Information and Computer Network Security Policy for Sudanese Telecom Companies

Mohamed Ibrahim Gali[1], Mudawi Al Musharaf[2], Abdelrahman Elsharif Karrar[3]

[1]The National Ribat University, Graduate Studies and Scientific Research, Khartoum, Sudan.

[2]College of Computer Studies, The National Ribat University

[3]College of Computer Science and Engineering, Taibah University

Abstract: ***As networks grow and evolve, the risk of coming under attack increases Network security polices represent a very important task for telecommunication companies. This policy will prevent any threat or intervention to companies' networks. This research tries to provide a recommendation for implementing a network security policy for Sudan Telecommunication Company. To achieve research goals the author explores different security policies that is implemented in a different environment and summarize the strength and weakness of each. This research consists of five chapters, chapter one is an introductory chapter, covers problem overview, objectives, research question, methodology, and work scope. Chapter two: Literature Review covers different issues regarding this research. Chapter Three: covers history of telecommunication in Sudan, security challenges to the Telecom networks, comparison of network security polices between international telecommunication and Sudanese telecommunication companies, and network security improvement. Chapter Four: detailed Design and Implementation, it went through computer and network policy, and change management. The research concluded (chapter five: Conclusion), by implementing a track system for any security threat and provided a new security policy that can work as a guideline for any telecommunication company.***

Keywords: Information Security, Security Policy, Scrutiny Management

1. Introduction

As networks grow and evolve, the risk of coming under attack increases. To help counter this threat, Cisco has developed the Cisco Self-Defending Network (SDN) strategy. To effectively implement this strategy an organization can leverage their comprehensive security policies.

To implement an effective security policy, you must understand why a network security policy is required, common attack-mitigation techniques, the parameters of a secure network life cycle model, and in the end, how to develop a comprehensive security policy. In the past, most closed off from public access, today's networks are more often than not "open," and they are now vulnerable to attacks from both the inside and the outside. In addition, as time has passed, hacker tools have become easily available, and the technical knowledge required to use such tools has decreased. This scenario creates quite a challenge for the e-business. A balance must be maintained between the need to open up a network to support the evolution of the business versus the need to protect business information.

A network security policy is necessary for a number of reasons, including new laws that require certain levels of protection, an increase in terrorist activity, and the increased risk of being hacked.

2. Problem Overview

The research problem in the Network Security Policy Purpose of this stage is to perform a security assessment of the current environment including an analysis of the major business processes, operating functions, organizational units and information systems and a thorough evaluation of the configuration and design of the existing network and systems infrastructure and main servers.

3. Objectives

1) Security assessment of the Telecommunication Industries in Sudan existing environment including an analysis of the major business processes, operating functions, organizational units and information systems (and major risks associated) and a thorough evaluation of the configuration and design of the existing network and systems infrastructure and main servers
2) Development of a security strategy encompassing security organization, security policy definition and security management process including recommendations on the methodology to be used for maintaining the security policy in a dynamically changing environment, as well as the related procedures, standards and controls for the effective roll out of the policy, and the approach in enhancing user awareness regarding security issues of Telecommunication Industries in Sudan.
3) Security architecture design including gap analysis based upon the results of the current state assessment and contrasted to the defined future state with a migration plan to meet policy requirements and further development of the organizational and technical security measures identified in the previous phase, including risk assessment of proposed policy and solution.

4. The Questions

1) How much networks security policies that currently implemented in Sudan are satisfying companies needs?

2) What kind of international standardizations can be injected into Sudan local security policies for the telecommunication Industries?
3) How plans and policies help develops secure networks and increase performance and control?

5. Telecommunications Network

A telecommunications network is a collection of terminal nodes, links are connected so as to enable telecommunication between the terminals.

The transmission links connect the nodes together. The nodes use circuit switching, message switching or packet switching to pass the signal through the correct links and nodes to reach the correct destination terminal.

Each terminal in the network usually has a unique address so messages or connections can be routed to the correct recipients. The collection of addresses in the network is called the address space. [Halsaal, F, 2006]

5.1 Examples of Telecommunications Networks

- Computer networks
- The internet
- The telephone network
- The global telex network
- The aeronautical acars network

6. Benefits of Telecommunications and Networking

Telecommunications can greatly increase and expand resources to all types of people. For example, businesses need a greater telecommunications network if they plan to expand their company. With Internet, computer, and telephone networks, businesses can allocate their resources efficiently. These core types of networks will be discussed below:

1) Computer Network

A computer network consists of computers and devices connected to one another. Information can be transferred from one device to the next. For example, an office filled with computers can share files together on each separate device. Computer networks can range from a local network area to a wide area network. The difference between the types of networks is the size. These types of computer networks work at certain speeds, also known as broadband. The Internet network connects computers worldwide. [Halsaal, F, 2006]

2) Internet Network

Access to the network allows users to use many resources. Over time the Internet network will replace books. This will enable users to discover information almost instantly and apply concepts to different situations. The Internet can be used for recreational, governmental, educational, and other purposes. Businesses in particular use the Internet network for research or to service customers and clients. [Halsaal, F, 2006]

3) Telephone Network

The telephone network connects people to one another. This network can be used in avariety of ways. Manybusinesses use the telephone network to route calls and/or service their customers. Some businesses use a telephone network on a greater scale through a private branch exchange. It is a system where a specific business focuses on routing and servicing calls for another business. Majority of the time, the telephone network is used around the world for recreational purposes. [Halsaal, F, 2006]

7. Secure Network Life Cycle

Here is a diagram that shows our secure network life cycle. At the center of this, of course, is our converged security policy, which dictates our IT governance, risk management, and compliance. There are five phases we're going to talk about here starting with the initiation phase, then the acquisition and development phase, followed by the implementation phase. Then step four is the operations and management phase, and then step five – the disposition phase. Each of these five phases has a kind of a minimum required set of steps that you have to effectively incorporate into your development system. And basically, in the context of IINS here, our system would be the network. [Lampson, B, 2005]

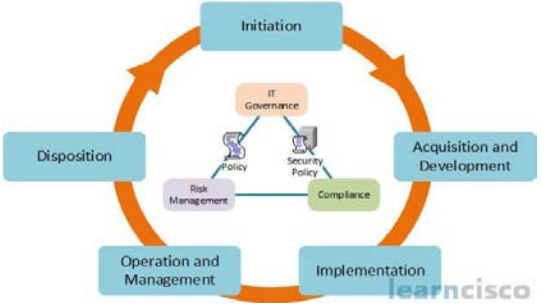

Figure 1: Secure Network life Cycle [Halsaal, F, 2006]

By framing security within the context of IT governance, compliance, and risk management, and by building it with a security sound architecture at its core, the result is usually a less expensive and more effective process. Including security early in the information process within the system design life cycle (SDLC) usually results in less-expensive and more-effective security when compared to adding it to an operational system.

A general SDLC includes five phases:
1) Initiation
2) Acquisition and development
3) Implementation
4) Operations and maintenance
5) Disposition

Each of these five phases includes a minimum set of security steps that you need to follow to effectively incorporate security into a system during its development. An organization either uses the general SDLC or develops a tailored SDLC that meets its specific needs. In either case, the National Institute of Standards and Technology (NIST) recommends that organizations incorporate the associated IT security steps of this general SDLC into their development process.

8. Models and Frameworks

The five-phase approach of the SDLC gives context to the process of designing, creating, and maintaining security architectures. It is based on NIST Publication 800-64 revision 2. Other frameworks and models exist, providing similar guidance to your security architecture:

- The ISO 27001 series is a comprehensive set of controls comprising best practices in information security. It is about information security, not IT security. It is also an internationally recognized information security standard, broad in scope and generic in applicability. It focuses on risk identification, assessment, and management. It is aligned with common business goals:
  - ○ Ensure business continuity
  - ○ Minimize business damage
  - ○ Maximize return on investments

  ISO 27000 standards are much more commonly applied in commercial organizations than in government. Originally created as BS17799, this framework was first submitted in 1995, and revised in 1998, but was not adopted by the ISO until 1999. Significantly revised in 2005, it was formally converted to two related ISO/International Electro technical Commission (ISO/IEC) standards, 27001 and 27002.
- Control Objectives for Information and Related Technology (COBIT) provides good practices across a domain and process framework and presents activities in a manageable and logical structure. The good practices provided by COBIT represent the consensus of experts. These good practices are strongly focused more on control and less on execution.
- These practices will help optimize IT-enabled investments, ensure service delivery, and provide a measure against which to judge when things do go wrong. COBIT is generally considered complementary to ISO/IEC 27001 and 27002.
- The Information Technology Infrastructure Library (ITIL) was developed under the supervision of the Central Computer and Telecommunications Agency in the UK. ITIL is a set of eight practice guidebooks covering most aspects of IT service management. The fourth service management set is Security Management. ITIL Security Management is based on the code of practice in ISO 27002.

Table 1: Comparison of Frameworks

Framework	*Strengths*	***Focus***
COBIT	IT controls IT metrics	IT governance Audit
ISO 27000 series	Global acceptance Certification Security control	Information security Management system
ITIL	Processes Certification	IT service management
NIST 800 series	Detailed, granular Tiered controls Available for free	Information systems FISMA (federal government)

frameworks. [Pieprzyk, J, 2007]

9. Computer and Network Security Policy in Sudanese Telecom Companies

Following are some of the very important security policy in Sudanese Companies covers the following issues:

Secure areas

a) Security Perimeter - Authorized Personnel Access to all companies work areas must be limited to those employees and partners whose jobs require entrance to those areas.

b) Physical Intrusion Alarms: All companieswork areas must be equipped with physical intrusion alarm systems that automatically alert those who can take immediate action.
- Fire Alarms
- Computer Room Doors

c) Physical Access: Physical access to companies highly secured areas is to be controlled with strong identification and authentication techniques. Staff authorized to enter such areas are to be provided with information security awareness on the potential security risks involved.
- Physical Access Tailgating
- Wearing Access Badges
- Physical Access Audit Trail

d) Visitor Identification Process: All visitors must provide official photo identification prior to gaining access to restricted companies work areas

e) Physical Security System Testing: The operation of all physical access control systems must be tested semi-annually.

f) Lockable Cupboards: Sensitive or valuable companies documents or equipment's must be stored securely and according to the classification status of the information being stored.

g) Secure Areas: Confidentiality Employees and partners who are authorized to access secure areas must not discuss the operations that occur within any secure area with any non-authorized person

h) Third Party Monitoring: Third-party services support personnel.

i) Base Stations SecurityAccess to all companiesbase stations must be controlled with strong identification and authentication techniques and should be restricted to the authorized personnel only.

Equipment Security

a) Fire RisksAll data and information must be protected against the risk of fire damage at all times. The level of such protection must always reflect the risk of fire and the value and classification of the information being safeguarded.

b) Preparing Premises to Site ElementsThe sites chosen to locate network elements, computers and to store data must be suitably protected from physical intrusion, theft, fire, flood, and other hazards.

c) Electronic EavesdroppingElectronic eavesdropping should be guarded against by using suitable detection mechanisms

d) Data CentersLocal management must provide and adequately maintain humidity control systems,

e) Smoking, Eating and Drinking in the Equipment Room Workers and visitors must not smoke, eat, or drink in the raised floor area at all companies equipment rooms.
f) Using Portable Devices companies personnel who are issued portable computer devices must be aware of the information security issues relating to these devices
g) Off-site Equipment – Unattended companies equipment that is taken off site must be never left unattended.
h) Release of Used Equipment and Media Before information systems equipment or storage media that has been used for companies business is provided to any third party,
i) Property Pass Computer peripherals, portable computers, modems, and related information systems equipment must accompanied by an approved property pass and must be inspected by the security personnel prior to leaving companies premises. Property pass logs must include the dates that the item was removed from and returned to companies.

10. Network Security Improvement

"Don't take risks with your company data. The data you collect can be just as valuable as the physical assets of your business". "You gauge and adjust your company's data security in order to successfully complete a middle-market business transaction"

4 Steps to Improve Network Security: [William Stallings,2008]

1. Establish and enforce a proven password strategy. Use fairly complex passwords and change those passwords at least every 90 days. Never use simple passwords like "Password01" or "Admin1." Microsoft-based network Active Directory will allow you to override the recommended password protocols. (If you are not required to change your password every quarter, this feature may have been turned off.)

2. Use a secure backup plan. This should already be a key part of your IT strategy. Secure backups help you survive everything from accidental file deletion to hurricane destruction. Those same backups can also help you survive cyber blackmail. If a cybercriminal threatens to delete your data, you can have it back online almost immediately using your backup system. As a best practice, backup datashould be stored in a secure, remote location away from your primary place of business. This protects your data from both physical and cyber threats**.**

3. Purchase some protection. There are numerous proven vendors that can provide firewalls, malware blocking, spam filtering, phishing blocking, virus protection, and intrusion detection software. These companies specialize in network protection and can provide data security that meets the needs and budgets of most businesses.

4. Create a security culture in your company
Ultimately, everyone who has a user name and password is responsible for keeping company data secure. Periodically remind your managers and employees that it is important to the company's future that they do not share log-in information. Encourage them to be more vigilant with securing their passwords. Writing passwords on a sticky note placed under a keyboard or in a file saved on a computer should be prohibited. Take internal data security protocols seriously. A 2013 Coreo study revealed that 43% of networks hacked were attacked using information criminals secured inside the company.

Don't take risks with your company data. The data you collect can be just as valuable as the physical assets of your business. Your company can't function efficiently or safely without it, and you definitely can't sell your business or secure growth capital without a secure data management plan in place. Just as you wouldn't leave the doors to your warehouse or office unlocked, you shouldn't leave the door open for cybercriminals either. Take steps to protect your data and your company's future today.

11. Recommendations

1) Security is everybody's business

- Collaboration in providing a good security policies is necessary
- Security needs to be designed in upfront
- Security must be an ongoing effort
- Systematically addressing vulnerabilities (intrinsic properties of networks/systems) is key so that protection can be provided independent of what the threats (which are constantly changing and may be unknown) may be

2) Scrutiny Management

- Centralize Malware Management
- Establish Boundary Control
- Implement Acceptable Use Policy
- Build Security into Applications Starting in the Design Phase
- Understand and implement all compliance and audit requirements
- Implement Monitoring and reporting processes
- Manage security deployment and infrastructure processes
- Implement network and host defenses
- Constantly validate network and system resource integrity

3) Data Security

- Understand who is accessing data via frequent auditing and real-time monitoring of data access
- Keep current records on data access permissions
- Classify data by sensitivity
- Minimize and remove global access rights
- Identify data owners and users
- Include data access reviews when individuals are transferred, promoted, or terminated
- Align groups to data ownership and management
- Audit permissions and group changes
- Lock down, delete or archive stale, unused data
- Clean up security groupings

4) Backup

- Restore desktops and mobile users quickly
- Restore systems to dissimilar hardware or virtual systems
- Back up data and system information to off site- -- locations, so that you can quickly recover your - -- - business even from a total loss of your facility
- Leverage new cloud based backup offerings to - - - properly secure, back up, and archive critical data

12. Strength and Weaknesses

1) Strength

- Follow the international standards in making a security polices.
- Introduce the use of computer aid in helping preventing any misuses and threats.

2) Weakness

- Some of security policy issues were not covered as it is out of research scope
- Real concern regarding the telecommunication staff industry of their abilities and motivations
- Shortages of technical training and technical abilities

3) Future Work

- Develop different applications for implementing and monitoring the network security within telecommunication and other industries
- Promote for establishing a security culture within any organizations employees

References

[1] A. Bonnaccorsi, "On the Relationship between Firm Size and Export Intensity," Journal of International Business Studies, XXIII(4),pp. 605-635, 1992. (journal style)

[2] R. Caves, Multinational Enterprise and Economic Analysis, Cambridge University Press, Cambridge, 1982. (book style)

[3] M. Clerc, "The Swarm and the Queen: Towards a Deterministic and Adaptive Particle Swarm Optimization," In Proceedings of the IEEE Congress on Evolutionary Computation (CEC), pp. 1951-1957, 1999. (conference style)

[4] H.H. Crokell, "Specialization and International Competitiveness," in Managing the Multinational Subsidiary, H. Etemad and L. S, Sulude (eds.), Croom-Helm, London, 1986. (book chapter style)

[5] K. Deb, S. Agrawal, A. Pratab, T. Meyarivan,"A Fast Elitist Non-dominated Sorting Genetic Algorithms for Multiobjective Optimization: NSGA II," KanGAL report 200001, Indian Institute of Technology, Kanpur, India, 2000. (technical report style)

[6] J. Geralds, "Sega Ends Production of Dreamcast," vnunet.com, para. 2, Jan. 31, 2001. [Online]. Available: http://nl1.vnunet.com/news/1116995. [Accessed: Sept. 12, 2004]. (General Internet site)

[7] Alvare, A, How Crakers Crack Passwords to Avoid, Proceedings, Security Workshop II, August 2000.

[8] Anderson, J, Computer Security Threat Monitoring and Surveillance, P.Anderson Co, 2002.

[9] Alexander, S, Password Protection for Modern Applications, login, 2004.

[10] Andrews, M., and Whittaker, J, Computer Security IEEE security and Privacy, 2004.

[11] Ante, S, and Grow, B, Meet the Hackers, 2006.

[12] Barker, W, Introduction to the Analysis of the Data Encryption Standard(DES), Aegean Park Press, 2001.

[13] Bhargava, B., and ed, Concurrency and Reliability in Distributed Systems, Van Nostrand-Reinhold, 2007.

[14] B Bhargava, B., and Helal, Efficient Reliability Mechanisms in Distributed Systems, CIKM 2003.

[15] Bray, O., Computer Integrated Manufacturing -The Data Management Strategy, Digital Press, 2008.

[16] Bellare, M, and Rogaway, P, Optimal Asymmetric Encryption, 2004.

[17] Bellare, M, Canetti, R Kilian, and Rogaway, The Security of the Cipher Block Chaining Message Authentication Code, 2002.

[18] Bishop, M, Computer Security, Boston, Addison-Wesley,2005.

[19] Boneh, D, Twenty years of Attacks on the RSA, Spring, 2002.

[20] Barkley, J, Comparing Simple Role-Based Access Control Models and Access Control Lists, Proceedings of the second ACM Workshop on Role-Based Access Control, 2009.

[21] Bhatti, R, Bertino, E, and Ghafoor, An Integrated Approach to Federated Identity and Privilege Management in Open Systems, ACM,2007.