ahmedabad. His research interests encompass Wireless Networks, Global System for Mobile (GSM), Short Message Service (SMS), Data Warehousing, Voice over IP, Wireless Application Protocol (WAP) etc. He received the first prize in research paper contest conducted by Computer Society of India in 2001.**