Leonardo Journal of Sciences Issue 13, July-December 2008
ISSN 1583-0233 p. 7-21

Network Security: Policies and Guidelines for Effective Network Management

Jonathan Gana KOLO, Umar Suleiman DAUDA

Department of Electrical and Computer Engineering, Federal University of Technology, Minna, Nigeria.

jgkolo@gmail.com, usdauda@gmail.com

Abstract

Network security and management in Information and Communication Technology (ICT) is the ability to maintain the integrity of a system or network, its data and its immediate environment. The various innovations and uses to which networks are being put are growing by the day and hence are becoming complex and invariably more difficult to manage by the day. Computers are found in every business such as banking, insurance, hospital, education, manufacturing, etc. The widespread use of these systems implies crime and insecurity on a global scale. In addition, the tremendous benefits brought about by Internet have also widened the scope of crime and insecurity at an alarming rate. Also, ICT has fast become a primary differentiator for institution/organization leaders as it offers effective and convenient means of interaction with each other across the globe. This upsurge in the population of organizations depending on ICT for business transaction has brought with it a growing number of security threats and attacks on poorly managed and secured networks primarily to steal personal data, particularly financial information and password.

This paper therefore proposes some policies and guidelines that should be followed by network administrators in organizations to help them ensure effective network management and security of ICT facilities and data.

Keyword

ICT; Security; Network; Management; IT; Hardware; Software; Access; Risk; Control; Asset; Resources; Data; Passwords; Hacker.

Introduction

We are living in an information engrossed world and the premium placed on information in this digital age has made it to become a precious and an invaluable commodity that all nations and groups of individuals across the globe are scrambling to get. Since information is now a precious and an indispensable commodity, the need to protect the data that are being transmitted becomes mandatory. Also, there are a growing number of security threats and attacks on networks primarily to steal personal data, particularly financial information and passwords. In addition, fraudulent network users may trade off their subscribers' password to a hacker for a fee. Network security and management in ICT is the ability to maintain the integrity of a system or network, its data and its immediate environment. This involves controlling access, regulating use and implementing contingency plans. It also involves the authorization and monitoring of access, investigation of unauthorized access and the protection of data, infrastructure and services. Breaches in security may be caused by human actions, which could be accidental, malicious or negligent, or through incorrect installation, configuration or operation.

Thus, in view of the above, to ensure effective management of an organization network, each department within the organization should be responsible for developing procedures to implement and enforce a security plan that includes the general organizational policies as well as any additional policies necessary to maintain the security of its Information Technology (IT) resources. The policies and guideline should reflect the standard and goals of the organization/institution and should address the problems of global networking and other new technologies.

This paper therefore presents policies and guidelines that should be followed to ensure effective management and security of any ICT network. The paper is written with the less experienced system administrator and information system manager in mind, to help them understand and deal with the risks they face daily on their networks.

This paper contributes to knowledge by suggesting policies and guidelines that must be implemented to solve the problems associated with poorly managed and secured networks.

These policies and guidelines are presented along the following major headings: IT security policies, organizational security, asset classification and control, personnel security, operation management and information management. These guidelines if implemented by the appropriate authorities will go a long way in alleviating problems of network insecurity.

IT Security Policy

IT security policies are the rules and practices that an institution uses to manage and protect its information resources. These policies must be developed, documented, implemented, reviewed and evaluated to ensure a properly managed and secured network. Hence, the need for IT security policies in any institution cannot be overemphasized.

Developing Security Policies

Developing security policies involves developing the following: Program policies, System-specific policies and Issue-specific policies [1], [2].

Program policies: addresses overall IT security goals and it should apply to all IT resources within an institution. The institution's president or an appointed representative must direct policy development to ensure that the policies address the IT security goals of all systems operating within the institution. For instance, program policies can address confidentiality or service availability. All program policies should meet the following criteria:

- Comply with existing laws, regulations, and state and federal policies.
- Support and enforce the institution's mission statement and organizational structure.

The components of an adequate program policy are defined in table 1.

System-specific policies: addresses the IT security issues and goals of a particular system. Large facilities may have multiple sets of system-specific policies that address all levels of security from the very general (access control rules) to the particular (system permissions that reflect the segregation of duties among a group of employees).

Issue-specific polices address particular IT security issues such as, Internet access, installation of unauthorized software or equipment, and sending/receiving e-mail attachments.

Once you have identified the IT security issues you need to address, develop issue-specific policies using the components defined in table 2

The guidelines for developing security policies are:

- Obtain a commitment from senior management to enforce security policies.
- Establish working relationships between departments, such as human resources, internal audit, facilities management, and budget and policy analysis.
- Establish an approval process to include legal and regulatory specialists, human resources specialists, and policy and procedure experts. Allow enough time for the review and respond to all comments whether you accept them or not.

Table 1. Component of an adequate program policy

Component	**Description**
Purpose Statement	Explains why the program is being established and what IT security goals it will address.
Scope	Define which IT resources are address by the program, such as hardware, software, data, personnel etc.
Assignment of responsibilities	Defines responsibilities for IT program management.
Compliance	Describe how the institution will develop and enforce the program. Also establish any disciplinary process for breaches of the program policy.

Documenting Security Policies

Once an institution has developed its IT security policies, all policies and procedures should be documented. Each department should protect its networks, critical information systems, and sensitive information from unauthorized disclosure, modification or destruction. Information security policies and procedures must be documented to ensure that integrity, confidentiality, accountability, and availability of information are not compromised. The documentation guideline for this security policy is summarized in table 3 [3].

Implementing Security Policies

Successful implementation of IT security policies requires security awareness at all levels of the organization. You can create awareness through widely disseminated documentation, newsletters, e-mail, a web site, training programs, and other notifications about security issues. Table 4 outlines the guidelines for implementing IT security policies:

Table 2. Issue Specific Policy

Component	Description
Issue statement	Identify the terms, definitions, and conditions pertinent to the issue. For instance, how do you define unauthorized software or acceptable Internet use? Include the rationale or justification for the policy.
Statement of the institution's position	Reflects management's decision on the policy. E.g. the use of unauthorized software is prohibited.
Applicability	Specifies where, how, when, to whom, and to what the policy applies.
Compliance	Defines who is responsible for enforcing the policy
Points of contact	Identifies resources for information and guidance.

Reviewing and Evaluating Policies

Institutions/organizations should review their security policies periodically to ensure they continue to fulfill the institutions security needs. Each department is also responsible for reviewing and evaluating the effectiveness of their policies and the accompanying procedures. After an institution/organization has developed IT security policies, the appointed security team will evaluate the policies and provide feedback.

Policy Review within the Institution

Each institution/organization should develop a plan to review and evaluate their IT security policies once they are in place. The guidelines are [2]:

Table 3. Documentation guideline for security policy

Guideline	Description
Define policies	Define policies by documenting the following information: • Identify general areas of risk. • State generally how to address the risk. • Provide a basis for verifying compliance through audits. • Outline implementation and enforcement plans. • Balance protection with productivity.
Define standards	Define IT security standards by documenting the following information: • Define minimum requirements designed to address certain risks. • Define specific requirements that ensure compliance with policies. • Provide a basis for verifying compliance through audits. • Outline implementation and enforcements plans. • Balance protection with productivity.
Define guidelines	Define IT security guidelines by documenting the following information: • Identify best practices to facilitate compliance • Provide additional background or other relevant information
Define enforcement	Define how policies will be enforced by documenting the following information: • Identify personnel who are authorized to review and investigate breaches of policy. • Identify the means to enforce policies.
Define exceptions	Define the possible exceptions to the IT security policies.

Table 4: Guidelines for implementing IT security policies

Guideline	Description
Create awareness	Create user awareness using the following methods: • Notify employees about the new security polices. • Update employees on the progress of new security policies. • Publish policy documentation electronically and on paper. • Develop descriptive security documentation for users. • Develop user-training sessions. • Require new users to sign a security acknowledgement.
Maintain awareness	Maintain user awareness of ongoing and new security issues using the following methods: • Web site • Posters • Newsletters • E-mail for comments, questions, and suggestions

- Assign responsibility for reviewing policies and procedures.
- Implement a reporting plan in which departments report security incidents to designated security personnel

- Implement regular reviews to evaluate the following:
  - Nature, number, and impact of recorded security incidents.
  - Cost and impact of controls on business efficiency, including third-party vendor compliance.
  - Effects of changes to organizations or technology.

Organizational Security

These are security measures that any organization should consider particularly when granting others access into its network. Each department in an institution/organization that develops, uses, or maintains information systems will also develop and maintain an internal information security infrastructure. An information security infrastructure protects an institution's information assets by defining assets and the necessary resources to protect them, and assigning responsibility for assets. This infrastructure must consist of information and programs that ensure the confidentiality, availability, accountability, and integrity of information assets. Institution must be able to identify the following for a viable security infrastructure [4]:

Managing Risks from Third-Party Access

Any institution that allows third party to access its IT resources should analyze the risk and develop security procedure to control access. The most significant risk in third-party access to many institution/organization IT resources is network-network connections that allows multiple users or systems from the third-party to interact with their system. Any department that allows third-party access to its information systems should conduct risk assessment and identify risk, and provide measures for checking this.

In other to manage risk from third-party, security awareness must be created and control access should be implemented.

Contracting with Third-Party Entities

Institution/organization as well as departments under them that allow third-party access to its information should address the security issues of that access and require the third-

party to adhere to all established security policies. Some of the guidelines that should be followed when contracting with a third party are: (1) Control access; (2) Protect asset; (3) Manage service; (4) Manage liabilities; (5) Ensure compliance; (6) Secure equipment; (7) Manage personnel.

Defining Security Requirement for Outsourcing Contract

Outsourcing agreements should address all IT security issues identified for the particular resources included in the contract.

Asset Classification and Control

Assets should be classified in order to determine which are sensitive or mission critical assets. This section contains guidelines for the following policies [1], [5]:

- Classifying assets
- Developing and maintaining an asset inventory
- Analyzing and assessing risk

Classifying Assets

Once an IT security plan have been developed, it is important to classify the information assets to determine which information systems, data, facilities, equipment, and personnel constitute the critical information infrastructure of the institution. The guidelines for classifying IT assets are outline in table 5.

Developing and Maintaining an Asset Inventory

An important component of IT security is establishing accountability for all IT resources. A documented asset inventory helps identify and assign responsibility for all resources. Asset inventories allow every institution and their departments to account for all purchases made with public funds. As items become out of date or no longer in use they should be removed from the inventory lists in accordance with institutional asset management procedures.

Analyzing and Assessing Risk

Once the critical IT assets have been identified, a risk analysis and assessment can help one to identify the vulnerabilities and risks associated with those assets.

Risk Analysis

Risk analysis is used to analyze the risk to critical IT assets by finding and documenting the vulnerabilities. A thorough analysis requires the assistance of experts in the hardware and software used at the institution. A risk analysis should analyze areas of control, critical asset elements, and areas of potential compromise [6].

Table 5. Guidelines for classifying IT assets

Guideline	**Description**
Organize assets	Organize assets into basic categories, such as: Data, Equipment, Hardware/software, Personnel, Facilities and Operations
Review relevant information	Review reports, databases, and documents with information about personnel, information and equipment.
Interview personnel	Interview personnel, such as managers, customers, suppliers, users, and others to help determine critical assets.
Conduct surveys	Develop survey questions to identify critical assets, such as: • What are the mission critical or sensitive activities and/or operations? • Where is critical or sensitive information stored or processed? • Where are the mission critical or high value equipment or material located (onsite or off)? • What kind of physical security, access control, and other protective measures are in place in these locations? • What impact would a lost or damaged asset have on critical mission functions, operations, and customers?
Identify interdependencies	Identify interdependencies among the components of individual systems and the overall infrastructure.
Classify assets	Classify assets based on your findings. Typically, the more goals an asset supports the more important it is.

Risk Assessment

Once you have identified the risks and vulnerabilities through a risk analysis, a risk assessment will help you determine which critical IT assets are most sensitive and at greatest risk. The cost of security enhancements typically exceeds available resources and the objective is to minimize the known vulnerabilities associated with the most critical IT assets. A risk assessment will help you prioritize IT security needs. A thorough risk assessment

should include the following questions [4]:

- Can vulnerability be better minimized with physical or IT measures?
- How much would it cost to minimize the risk posed by the vulnerability?
- Are the security enhancement costs commensurate with the asset's overall importance?
- What is the countermeasure's function: deter, detect, delay, or destroy?
- Is the effectiveness of the countermeasure related to time or events?
- Is the countermeasure effective institution-wide or for a specific area only?
- Do projected plans or anticipated developments suggest that the vulnerability is likely to become irrelevant in the near future?
- How long will it take to fully implement the proposed security enhancement?
- Will a proposed security enhancement be defeated by IT advances in the near future?

Personnel Security

This addresses the security issues that network administrator must deal with with respect to personnel. The following areas must be considered to ensure a complete Personnel Security as regards Information Network Security, and contains guidelines for proper execution.

Hiring new personnel

When hiring new personnel, IT departments should implement security procedures to minimize the risks of human error, fraud, and misuse of resources. Security concerns should be addressed as early as the recruitment stage. The guidelines that should be enforced when screening employees should encompass the following:

- Screening potential employee.
- Outline employee responsibilities.
- Evaluate the duties of new employees.

Ensuring appropriate use of technology

Institution's facilities should provide IT resources to authorized users to facilitate the efficient and effective performance to their duties. Authorization imposes certain

responsibilities and obligations on users and is subject to institution/organization policies and applicable laws. Users at all levels should be trained in the appropriate use of IT resources. The guidelines for ensuring appropriate use of technology are:

- Development of appropriate user policies.
- Enforcement of those policies.

Training users

Users of IT resources should be trained to make them to be aware of potential security concerned and to understand their responsibility to report security incident and vulnerabilities. The guidelines for training users are:

- Establish information access.
- Establish acceptable use of software.
- Establish accepted use of system.

Reporting security incidents and weaknesses

All users should be trained to report incidents and weaknesses in accordance with policy. The guidelines for this are as follows:

- Report incidence.
- Manage incidence.
- Collection and sharing IT information.
- Develop user awareness.
- Define user responsibilities.

Developing a disciplinary process

A disciplinary process ensures correct and fair treatment of users who breach security and may also deter users from disregarding security procedures. The guidelines for developing disciplinary policies are:

- Development of disciplinary process.
- Development of disciplinary process for third parties.

Operation Management

This section contains guidelines for the following policies:

- Developing network controls.
- Separating development and operational facilities.
- Securing external facilities management.

Developing network controls

Network controls ensure the security of information and connected services. To achieve and maintain security on computer networks a range of controls must be utilized. The common objective of these controls should be to protect all information and all connected service from unauthorized access. Security management of networks may span organizational boundaries and may involve protecting sensitive data passing over public networks. The guidelines for developing network controls include:

- Separate operational responsibilities for networks and computer operations where appropriate.
- Establish remote equipment management
- Establish special controls to protect data passing over public networks and connected systems.
- Use network management tools and procedures to ensure controls are consistently applied and services are optimized.

Separating Development and Operation Facilities

Separation of development, operation, and test systems reduces the risk of unauthorized changes or access. To operate properly, each type of computing system requires a known and stable environment. Guidelines for separating facilities are:

- Operate development and operational software on different computer processors, in different domains, or in different directories.
- Separate development and testing activities from production activities
- Prevent the access of software development utilities from operational systems, unless required.

- Avoid using the same log-on procedures, passwords, and display menus for both operational and test systems to reduce the risk of accidental log-on and other errors.
- Implement controls to ensure that administrative passwords for operational systems are closely monitored and controlled.
- Define and document the procedures for transferring software from development to operational status. Such transfers should require management approval.

Securing External Facilities Management

External facilities management introduces additional security risks that require special precautions. Specific risks should be identified in advance and appropriate controls should be agreed upon with the contractor. Guidelines for securing external facilities management are:

- Identify sensitive or critical applications that should be retained in-house.
- Obtain approval of business application owners to utilize external facilities.
- Consider business continuity plan implications.
- Specify security standards and compliance measurement processes.
- Implement procedures to effectively monitor all relevant security activities.
- Perform background checks and other techniques to screen vendor personnel and require confirmation that background checks have been successfully completed.
- Define responsibilities and procedures for reporting and handling security incidents.
- Define the security parameters for communications and data to the external site.

Information Management

This section contains guidelines for the following policies: Handling information & Disposing of media.

Handling Information

Electronically stored information should be protected from unauthorized access or misuse. Each department in an institution should establish internal procedures for the secure handling and storage of its electronically stored information to prevent unauthorized access or misuse. The guidelines for handling electronically stored information are:

- Develop procedures to invoice and manage the following:
  Documents, Computing systems, Networks, Mobile users, Postal services, E-mail, Voice mail, Voice communications, Fax machines, Multi-media and Other sensitive items
- Develop methods for handling and storing media.
- Develop access restrictions to identify unauthorized users.
- Maintain formal records of the recipients of data.
- Store media in accordance with manufacturer's specifications
- Restrict distribution of information.
- Indicate the authorized recipient of all copies of data.

Disposing of Media

To ensure the security of information, Institutions should develop procedures to render information unrecoverable before disposing of media. Each department should develop a media disposal process based on the sensitivity of the data as determined by law and the data owners. Guidelines for disposing of media are:

- Dispose of paper media
- Cleanse magnetic or optical media
- Develop disposal procedures

Conclusions

Once an institution has agreed upon on a set of security policies, then the procedure, plans, guidelines and standards that support those policies should be documented and disseminated to the appropriate managers and users. In addition, a back-up plan is necessary to ensure that essential stored data be recovered in the event of a system failure or disaster.

References

1. National Communications System, Public Switched Network Security Assessment Guidelines, National Communications System publication, 2000.

2. Swanson Marianne and Federal Computer Security Program Managers' Forum Working
3. Group, Guide for Developing Security Plans for Information Technology Systems, NIST Special Publication 800-18, 1998.
4. British Standard Institution, BS7799: A Code of Practice for Information Security, British ,Standard Publication, London.
5. Stoneburner, G. Risk Management Guide. Draft –Rev, NIST Special Publication ,800-30, 2001.
6. Information Systems Audit and Control Foundation, Control Objectives for Information and Related Technology (COBIT), 3rd Edition, July 2000.
7. Office of Information and Instructional Technology, Information Technology, 2003.
8. Security Guidelines. Gaithersburg, MD, National Institute of Standards and Technology.