Network Security - A tool for Network Governance

Author: **Dr.Anuradha Sarkar**
Associate Professor. Neville Wadia Institute of Management Studies and Research, Pune

Abstract:

As technology improves, firms are using IT as an essential part of their business. IT has helped business to be more efficient internally with various applications and infrastructure. It has also helped business externally by making it easier to conduct business through variousmethods such as the ability for clients to order products online. With these advances in IT,people's lives are made easier and firms are able to tap into markets that weren't available before.This convenience does come at a price though. Hackers and other cyber criminals look forweaknesses in a company's IT infrastructure and attack it in various ways. The effects of theseattacks could be harmless if the person does not do anything with the findings; however, if thecriminal uses the information that was obtained, the losses to the company could be tremendous.There can be internal threats as well. For example, a careless employee could accidentally leakcompany information to people who should not have access to the data. Much like externalthreats, internal ones could cause tremendous damage as well. That is why it is important tosecure a company's IT infrastructure from threats, both internal and external. The term 'security' has always been a priority but it has also gained special importance in the recent times both due to internal and external threats to organizations. Network Security is one such area which is of prime concern these days to the IT Professionals and needs to pay top attention to. This article defines Network Security, Analyses the need of Network Security, Root causes of analysis of Network problems, Network Security tools,Network Security checklist.

Key words: *Network Security, Network problems, Network Security checklist.*

Definition and Introduction

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.(*wikipedia.com*) Network security involves all activities that organizations, enterprises, and institutions undertake to protect the value and ongoing usability of assets and the integrity and continuity of operations. An effective network security strategy requires identifying threats and then choosing the most effective set of tools to combat them.

"Unprotected networks leak data both out of the network as well as into it."

Network security has become more important than ever in our lives as more andmore of our private and valuable information moves around on data networks.These data include not merely our financial information, as in the case of anonline order that includes a credit card number, but they also, increasingly, includemedical information that travels among doctors, hospitals, and insurance providers;and personal information that travels among friends and to or from our employers.It is clear that unprotected networks leak data both out of the network as well asinto it. It is no longer enough to protect data only at the computer and while instorage. We must protect data while in transit.

Business Benefits of Network Security?

An organization can experience many benefits if the networksecurity is in place. Likewise the company is protected against business disruption, which helps keep employees productive. Network

security helps your company meet mandatory regulatory compliance. Because network security helps protect your customers' data, it reduces the risk of legal action from data theft.
Hence ultimately, network security helps protect a business's reputation, which is one of its most important assets.(www.Cisco.com)

Why Network Security?
The need of network security has increased due to the following reasons:

- *To protect company assets:* One of the primary goals of computer and network security is the protection of company assets, which includes information, hardware and software computers and networks. Network security is concerned, with the protection, integrity, and availability of information.
- *To gain a competitive advantage:* Developing and maintaining effective security measures can provide an organization with a competitive advantage over its competition. Network security is particularly important in the arena of Internet financial services and e-commerce.
- *To comply with regulatory requirements and fiduciary responsibilities:* Corporate officers of every company have a responsibility to ensure the safety and soundness of the organization. Part of that responsibility includes ensuring the continuing operation of the organization. Accordingly, organizations that rely on computers for their continuing operation must develop policies and procedures that address organizational security requirements. Such policies and procedures are necessary not only to protect company assets but also to protect the organization from liability.
- *To keep your job:* Finally, to secure one's position within an organization and to ensure future career prospects, it is important to put into place measures that protect organizational assets. Security should be part of every network or systems administrator's job. Failure to perform adequately can result in termination. One thing to keep in mind is that network security costs money: It costs money to hire, train, and retain personnel; to buy hardware and software to secure an organization's networks; and to pay for the increased overhead and degraded network and system performance that resultsfrom firewalls, filters, and intrusion detection systems (IDSs). As a result, network security is not cheap.

Previous work and Studies :

It was estimated that 83 percent of threats faced by the Indian companies are because of internal security breach. Internal security breaches by employees constituted 43 percent, former employees (28 percent) and partner/supplier (12 percent). Of the companies, 42 percent suffered financial losses, while 35 percent suffered intellectual property losses. Keeping this in mind, enterprises today are taking special measures to ensure the physical safety of their employees and the safety of the IT systems to guarantee the smooth flow of business. The current economic environment has stirred enterprises to manage their expenses diligently and at the same time not compromise on securing their organization in any way.

According to the Frost &Sullivan(2009) survey done with CIOs across industries, 85 percent of the respondents believed that Viruses, Worms and Trojan Horses were the major disquiet in today's IT environment. Downtime and physical security were some of the other security concerns for CIOs."Enterprise security is no longer confined to external threats alone. Internal incidents of data loss are on the rise and enterprises need to seriously evaluate the impact such incidents will have on compliance, credibility and competition issues.

CIO study found that 90 percent of CIOs agreed that IT security is a vital component.

Root cause analysis of network problems

Network Security Audits is that organizations do not give required emphasis on proper house-keeping and regular health-check of their network and network devices. Often, you would find that there is no process defined for regular patch/OS upgrade for switches, routers, firewalls etc. or network administrators

do not visit vendors' Web site to check known vulnerabilities and upgrades. Some of the other causes are listed below:

- Unavailability of Network Design Guidelines
- Unavailability of Patch Management Process for Network Devices
- Absence of regular Health-Check schedule for devices

Commonly made Network Security Mistakes

Businesses use networking to connect their employees to one another and create a productive shared work environment. However, in their haste to get the network up and running, some businesses do not take the time to make sure all security measures are in place. Here are a few common network security mistakes.

Improper password use: Passwords are the simplest form of security. By leaving passwords blank or simple (i.e., *password* or *admin*), unauthorized users are practically invited to view sensitive data. Passwords are more secure when they contain both letters and numbers in a combination of upper-case and lower-case characters, and they should be changed periodically.

Lack of education: Educate users in the use of their software, especially with regard to e-mail, attachments, and downloads. They need to know exactly what kinds of threats are out there. Uneducated computer users are often those who fall victim to viruses, spyware, and phishing attacks, all of which are designed to corrupt systems or leak personal information to a third party without the user's consent.

No backups: Laziness is one of the biggest security threats. It's considerably more difficult to completely re-create a crippled system than it is to take the time to create proper backups. Create backups often, and do not immediately overwrite them with the next set of backups. In addition, make copies and keep them off-site in case of emergency.

Plug and surf: Unfortunately, computers are not designed to be connected to the Internet straight out of the box. Before a phone line, Ethernet cable, or wireless card is anywhere near a new computer, install a line of defensive software. Ideally, this should include virus protection, multiple spyware scanners, and a program that runs in the background to prevent malicious software from ever being installed.

Not updating: What good are all those virus and spyware scanners if they're not updated? It's crucial to update what are called the "virus/spyware definitions" every week. This keeps the scanners up-to-date to detect the latest malicious software.

Ignoring security patches: Security holes may exist in your operating system. No software is perfect. Once an imperfection or hole is found, it's usually exploited within a very short period of time. Therefore, it is imperative to install security patches as soon as possible.

Trust: Ads on the Internet have become devious and deceptive. They now appear as "urgent system messages" and warnings designed to scare users into clicking. As a rule of thumb, if a popup window contains an ad claiming to end popups, chances are it's a scam of some sort.

Not using encryption: Encryption is especially important when dealing with banking and credit cards. Storing and transferring unencrypted data is the equivalent of posting that data for everyone to see. If you're not comfortable implementing encryption technology, have an IT specialist assist you.

Trying to do it all yourself: Setting up a network, applying proper security measures, and downloading and installing software can be tricky. Large companies have IT departments. Small business owners should also ask for advice or even hire help. It's worth the extra cost.

Proper instruction: Security measures are most effective if everyone is aware of how the system operates. Give employees a brief overview of the security measures they're expected to follow.

Network security tools

Some of the Network Security tools which are commonly used by most of the businesses are listed below:

Antivirus software packages: These packages counter most virus threats if regularly updated and correctly maintained.

Secure network infrastructure: Switches and routers have hardware and software features that support secure connectivity, perimeter security, intrusion protection, identity services, and Security management.Dedicated network security hardware and software-Tools such as firewalls and intrusion detection systems provide protection for all areas of the network and enable secure connections.

Virtual private networks: These networks provide access control and data encryption between two different computers on a network. This allows remote workers to connect to the network without the risk of a hacker or thief intercepting data.

Identity services: These services help to identify users and control their activities and transactions on the network. Services include passwords, digital certificates, and digital authentication keys.

Encryption: Encryption ensures that messages cannot be intercepted or read by anyone other than the authorized recipient.

Security management: This is the glue that holds together the other building blocks of a strong security solution.

Network Security Checklist: Centuries ago, security professionals may have debated the merits of new technologies, like moats or drawbridges for example. Today, the equipment may have changed, but the debate remains the same.

Today, your network has become the castle; and instead of invading armies, the security professional is constantly besieged by school goers with downloaded cracker suites and thirty-year-old entrepreneurs looking to host a newly made site.

While 100% security is hardly a possibility, there are several things that you can do to make your network more secure.

- Ensure that your firewalls are up-to-date and properly configured.
- Ensure that virus protection is up-to-date.
- Maintain a security point of contact (POC)
- Is your data passing through an unsecured medium?
- Baseline your network.
- Ensure that OS and applications are properly patched.
- Utilize and configure an IDS.
- Secure the wireless network
- Consider your most dynamic security threat: human nature.

- SLA signed with vendors if network security is outsourced.

Conclusion: Security is a very intense need of any business. Everyorganisation has a different idea of what ``security'' is, and what levels of risk are acceptable. The key for building a secure network is todefine what security means to your organization . Once that has been defined, everything that goes on with the network can be evaluated with respect to that policy. This article has brought out a checklist that an organization could follow to ensure good governance of their networks and secure their businesses.

References

Textual:
Canavan John E(2001), Fundamentals of Network Security, London, www.artechhouse.com
CSI Survey 2007, Computer Security Institute.
Frost & Sullivan's South Asia Enterprise Security Summit 2009,Annual Executive MindXchange on Enterprise Security, Mumbai
Mallard Steve(2008), Computer and Network Security Research,www.brighthub.com
Payne Shirley C.,(2006), A Guide to security metrics , SANS Security Essentials GSEC Practical Assignment

Websites
www.cisco.com
www.cc.boun.edu.tr/network_security.html
www.expresscomputeronline.com
www.networkmagazine.com
http://searchnetworking.techtarget.com/tip/Network-security-checklist

******