Chapter 5

STEPS TO TAKE NOW

INTRODUCTION

In today's environment of severely constrained resources (both staffing and financial) investments in security controls must show a positive return on investment. Internet security can be looked as an enabling investment, reducing operational costs or opening new revenue streams, or as a protective investment, preventing potential costs or negative business impacts. In either case, the cost of the security controls must be appropriate for the risk and reward environment faced by your enterprise [1].

In simple terms, a risk is realized when a threat takes advantage of a vulnerability to cause harm to your system. Security policy provides the baseline for implementing security controls to reduce vulnerabilities and reduce risk. In order to develop cost effective security policy for protecting Internet connections some level of risk analysis must be performed to determine the required rigor of the policy, which will drive the cost of the security controls deployed to meet the requirements of the security policy. How rigorous this effort must be is a factor of:

- The level of threat an enterprise faces and the visibility of the enterprise to the outside world
- The sensitivity of the enterprise to the consequences of potential security incidents
- Legal and regulatory issues that may dictate formal levels of risk analysis [1]

> **Note:** This does not address the value of information or the cost of security incidents. In the past, such cost estimation has been required as a part of formal risk analyses in an attempt to support measurements of the ROI of security expenditures. As dependence on public networks by enterprises and government agencies has become more widespread, the intangible costs of security incidents equal or outweigh the measurable costs. Information security management time can be more effectively spent assuring the deployment of good enough security rather than attempting to calculate the cost of anything less than perfect security.

For enterprises that are subject to regulatory oversight, or that handle life-critical information, more formal methods of risk assessment may be appropriate. This chapter

provides a methodology for the steps you must take now to rapidly develop a risk profile for your enterprise; and, the enterprise requirements you must adhere to in developing an Internet security policy [1].

THREATS/VISIBILITY

A threat is any circumstance or event with the potential to cause harm to an enterprise through the disclosure, modification or destruction of information, or by the denial of critical services. Threats can be non-malicious, through human error, hardware/software failures, or natural disaster. Malicious threats can be categorized within a range going from rational (obtaining something of value at no cost) to irrational (destroying the information or reputation of others). Typical threats in an Internet environment include:

- Component Failure: Failure due to design flaws or hardware/software faults can lead to denial of service or security compromises through the malfunction of a system component. Downtime of a firewall [2] or false rejections by authorization servers are examples of failures that affect security.
- Information Browsing: Unauthorized viewing of sensitive information by intruders or legitimate users may occur through a variety of mechanisms: mis-routed electronic mail, printer output, mis-configured access control lists, group IDs, etc.
- Misuse: The use of information assets for other than authorized purposes can result in denial of service, increased cost, or damage to reputations. Internal or external users can initiate misuse.
- Unauthorized deletion, modification or disclosure of information: Intentional damage to information assets that result in the loss of integrity or confidentiality of enterprise functions and information.
- Penetration: Attacks by unauthorized persons or systems that may result in denial of service or significant increases in incident handling costs.
- Misrepresentation: Attempts to masquerade as a legitimate user to steal services or information, or to initiate transactions that result in financial loss or embarrassment to the organization. The presence of a threat does not mean that it will necessarily cause actual harm. To become a risk, a threat must take advantage of a vulnerability in system security controls (discussed later in the chapter) and the system must be visible to the outside world. Visibility is a measure of both the attractiveness of a system to malicious intruders and of the amount of information available in the public domain about that system [1].

All enterprises with Internet access are to some extent visible to the outside world, if by nothing more than through Domain Name Services. However, some enterprises are more visible than others are, and the level of visibility may change regularly or due to extraordinary events. The Internal Revenue Service is much more visible than the Migratory Bird Management Office, and the IRS is particularly visible as April 15th nears. Exxon became much more visible after the Valdez disaster and various other oil spill accidents, while MFS became much less visible after being acquired by Worldcom [1].