849 International Drive
Suite 450
Linthicum , MD 21090
410-981-6000
410-691-1506 (FAX)

www.silentrunner.com

White Paper

RISK MANAGEMENT AND SECURITY

Analysis of the Risk Assessment Process

Raytheon

Copyright Raytheon Company – SilentRunner®

RISK MANAGEMENT AND SECURITY

Risk management has reached a new level of importance in the information age. The growth of networked information systems and distributed computing has created a potentially dangerous environment. From trade secrets, proprietary information, sensitive medical records and financial transactions, critically important data flows through these systems. Independent reports, such as the recently published FBI/CSI Computer Crime Survey, detail the losses that have been sustained by information systems. The theft of proprietary information is up from $66B in ’00 to over $151B in ’01, with the average loss increasing from just over $1M per occurrence to $2.8M per occurrence. Financial Fraud is up from $56B to over $92B, or from $172M per incident to over $453M. With losses of this magnitude, organizations are becoming increasingly concerned with their potential exposure and looking for ways to evaluate their organization’s security profile.

To be effective, security organizations within companies will have to be data-driven, technology-based and decentralized. Security, which has often been administered as more of an art than a science, will have to be quantified and measured. Measurement tools of a security program are the risk assessment and audit, and the Return on Investment (ROI) associated with risk mitigation.

In the past five years, the use of tools such as intrusion detection monitors, virus detection software, firewalls, and other combinations of hardware, software, and firmware, have been used to control the attacks that may come from the outside on an organization’s information assets. Unfortunately, the controls, monitoring and policies related to how insiders access systems have not been as comprehensive. As a result, there are numerous reports of employees doing everything from selling government secrets to foreign governments, to using company secrets for their own financial gain, to browsing an ex-spouse’s medical records, or tax returns.

ELEMENTS OF RISK ASSESSMENT

The formal, quantitative risk assessment is the foundation and starting point of a good risk management program. The risk assessment process is a method of determining what kinds of controls are needed to protect an organization’s information systems and other assets and resources not just adequately, but cost-effectively. Basically, the assessment identifies risks, recommends steps to mitigate the risks, analyses the cost associated with that mitigation and correlates this information to determine feasibility.

The risk assessment process analyses a set of five variables, and comes up with recommended actions based on the relationships of these variables to each other. First, what are you trying to

protect, how much is it worth, and how much depends on it. Second, what could potentially threaten the asset. Third, what weakness exists that would allow the threat to materialize. Fourth, if the threat occurs, what kind of loss could be sustained? And, fifth, what controls could you put into place that would reduce the loss if a threat occurred, or eliminate the threat altogether.

The five variables include:

- *ASSETS* - whatever you're trying to protect.

- *THREATS* - events which could occur, and cannot ever be completely eliminated, although you can reduce the likelihood of occurrence, or mitigate its impact .

- *VULNERABILITIES* - weaknesses in the organization which would create a condition which would allow the threat to materialize, triggering a data loss or misuse.

- *LOSSES* - Loss categories include direct loss, disclosure losses, loss of data integrity, losses due to data modification, losses due to delays and denials of service, loss of reputation, etc.

- *SAFEGUARDS* - security controls which, when put in place, can eliminate, reduce or mitigate the impact of a threat occurrence.

RISK ASSESSMENT METHODOLOGY

Risk assessment is composed of two parts, the vulnerability assessment and the countermeasure (safeguard) assessment. The vulnerability assessment looks at existing systems and evaluates existing usage for possible security loopholes. Information must also be obtained on how personnel are complying with existing policies and guidelines. The result of the vulnerability assessment will present a detailed road map of all the existing weaknesses, including information of how widespread any problem is, and which individuals contribute to the vulnerability.

The Vulnerability Assessment

Vulnerability assessment is a key component of the risk assessment. Technical vulnerability assessments give very micro-level details about the weaknesses in the configuration and use of a network. Vulnerability data is then matched to see what combination of Asset/Threat/Vulnerability could trigger a loss, and then deciding what safeguards might be put in place to reduce or eliminate the

potential loss. By discovering network systems, identifying actual users and usage, and obtaining benchmark and trend information, SilentRunner can be a key data source for the technical vulnerability assessment.

The Technical Vulnerability Assessment

Technical vulnerability assessments use discovery tools to survey the actual network and report the technical weaknesses that are discovered. A product, such as SilentRunner, uses passive analysis to identify security vulnerabilities, which will provide efficiency in vulnerability identification and reduce false positive results of some network devices. These technical assessments can differentiate between infrastructure devices (such as routers, and firewalls) and host devices (user workstations or servers, such as-mail or Web servers.)

Technical discovery, analysis and visualization tools can readily find vulnerabilities in network TCP/IP hosts, Intranet web servers, mail servers, FTP servers, as well as firewalls and intrusion detection systems. At a very high level, the vulnerability assessment will analyze and summarize the results of the all the weaknesses, which were discovered, in the systems under review.

The Cost Benefit Analysis - Establishing Return on Investment (ROI)

The cost benefit analysis combines information from the vulnerability assessment along with relevant threat data and asset information such as present day replacement values, criticality, integrity and availability of the information contained in the system under review, as well as how completely safeguards are currently being implemented. The result of the cost benefit analysis will be to create a return on investment ratio (ROI), balancing the value of the information against the cost of controls to protect it. By establishing Return On Investment data, managers and directors can make more informed decisions regarding which controls to implement based on the current threat exposure of the organization.

This financial analysis, a built-in component of the risk assessment, is increasingly attractive to top-level management in private industry, as well as government agencies. Board members and shareholders want quantitative numbers to use in assessing the required security level of an organization and making the resultant management recommendations.

AUTOMATING THE RISK MANAGEMENT PROCESS

The new emphasis on the need for risk management is causing heightened interest in automated risk analysis software tools, which can reduce the time involved in a large risk assessment project by

months to one year to complete. Using an automated discovery, analysis and visualization program can cut the time from 6 months to 6 weeks.

The risk analysis manager will spend most of his time on this analysis, enlisting help from other departments - facilities managers (to provide some threat data); from accounting (to help establish asset values); and from all the departments that will be included in the review. For large, multinational companies, expertise in conducting risk management activities may vary from someone with 2 years experience, to a security professional with over thirty years experience. Obviously, the difference in experience will make a big difference in the analysis results, unless an automated tool is used, which can standardize the asset and threat data. Standardized data will allow large, distributed companies to establish a baseline over many sites and normalize the experience differences between many analysts.

RISK MANAGEMENT — A CRITICAL MANAGEMENT TOOL

A high-level risk assessment is, in itself, the most cost-effective safeguard available. It is a way of looking at a large organization in a consistent and quantifiable manner, with defensible results. It also provides a way of benchmarking the effectiveness of security across an organization and it will identify the weak areas so those can be revisited with a more intensive analysis at a later date. Corporate security policies and government regulations are being constantly re-written to address the increasingly networked environment, with a less loyal work force. Under these fast-changing conditions, risk management is becoming an increasingly important tool in corporate management strategies.

About SilentRunner®

Raytheon's SilentRunner is a network discovery, analysis and visualization tool designed to safeguard a company's information assets. Since its official launch in June 2000, SilentRunner has been servicing a variety of Fortune 500 corporations in the financial, electronics, pharmaceutical and high-tech industries, among others. SilentRunner identifies security risks and network vulnerabilities and alerts management to potential loss of data. It is the only security system that enables a rapid response to protect a company's assets by quickly correlating complex network events and displaying readily understood graphics. When combined with firewalls and intrusion detection systems, SilentRunner effectively completes the total network security suite. For more information, please visit www.silentrunner.com.