3 Risk Profiling

In today's environment of severely constrained resources (both staffing and financial) investments in security controls must show a positive return on investment. Information 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 organization.

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 organization faces and the visibility of the organization to the outside world
- The sensitivity of the organization to the consequences of potential security incidents
- Legal and regulatory issues that may dictate formal levels of risk analysis

Note that 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 businesses 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 organizations that are subject to regulatory oversight, or that handle life-critical information, more formal methods of risk assessment may be appropriate. Sources of information on risk assessment methods are listed in the Resources section of this document. The following sections provide a methodology for rapidly developing a risk profile for your organization.

3.1 Threats/Visibility

A threat is any circumstance or event with the potential to cause harm to an organization 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 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 business 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 in the following section) and the system must be visible to the outside world. Visibility is a measure both of the attractiveness of a system to malicious intruders and of the amount of information available in the public domain about that system.

All organizations with Internet access are to some extent “visible” to the outside world, if by nothing more than through Domain Name Services. However, some organizations 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, while MFS became much less visible after being acquired by Worldcom.

Since many Internet-based threats are opportunistic in nature, an organization’s level of visibility directly drives the probability that a malicious “actor” will attempt to cause harm by realizing a threat. In the Internet environment, curious college students, teenage vandals, criminals, agents of espionage, or curious cyber-surfers can carry out threats. As the use of public networks for electronic commerce and critical business functions increases, attacks by criminals and espionage agents (both economic and foreign) will increase.

3.2 Sensitivities/Consequences

Organizations have different levels of sensitivity to risk. Security policy needs to reflect the organization's particular sensitivity to various types of security incidents and prioritize security investments on those areas of highest sensitivity.

There are two major factors that drive an organization's level of sensitivity. The first factor is the consequences of a security incident. Almost all organizations have some level of cost sensitivity - security incidents can result in significant recovery and restoration costs even if no critical services are affected. However, means of transferring risk (such as insurance policies or contractual terms and conditions) may mean that a certain level of cost exposure does not change the business financial bottom line.

One important step towards determining the consequences is performing an information asset inventory, discussed in more detail in section 5.6.3. While it sounds simple, keeping an accurate inventory of what systems, networks, computers, and databases are currently in use is a complex task. Organizations should combine such an inventory with a data classification effort, discussed in section 5.6.4, where the information stored on line is categorized by its importance to the goals of the business or mission.

More serious consequences occur when internal functions are disrupted, resulting in costs of missed opportunities, personnel down time, as well as recovery and restoration. The most serious consequences are when external functions are effected, such as delivery of products to customers or receipt of orders. These consequences are related directly to the financial impact of a security incident through disruption of services, or to a potential future impact due to loss of customer trust.

The second factor to consider is more a function of political or organizational sensitivities. In some corporate cultures upper level management may feel that an article in the mainstream press highlighting a break-in at your agency or business is a major disaster, whether or not there are significant costs involved. In more open environments, such as universities and scientific research communities, management may feel that an occasional incident is preferable to any restriction on the flow of information or outside access. These factors need to be considered when determining organizational sensitivity to security incidents.

3.3 Profile Matrix

Table 3.1 Risk Profile Matrix

Risk Profiling Matrix				
Threats:	Rating	Visibility	Rating	Score
None identified as active; exposure is limited	1	Very low profile, no active publicity	1	
Unknown state or multiple exposures	3	Middle of the pack, periodic publicity	3	
Active threats, multiple exposures	5	Lightning rod, active publicity	5	

Risk Profiling Matrix				
Threats:	Rating	Visibility	Rating	Score
Consequences	Rating	Sensitivity	Rating	Score
No cost impact; well within planned budget; risk transferred	1	Accepted as cost of doing business; no organization issues	1	
Internal functions impacted; budget overrun; opportunity costs	3	Unacceptable Business Unit management impact; good will costs	3	
External functions impacted; direct revenue hit	5	Unacceptable Corporate Management impact; business relationships affected	5	
	Total Score:			

Rating: Multiply Threat rating by Visibility rating, and Consequences rating by Sensitivity rating. Add the two values together:

- 2 - 10: Low Risk
- 11 - 29: Medium Risk
- 30 - 50: High Risk

3.4 Information Asset Inventory

To assure protection of all information assets and so that the current computing environment may be quickly re-established following a disaster, each Network Administrator must maintain an inventory of production information systems. This inventory must indicate all existing hardware, software, automated files, databases and data communications links.

For each information asset, the following information should be defined:

- Type: hardware, software, data
- General Support System or Critical Application
- Designated “owner” of the information
- Physical or logical location
- Inventory item number, where applicable.

3.5 General Support Systems

A general support system is “an interconnected set of information resources under the same direct management control which shares common functionality.” Normally, the purpose of a general support system is to provide processing or communications

support across a wide array of applications. General support systems consist of all computers, networks, and programs that support multiple applications, and are usually managed and maintained by a central IRM or ADP organization.

Security policy for general support systems is generally the most applicable to Internet usage, as the servers, communications software, and gateways that provide Internet connectivity are generally centrally controlled.

3.6 Critical/Major Applications

All applications require some level of security, and adequate security for most of them should be provided by security of the general support systems in which they operate. However, certain applications, because of the nature of the information in them, require special management oversight and should be treated as major. A major or critical application is any use of computers or networks that would seriously impact the ability of the organization to perform its mission if that application was altered or unavailable.

Examples of critical applications are personnel systems, billing systems, financial or billing systems, etc. Since most users spend the majority of their computer time interacting with one of these major applications, security awareness and education should be integrated into the training and documentation for these systems.

Most major applications do not currently involve Internet connectivity; however, this is beginning to change. Next generation operating systems are incorporating Internet connectivity, as are groupware and publishing software programs.

3.7 Data Categorization

In order to develop effective information security policy, the information produced or processed by an organization must be categorized according to its sensitivity to loss or disclosure. Based on this categorization, policy for allowing Internet access to information or for transmitting information over the Internet can be defined.

Most organizations use some set of information categories, such as “Proprietary,” “For Internal Use Only,” or “Company Sensitive.” The categories used in the information security policy should be consistent with any existing categories.

Data must be broken into four sensitivity classifications with separate handling requirements: SENSITIVE, CONFIDENTIAL, PRIVATE, and PUBLIC. This standard data sensitivity classification system must be used throughout COMPANY. The designated owners of information are responsible for determining data classification levels, subject to executive management review. These classifications are defined as follows:

- SENSITIVE: This classification applies to information that requires special precautions to assure the integrity of the information, by protecting it from unauthorized modification or deletion. It is information that requires a higher than normal assurance of accuracy and completeness. Examples of

sensitive information include COMPANY financial transactions and regulatory actions.

- CONFIDENTIAL: This classification applies to the most sensitive business information that is intended strictly for use within COMPANY. This information is exempt from disclosure under the provisions of the Freedom of Information Act or other applicable federal laws or regulations. Its unauthorized disclosure could seriously and adversely impact COMPANY, its stockholders, its business partners, and/or its customers. Health care-related information should be considered at least CONFIDENTIAL.

- PRIVATE: This classification applies to personal information that is intended for use within COMPANY. Its unauthorized disclosure could seriously and adversely impact COMPANY and/or its employees.

- PUBLIC: This classification applies to all other information that does not clearly fit into any of the above three classifications. While its unauthorized disclosure is against policy, it is not expected to impact seriously or adversely COMPANY, its employees, and/or its customers.