How to develop a Network Security Policy?

1.1 Introduction

The world of computers has changed dramatically over the past 25 years. Twenty-five years ago, most computers were centralised and managed in data centres. Computers were kept in locked rooms and links outside a site were unusual. Computer security threats were rare, and were basically concerned with insiders These threats were well understood and dealt with using standard techniques: computers behind locked doors and accounting for all resources. Twenty-five years later, many systems are connected to the Internet. The Internet is a huge network and has no boundaries. Businesses find an increasing need to connect to the internet to take advantage of the business opportunities.

The security framework for systems with internet connections is however very different. Information on the internet can be accessed from anywhere in the world in real time. While this is good for the spread of information, it has also allowed for the proliferation of 'malicious information'. Hacker tools are now widely available on the internet. Some web sites even provides tutorials on how to hack into a system, giving details of the vulnerabilities of the different kinds of systems. It does not take an expert programmer to break into a system. Anyone with malicious intentions can search the internet for programs to break into a system which is not properly secured.

It is hence vital for businesses with connections to the internet to ensure that their networks are secure. This is important to minimise the risk of intrusions both from insiders and outsiders. Although a network cannot be 100% safe, a secure network will keep everyone but the most determined hacker out of the network. A network with a good accounting and auditing system will ensure that all activities are logged thereby enabling malicious activity to be detected.

1.2 Need for Network Security Policy

Before a network can be secured, a network security policy has to be established. A network security policy defines the organisation's expectations of proper computer and network use and the procedures to prevent and respond to security incidents. A network security policy is the foundation of security because it outlines what assets are worth protecting and what actions or inactions threaten the assets. The policy will weigh possible threats against the value of personal productivity and efficiency and identify the different corporate assets which need different levels of protection. Without a network security policy, a proper security framework cannot be established. Employees cannot refer to any established standards and security controls would be circumvented for the sake of increasing efficiency.

A network security policy should be communicated to everyone who uses the computer network, whether employee or contractor..

1.3 Risks of Network Connectivity

Before a network security policy can be established, a risk analysis has to be studied. Risk analysis is the process of identifying what you need to protect, what you need to protect it from, and how to protect it. It is the process of examining all of your risks, and ranking those risks by level of severity.

A good way of assessing the risks of network connectivity is to first evaluate the network to determine which assets are worth protecting and the extent to which these assets should be protected. In principle, the cost of protecting a particular asset should not be more than the asset itself. A detailed list of all assets, which include both tangible objects, such as servers and workstations, and intangible objects, such as software and data should be made. Directories that hold confidential or mission-critical files must be identified. After identifying the assets, a determination of how much it cost to replace each asset must be made to prioritise the list of assets.

Once the assets requiring protection are identified, it is necessary to identify the threats to these

assets. The threats can then be examined to determine what potential for loss exists. Examples of threats might include:

i) Unauthorised access/use of resources (authentication)
ii) Denial of Service (availability)
iii) Leakage of information (confidentiality)
iv) Corruption/unauthorised change of data (integrity)
v) Natural disasters

A thorough risk assessment will be the most valuable tool in shaping a network security policy. The risk assessment indicates both the most valuable and the most vulnerable assets. A security policy can then be established to focus on security measures that can identify these assets.

1.4 Components of a Network Security Policy

Although network security policies are subjective and can be very different for different organisations, there are certain issues that are relevant in most policies. This section explains some of the common components of a network security policy.

Physical Security

Network security interacts with physical security because the size or shape of the network "machine" or entity can span a building, campus, country or the world due to interconnections and trust relationships. Without physical security, the other issues of network security like confidentiality, availability and integrity will be greatly threatened. The physical security section states how facilities and hardware should be protected. This section will also define which employees should be granted access to restricted areas such as server rooms and wiring closets.

Network Security

The network security section states how assets stored on the network will be protected. This section might include security measures regarding access controls, firewalls, network auditing, remote access, directory services, Internet services, and file system directory structures.

Access Control

Access control determines who has access to what. There must be a proper procedure to ensure that only the right people have access to the right information or services. Good access control includes managing remote access and enabling administrators to be efficient in their work. It should not be so complex that it becomes easy to commit errors.

Authentication

Authentication is how users tell the network who they are. The type of authentication used varies depending on from where users are authenticating. From their desk, a simple user id and password may be sufficient because of the accompanying physical security. When connecting from the Internet, a more secure 2-factor authentication (token-based authentication) may be necessary.

Encryption

Encryption can ensure data integrity or protect sensitive information sent over insecure lines. Such protection is usually essential for remote access to important assets or as an extra protection when using the organisation’s intranet.

Key Management

Keys are used to encrypt and decrypt data. A serious issue with encryption is the management of keys. A proper policy has to be established to address the following issues as these will affect the effectiveness of using encryption.

i) Key length – how long
ii) Key change – how often
iii) Key escrow – to have or not, if yes, how

iv) Key generation – who, how
v) Key distribution – who how

Compliance

The compliance section explains how enforcement of the network security policy will be done. It might also state the methods that will be used to investigate breaches of the policy. Penalties on violations of the policy can also be state here.

Auditing and Review

Once a security policy has been implemented, it must be checked to ensure that all components and employees are in compliance. Without sufficient auditing, an organisation may have no legal recourse if there is a security breach. Auditing can also identify problems before they turn into security breaches. The policies must also be reviewed regularly to ensure that they are still relevant.

Security Awareness

"Clueless users" are widely recognised as the most serious threat to network security. If employees do not understand the power and proper use of the network, they can unintentionally compromise security (or be duped into it). In particular, employees must manage passwords properly and be aware of "social engineering" attacks.

Incident Response & Disaster Contingency Plan

An organisation is most vulnerable when it detects an intrusion or when it is faced with a disaster. What happens in the next few minutes and hours can determine if billions of dollars in intellectual property is recoverable. The disaster contingency plan explains how an organisation will recover from any type of natural disaster or attack, including attacks from hackers and employees. For example, it might include security measures for backing up servers, detailing how often backups must be performed and how backups must be stored off-site. The disaster contingency plan might also list the members of an emergency response team that will handle a natural disaster or attack. In addition, the plan might include security measures for conducting drills to ensure that all users and the emergency response team know what to do when a disaster or attack occurs.

Acceptable Use Policy

The acceptable use policy section states how users will be allowed to use network resources. For example, it might describe the types of information that can be included in Internet e-mail messages and explain when e-mail messages must be encrypted. This section might also address issues such as whether or not users can play computer games or use resources such as e-mail and Internet access for personal use.

Software Security

The software security section explains how the organisation will use commercial and non-commercial software on servers, workstations, and the network. This section might also identify who is allowed to purchase and install software and the security measures for downloading software from the Internet.

1.5 Steps to developing a Network Security Policy

Objective

Before starting work on the policy, a clear idea of the objectives of the policy must be defined. This will ensure that the policy does not stray from its initial objective. The objective defines the approach to network security. A typical objective might be that information is an important asset and that the organisation will implement security measures to protect that asset.

Scope

The scope defines the assets that will be protected by the network security policy. Network security

can cover a wide range of issues from physical security to personnel security to procedural security. A scope might define whether the policy addresses only network security or includes other areas of security. The scope also defines who must follow the network security policy. Does the policy pertain only to the employees? Or does the policy extend to contractors, customers, and vendors, who might be required to follow the policy if they connect their network to the organisation's network?

Support from upper management

After defining the scope and objectives. Support should be obtained from the upper-level managers before actual work on developing the policy. Without the support of upper management, it will be very difficult to ensure compliance of a network security policy. If possible, the security committee should also include some upper-level managers

Reference of Other Policies

In order to get a feel of how a network security policy should look like. References to other policies should be made. This will also help in redefining the scope and objectives of the policy.

Risk Assessment

Before starting the actual writing of the policy, a thorough risk assessment must be done. An assessment of the risks will determine what are the issues that need to be addressed. The risk assessment report will be valuable tool in the shaping of the network security policy.

Determination of Components and Writing of Policy

The components of the Security Policy should be determined. These will be dependent on the risk assessment report. Not all components must be included. These will depend on the network structure, the location and structure of the organisation. The policy should aim to address all the risks stated in the risk assessment report. Where certain risks cannot be address, they should be noted.

Evaluation

After the policy is developed, an evaluation of the policy should be done to ascertained if the objectives of the policy has been achieved.. Some of the questions to be addressed might include:

i) Does your policy comply with law and with duties to third parties?
ii) Does your policy compromise the interest of your employees, your organisation or third parties?
iii) Is your policy practical, workable and likely to be enforced?
iv) Does your policy address all the different forms of communication and record keeping within your organisation?
v) Has your policy been properly presented and agreed to by all concerned parties?

Real World Problem Cases Caused By Missing Policies

At A Government Agency...
A clerk spent a great deal of time surfing the Internet while on the job. Because there was no policy specifying what constituted excessive personal use, management could not discipline this employee. Then management discovered that the clerk had downloaded a great deal of pornography. Using this as a reason, management fired him. The clerk chose to appeal the termination with the Civil Service Board, claiming that he couldn't be fired because he had never been told that he couldn't

download pornography. After a Civil Service hearing, the Board ordered him to be reinstated with back pay.

At A Law Firm...
The manager of data processing took a job with a competing law firm. Because his former employer had nobody who could do the job that he did, they kept him on as a contractor. On a part-time basis, he would perform systems management tasks. In order to do these tasks he needed full privileges on the former employer's network. One day the former employer learned that the manager's new employer was opposing them in a high-visibility lawsuit. Could the former data processing manager gain access to the shared legal strategy files for this case on the network? The answer was yes, but nobody knew whether the manager had exploited these capabilities because no data access logs were being kept. This situation could have been avoided if the former employer had policies about conflicts of interest, system access privileges, and keeping logs.

At An Oil Company... An oil company computer technician compiled a list of jokes about sex. Proud of his list, he broadcast this list on the Internet, appending his electronic mail address to the end, just in case the recipients happened to have heard any new ones. Management was able to have the posting deleted from several discussion groups, but was not able to control copies that had been made. Around the same time the same technician had printed a copy of his list, and when distracted by something else, had left it in the hopper of a departmental printer. Women in the department objected that they had been subjected to sex jokes via email that they didn't want to hear. They pointed to the Internet postings and the printer output as examples. The pending sexual harassment lawsuit was settled for an undisclosed sum. A policy about permissible use of the Internet, as well as a policy about representations made using the company name on the Internet were noticeably lacking.

At A Local Newspaper...
A local newspaper had no policy requiring the termination of user-ID and password privileges after an employee left. A senior reporter left the newspaper, and shortly thereafter, the newspaper had trouble because the competition consistently picked-up on their exclusive stories (scoops). An investigation of the logs revealed that the former employee had been consistently accessing their computer to get ideas for stories at his new employer.

At A Midwest Manufacturing Company...
A virus hoax sent by email through the Internet indicated that if people receive a message with the heading "Join the Crew" they should not read it. The hoax went on to state that this email would erase a hard drive if ever it should be displayed. Thinking that they were doing others a favor, 10% of the staff at a large manufacturing company broadcast the hoax to all the people they knew. Because no policy defined how they should handle these warnings, they flooded the company's internal networks with email and caused a great deal of unnecessary technical staff time to be wasted.

At a West Coast Manufacturing Company...
Because it had no policy requiring employee private data to be encrypted when held in storage, a large manufacturing company found itself facing a public relations problem. A thief made off with a computer disk containing detailed personal details and bank account information on more than 20,000 current and former employees. The press speculated that this could be used to facilitate identity theft, including application for credit cards in the names of other people. The event precipitated a massive notification process including recommendations on changes to bank account numbers.

At a Major Online Service Company...
A Navy enlisted man registered with an Internet online service company and filled out a profile form which indicated that he was gay. An employee at the service company, after an inquiry from the Navy, shared this profile information with the Navy's "top brass." Based on this information, the enlisted man was given a dishonorable discharge. The enlisted man sued the Navy for violating its own "don't ask, don't tell" policy, and won an honorable discharge with retirement benefits as a result. The online service company publicly stated that its employee had violated "the Privacy & Security Policy," but this policy had been violated on multiple occasions before including top management's publicly stated intention to sell customer home telephone numbers to telephone marketers. At least the service firm now admits that it has a policy.

Sample Security Policy Outline

1. Introduction

1.1.1General Information
1.1.2 Objectives

1.2 Responsible Organizational Structure

1.2.1.1.1 Corporate Information Services
1.2.1.1.2 Business Unit Information Services
1.2.1.1.3 International Organizations
1.2.1.1.4 Tenants

1.2.2 Security Standards

1.2.2.1.1 Confidentiality
1.2.2.1.2 Integrity
1.2.2.1.3 Authorization
1.2.2.1.4 Access
1.2.2.1.5 Appropriate Use
1.2.2.1.6 Employee Privacy

2. Domain Services

2.1.1 Authentication
2.1.2 Password Standards
2.1.3 Resident Personnel Departure

2.1.3.1.1 Friendly Terms
2.1.3.1.2 Unfriendly Terms

3. Email Systems

3.1.1 Authentication
3.1.2 Intrusion Protection
3.1.3 Physical Access
3.1.4 Backups
3.1.5 Retention Policy
3.1.6 Auditing

4. WEB Servers

4.1.1 Internal
4.1.2 External

5. Data Center

5.1.1 Authentication
5.1.2 Intrusion Protection
5.1.3 Physical Access
5.1.4 Backups
5.1.5 Retention Policy
5.1.6 Auditing
5.1.7 Disaster Recovery

6. LAN/WAN

6.1.1 Authentication

6.1.2 Intrusion Protection
6.1.3 Physical Access

6.1.3.1.1 Modems
6.1.3.1.2 Dial-in Access
6.1.3.1.3 Dial-out

6.1.4 Backups
6.1.5 Retention Policy
6.1.6 Content Filtering
6.1.7 Auditing
6.1.8 Disaster Recovery

6.1.8.1.1 Network Operations Center
6.1.8.1.2 Physical Network Layer

7. Desktop Systems

7.1.1 Authentication
7.1.2 Intrusion Protection
7.1.3 Physical Access
7.1.4 Backups
7.1.5 Auditing
7.1.6 Disaster Recovery

8. Telecommunication Systems

8.1.1 Authentication
8.1.2 Intrusion Protection
8.1.3 Physical Access
8.1.4 Auditing
8.1.5 Backups
8.1.6 Retention Policy
8.1.7 Disaster Recovery

9. Strategic Servers

9.1.1 Authentication
9.1.2 Intrusion Protection
9.1.3 Physical Access
9.1.4 Backups
9.1.5 Retention Policy
9.1.6 Auditing
9.1.7 Disaster Recovery

10. Legacy Systems

10.1.1 Authentication

10.1.1.1.1 Password Standards

10.1.2 Intrusion Protection
10.1.3 Physical Access
10.1.4 Backups
10.1.5 Retention Policy
10.1.6 Auditing
10.1.7 Disaster Recovery

11. Security Services and Procedures

11.1 Auditing
11.2 Monitoring

12. Security Incident Handling

12.1 Preparing and Planning for Incident Handling
12.2 Notification and Points of Contact
12.3 Identifying an Incident
12.4 Handling an Incident
12.5 Aftermath of an Incident
12.6 Forensics and Legal Implications
12.7 Public Relations Contacts
12.8 Key Steps

12.8.1.1.1 Containment
12.8.1.1.2 Eradication
12.8.1.1.3 Recovery
12.8.1.1.4 Follow-Up
12.8.1.1.5 Aftermath / Lessons Learned

12.9 Responsibilities

13. Ongoing Activities

13.1.1 Incident Warnings

13.1.1.1.1 Virus warnings
13.1.1.1.2 Intrusion Vulnerabilities
13.1.1.1.3 Security Patches

14. Contacts, Mailing Lists and Other Resources

15. References