DATA SECURITY MANAGEMENT

NEW TRENDS IN RISK MANAGEMENT

Caroline R. Hamilton

INSIDE
The Information Age, New Directives and Guidelines, Risk Assessment Methodology, Vulnerability Assessment, Reporting to Management, Automating Risk Assessment, The Decision Point

RISKY BUSINESS — THE BACKGROUND

Risk management is a process used hundreds of times every day. From deciding whether to cross the street to deciding to take a shortcut home to avoid traffic to deciding to purchase health insurance or change jobs, each decision is based on principles of risk management.

Every time an individual crosses a city street, it involves a risk management decision. Is the light green? How fast is the traffic coming? How important is it to get across the intersection quickly? Is there a $1,000 bill laying on the curb? Is the person being chased by a man with a gun? All these considerations are analyzed in a split second and the decision is made: cross the street now, even against the light; or wait until the “walk” sign lights up.

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 to proprietary information to troop movements to sensitive medical records and financial transactions, critically important data flows through these systems. Independent reports detail the losses that have been sustained by information systems over the last 12 months. One survey reported that more than $100 million in losses was reported by 249 organizations. With losses of this magnitude, organizations are becoming increasingly concerned with their potential exposure and looking for ways to evaluate their security profiles.

PAYOFF IDEA
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. This article provides an overview of current approaches to assessing risk in the modern environment.
Our society depends on fast, accurate transmission of information. Everything from E-mail, stock quotes, credit ratings, bank balances, and travel arrangements, even the weather, is tracked by computer systems. Just 10 years ago, most employees worked with dumb terminals, which performed a prescribed set of functions. These terminals have migrated into personal computers on every desk, most linked to the Internet. Even prisoners are requesting modem access to conduct their in-prison business enterprises.

The availability of all this information and the ease of intercepting it has created an environment in which hackers are glorified as harmless “whiz kids,” even though the damage they do to a computer system may take weeks to undo. More serious incidents include the $10 million taken electronically from a major bank’s cash management system; an altered 911 message at a police station, which said, “We’re too busy eating donuts to come to the phone ...”; and a prostitution ring that operated for more than a year on a state government network.

Another problem in this new information society is the lessening of loyalty of employees to their organizations. Private companies have right-sized, downsized, and tried to trim overhead to keep profit margins high. Both federal and state governments have also been pushed to reduce their budgets and to do more work with fewer employees. The old days of having a job for life, where the company looked out for its employees and protected them, are over. The resulting lowering of morale contributes to a risky business environment in which the goals of the individual may no longer match the goals of the organization.

Risk assessment began as a process applied to large mainframes and data centers, which were in stand-alone, tightly controlled environments. However, as personal computers replaced dumb terminals on every desktop, and as these personal computers are increasingly linked to the Internet, computer security problems multiply. Hardware solutions, such as installing firewalls or automating audit logs, are sometimes difficult to justify to senior management and, where installed, do not always prevent security breaches. The interest in risk assessment as an effective method of analyzing these complex systems has increased dramatically over the last 12 months and serves two purposes: to identify existing weaknesses in the systems and to justify and prioritize the cost of additional safeguards.

The mood in the U.S. Congress is one of increasing accountability in government. In item three of the Republican Contract with America, risk management is discussed as a potential requirement for federal managers in such diverse departments as the Labor Department and the Environ-
mental Protection Agency. When eventually turned into legislation, it would require federal managers to cost-justify changes they make by detailing how much the proposed change would cost versus the money it would save the government.

NEW DIRECTIVES AND GUIDELINES
The General Accounting Office Report to Congress
In May 1996, the General Accounting Office (GAO), the audit branch of the federal government, released its report to Congress with the intriguing title, “Computer Attacks at Department of Defense Pose Increasing Risks” (GAO/AIMD-96-84 Defense Information Security). Using statistics from the Defense Information Systems Agency, as well as results of its own investigations, the report details more than 160,000 successful attacks against Department of Defense (DOD) computer systems. The report stated, “since the level of protection varies from installation-to-installation, the need for corrective measures should be assessed on a case-by-case basis by comparing the value and sensitivity of information with the cost of protecting it and by considering the entire infrastructure.”

In summarizing its results, the GAO report recommended more stringent security policies and that the DOD mandate risk assessments. In addition, the report included recommendations that DOD “develop Departmentwide policies for prevention, detection, and response to attacks.” (Currently, each branch of the service has its own, and sometimes different, security policies.)

The report also recommended that the DOD mandate that all security incidents be reported; that risk assessments be performed routinely to determine vulnerability to attacks; that vulnerabilities and deficiencies be corrected expeditiously, as they are identified; and that the damage from intrusions be expeditiously assessed to ensure data/system integrity.

The FBI/CSI 1997 Survey
The Computer Security Institute in San Francisco teamed with the Computer Crime Squad of the FBI in 1996 to do the first FBI/CSI Computer Crime Survey. The survey was conducted to provide statistical data on the state of computer crime and computer security, to quantify information losses, and to further cooperation between law enforcement and organizations to report computer crimes.

In 1997, the second survey was completed and the results were shocking. The sampling base included 5,000 information security professionals, 563 of whom completed the survey. Of these organizations, 249 reported losses of over $100 million from computer crime. Examples of losses included financial fraud (26 responses averaging $957,384), theft of proprietary information (21 responses averaging $954,666), telecom-
munications fraud (35 responses averaging $647,437), unauthorized access (22 responses averaging $181,436), sabotage (14 responses averaging $164,840), and system penetration (22 responses averaging $132,250).

Senate Permanent Subcommittee on Investigations
In June 1996, one month after the GAO report was released, U.S. Senator Sam Nunn convened the Senate Permanent Subcommittee on Investigations to hold hearings on “Security in Cyberspace.” The report of the subcommittee stressed the importance of vulnerability assessments to securing computer systems. The report stated, “Vulnerability testing and assessment of government and government interest computer systems is the best method of enhancing awareness of the vulnerabilities of our information infrastructure.”

The staff recommendations included emphasizing “that the federal government promote regular vulnerability assessments of government agencies, especially agencies outside of the Department of Defense.” Other safeguards recommended by the subcommittee were that the United States must formulate national policy to promote the security of its information infrastructure; the creation of a National Information Infrastructure Threat Center with real-time, 24-hour operational capabilities; and the creation of an international computer crime bureau with emergency response capability. The subcommittee report was widely reported in the national press.

The President’s Commission on Critical Infrastructure Protection
The following month (July 1996), the Clinton White House announced an executive order establishing the President’s Commission on the Critical Infrastructure Protection (PCCIP). Modeled after the NSTAC (a coalition of communications companies and the federal government), the PCCIP’s mission was to “assess the scope and nature of the vulnerabilities of, and threat to, critical infrastructures … and recommend a comprehensive national policy and implementation strategy for protecting critical infrastructures from physical and cyber threats and assuring their continued operations … .”

The Persian Gulf War had heightened security awareness by pointing out how many “private” resources were used in fighting it. Commercial long-distance lines and even cell phones formed a piece of the U.S. war effort. Yet, these resources were not under the direct control of the DOD, or even the federal government. The PCCIP identified eight critical infrastructures:

- Telecommunications
- Electrical power systems
• Gas and oil storage and transportation
• Banking and finance
• Transportation
• Water supply systems
• Emergency services (medical, fire, police, rescue)
• Continuity of government

Representatives from the highest levels of both government agencies and large private companies made up the PCCIP. In addition, the structure of the PCCIP included a task force (the Interim Coordinating Mission) “to provide/coordinate guidance to detect, prevent, halt or confine an attack and to recover and restore service; to issue threat and warning notices in the event advance information is obtained about a threat; and to provide training and education on methods of reducing vulnerabilities, and conduct after-action analysis.”

The PCCIP report was released in November 1997. The report concurred with many of the findings from the Senate Permanent Subcommittee on Investigations report, recommending vulnerability assessment as one of the most effective safeguards for government and private information systems. The report noted, “Government leaders are insufficiently aware of the vulnerabilities … .” It goes on to recommend a broad program of awareness and education, a major effort directed toward encouraging information sharing, an increased emphasis on vulnerability assessments, and quantitative risk management process.

Report of the Defense Science Board
The final major report issued in 1996 was the Report of the Defense Science Board. This lengthy report featured a series of recommendations including designating a czar for information warfare, establishing a Center for Intelligence/Threat Assessments, and establishing a Center for Information Warfare — Defense Operations. In addition, the report recommended a program to assess infrastructure dependencies/vulnerabilities; that DOD “raise the bar” with high-payoff, low-cost items such as training; and increasing awareness.

These diverse reports have one common thread — all the reports recommend increasing vulnerability assessments and mandating risk assessments.

WHAT IS RISK ASSESSMENT?
Risk assessment is a method of determining what kinds of controls are needed to protect an organization’s information systems and resources not just adequately but cost effectively.

The risk assessment process examines a set of five variables:

• Gas and oil storage and transportation
• Banking and finance
• Transportation
• Water supply systems
• Emergency services (medical, fire, police, rescue)
• Continuity of government
1. What is the security professional trying to protect, how much is it worth, and how much depends on it?
2. What could potentially threaten the asset?
3. What weakness exists that would allow the threat to materialize?
4. If the threat occurs, what kind of loss could the company have?
5. What controls can the security professional put into place that would reduce the organization’s loss if a threat occurred or eliminate the threat altogether?

The five variables include the following definitions:

1. **Assets**: Whatever is being protected. Assets can include databases, information, personnel, facilities, applications, computer hardware and software, and communications hardware and software.
2. **Threats**: Threats are events that could happen at any time. Even impeccable security cannot eliminate every threat — like hurricanes, earthquakes, or fraud — but security professionals can diminish the impact if the threat occurs and/or reduce its likelihood of occurrence. Examples of threats include natural disasters (e.g., cold, storms, lightning, and subsidence), as well as embezzlement, espionage, sabotage, loss of essential personnel, and theft.
3. **Vulnerabilities**: Vulnerabilities are weaknesses in the organization that would create a condition that allows the threat to affect the organization by triggering a loss. Examples of vulnerability areas include access control, administration, accountability, compliance, policy, operating procedures, and training.
4. **Losses**: Loss categories include direct loss, disclosure losses, loss of data integrity, losses due to data modification, and losses due to delays and denials of service.
5. **Safeguards**: Safeguards are security controls which, when put in place, can eliminate, reduce, or mitigate the impact of a threat occurrence. Examples of safeguards would include biometric controls such as retina scanning and use of encryption, awareness programs, redundant power sources, audit trails, visitor controls, and electronic monitoring.

**RISK ASSESSMENT METHODOLOGY**

The risk assessment process includes gathering information about assets, finding sources for threat data, doing a survey to find the vulnerabilities, and then matching the information 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. The risk analysis manager must evaluate thousands of different combinations to write a comprehensive report.
STEPS IN A RISK ASSESSMENT
There are six steps in a risk assessment:

1. Set parameters for risk analysis.
2. Define system’s assets.
3. Determine relevant threat profiles.
4. Survey all system users to discover vulnerabilities.
5. Analyze all data.
6. Write the report.

VALUING ASSETS
Finding values for organizational assets is one of the most difficult tasks associated with risk assessment. It is relatively easy to assign present value replacement costs to assets such as hardware systems and software and physical assets such as a building, tape drives, and office equipment. Valuing information is much more difficult. Databases may contain very sensitive information, and how can the analyst put a dollar value on the database? It is probable that the database is backed up somewhere and therefore, its replacement cost will probably be less than $1,000. However, if the database contains a list of police informants, or a list of recently diagnosed HIV-positive individuals, additional values must be determined based on three components: (1) the confidentiality requirements of the database, (2) the expectations of availability of the database, and (3) the requirements for integrity of the database. In medical records, for example, patients may sue a hospital if the confidentiality of their medical records is compromised.

FINDING THREAT DATA
Use of threat data is an important part of the risk assessment. Calculating frequency of occurrence for threats is an essential element of the cost-benefit analysis. If a threat is expected to occur only once every 20 years, it is unlikely that an organization will spend millions to protect against the threat, unless, of course, the threat would cause a catastrophic loss, even with a one-time occurrence. Threat data can be obtained, for example, through research at national repositories of such data, through compilation of media accounts, by reviewing weather information for the last hundred years, and by reviewing actuarial tables. Comprehensive threat data is very difficult to get and usually those who have the best threat data are the most uninterested in sharing it.

MANAGING THE RISK ASSESSMENT
Risk assessment is a management process and, by its nature, should involve the whole organization. Because the vulnerability discovery pro-
cess includes questioning staff in many different parts of the organization, it is vitally important to the eventual acceptance of the risk assessment findings that different departments be involved initially in setting up the analysis. Midlevel managers may feel threatened that another group is asking questions of “their” employees. They may worry that the findings could reflect negatively on their performance as supervisors.

In addition, if the survey questions are not approved before their use by the various supervisors and department heads, the results they generate might be discounted and not taken seriously. For these reasons, it is important to set up a risk analysis team within the organization. The team members will include representatives from each department included in the analysis process. Team members will review questions, identify the correct standards for their areas, assist the risk analyst in arriving at current asset replacement values, and serve as administrative support for the surveys in their respective areas of responsibility.

VULNERABILITY ASSESSMENT
Risk assessment is composed of two parts: the vulnerability assessment and the countermeasure (safeguard) assessment. The vulnerability assessment looks at an existing system or facility and evaluates its existing security, including how personnel are complying with existing policies and guidelines. The vulnerability assessment results in a detailed road map of all the existing weaknesses in the present system, including information on how widespread the problem is and which individuals identified the weakness (vulnerability).

Surveying people who use the systems under review is a critical part of the vulnerability assessment. Paper surveys are laborious and difficult to aggregate, but automated questionnaires allow risk analysts to interview users electronically. Each survey question starts with a control standard that outlines the official policy of the organization. Questions should be set up to validate compliance against published policies, guidelines, and directives. There is little point to asking questions unrelated to requirements because the organization would find it difficult to enforce compliance if it was not a requirement.

The risk analysis manager is the analyst in charge. However, other individuals in the organization may be able to make major contributions. According to the audit guidelines for risk assessment, the more people interviewed, the more likely the risk analyst is to find vulnerability. Individuals should not be requested to answer more than 50 to 100 questions directly related to their job. For example, network users might answer questions related to whether they use their passwords, whether they log off their terminals when they leave their station, or whether they have attended basic data security training. Database administrators will answer a few general questions but will also answer more specific questions related to their jobs.
THE QUESTIONS

Asking good questions is the very heart of the risk assessment and also forms the core of the vulnerability assessment. Questions should always be compliance based and directly linked to a control standard or control objective. If the risk analysis manager asks questions not linked to standards and then discovers major problems, the path will not exist to force compliance. Limiting the number of questions is one of the most difficult aspects of the analysis.

Employees may be nervous when they are asked to answer questions related to how they perform their jobs. It is important to make sure that these individuals understand that the risk assessment is a scientific process, and any data gathered in the risk assessment will be seen by only one individual (the risk analysis manager). They should also be aware that their comments will not be reviewed by their supervisor, nor will they end up in their personnel file.

Random surveys are often used to predict election results, from local precincts in a particular city to federal elections, where the network news teams are able to predict the final results from a profile of only a few key states. In these examples, random samples are usually less than 1%. In a risk assessment, a random sample is not desirable. Instead, the objective should be to question as many people as possible. The more individuals questioned, the better the chances that the risk analyst will discover a vulnerability.

It is unrealistic to think that people will answer more than 50 to 100 questions. By assigning questions to job categories, or what are called “functional areas,” the analyst can avoid asking questions of individuals when the questions do not relate to their areas. Functional areas are pieces of a job. By dividing up questions into these categories, for example, Michael Smith may answer 20 questions for network users, 20 questions for personnel management (which is his area), and 15 general organization questions. More specialized personnel (e.g., a facilities manager, the physical security officer, or a database administrator) will answer questions that relate only to their particular area.

Questions start as control standards. The standard might be: “Passwords should be changed every month.” One might cite a reference representing this standard’s origin, for example, “Telecom Security Directive 3, p. 4, para. 5.” The question statement asks users how well they comply with this standard on a percentage scale from 0 to 100. The 0 answer means the user never complies with the standard. An answer of 100 means the user complies with the standard 100% of the time. Users are encouraged to answer with any percentage in between.

Users should be allowed two additional options in answering: (1) the opportunity to answer “not applicable” if the question does not apply to them, and (2) the opportunity to answer “I don’t know” if they do not know the answer.
COST-BENEFIT ANALYSIS — GETTING MORE BANG FOR THE BUCK

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. In reviewing the existing security controls, it is important to indicate percentages of current implementation. For example, maybe the “visitor-badging” policy is only 70% implemented, meaning that it is implemented on weekdays but not on weekends. In actual risk assessments, achieving implementation of an existing control to 100% is often the most cost-effective solution.

The cost-benefit analysis will result in a return on investment (ROI) ratio, balancing the value of the information against the cost of controls to protect it. By establishing ROI data, managers and directors can make more informed decisions regarding which controls to implement, based strictly on initial cost as well as on the current threat exposure of the organization.

The accountability that is a built-in component of risk assessment is increasingly attractive to top-level management, both in the federal sector and in private industry, where board members and shareholders want quantitative numbers to use in assessing the security level of an organization and making the resultant management recommendations.

REPORTING RESULTS TO MANAGEMENT

The value of a risk assessment is judged by how well it is presented to management. The vulnerability assessment report, in particular, usually comes as a surprise to upper management, who are often shocked to see how many of the organizational directives are not being complied with. Typical results of a vulnerability assessment done on a local area network (LAN) include the following findings: 50% of LAN users do not memorize passwords, users do not always log off terminals, supervisors loan passwords to new employees, no clear separation of duties exists, network files are not always labeled, and the disaster recovery plan may not have been fully implemented throughout the organization.

In most risk assessments, glaring problems are uncovered during the course of the analysis. Often, the problem is so severe that it must be corrected immediately, instead of waiting until the final risk-assessment report has been written and approved. In these cases, the report can be written to indicate that “several vulnerabilities were discovered during the course of the analysis and were immediately corrected.”

The analyst in charge of the analysis must be able to explain to management how the analysis was conducted, who was included in the survey population, and how the numbers were calculated. Knowledge in these three areas makes the analysis results defensible and enhances the overall value of the analysis.
AUTOMATING THE RISK ASSESSMENT

The new emphasis on the need for risk assessment is causing a renewed interest in automated risk analysis software tools, which can reduce the time involved in a big risk assessment by more than 60%.

A manual risk assessment on a major computer system — including the personnel, the facilities, any remote sites, a network of over 1,000 users tied to a mainframe — may take from six months to one year to analyze using a manual method. Using an automated software program can cut the time from six months to six weeks. The risk analysis manager spends most of his time on this analysis, enlisting help from other departments, facilities managers (to provide some threat data), accounting (to help establish asset values), and all the departments that will be included in the review.

Most automated risk assessment programs include an “expert knowledge base.” These programs have captured an expert’s working knowledge of risk-assessment relationships and modeled them into a software format. As a result, these programs can be used by much less experienced managers and will still produce an excellent result. In addition, software can reduce interviewer bias and allow an organization to survey a number of different locations and directly compare them. Most important, automating the risk-assessment task, which is a combinatorial nightmare, can reduce the time needed to analyze a large wide area network from six months to three weeks.

THE DECISION POINT — HOW TO APPLY THE RESULTS OF THE RISK ASSESSMENT

A high-level risk assessment is, in itself, the most cost-effective safeguard that can be found. It is a way of looking at a large organization in a consistent and quantifiable manner, with defensible results. It also provides a baseline across an organization and identifies the weak areas so they can be revisited with a more intensive analysis at a later date.

Corporate policies and government regulations are being constantly rewritten to address the networked environment, and risk assessments are becoming increasingly important in the management of information systems.

Caroline R. Hamilton is president of RiskWatch, Inc., a company specializing in security assessment software. She is a charter member of the National Institute of Standards and Technology’s Risk Management Model Builders Workshop, and recently served on the working group to create a Defensive Information Warfare Risk Management Model, under the auspices of the Office of the Secretary of Defense. She is a member of the American Society for Industrial Security’s Standing Committee on Computer Security, and is working with the U.S. Coast Guard and the Maritime Security Council to create technical guidelines for risk assessment.