

RISK MANAGEMENT AND SECURITY

Author: Caroline R. Hamilton

INFORMATION RISK MANAGEMENT IN A RISKY ENVIRONMENT

Our society depends on fast, accurate transmission of information. Everything from e-mail, stock quotes, credit ratings, bank balances, travel arrangements, even the weather, are all transacted by computer systems. When ten years ago, employees worked with dumb terminals that performed a prescribed set of functions, now these employees have full internet access. Even federal prisoners are now requesting modem access to conduct their in-prison enterprises.

The availability of all this information and the ease of intercepting it has created an environment where 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 ten million dollars taken electronically from a major bank's cash management system, violation of confidential medical records and fraud schemes that are borderless because they exist only in cyberspace.

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

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, troop movements, sensitive medical records and financial transactions, critically important data flows through these systems. Independent reports, such as the 2002 CSI/FBI Computer Crime and Security Survey, detail the losses that have been sustained by information systems. More than two hundred and fifty-five million dollars in losses were reported in this single report. 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.

THE CORPORATE CULTURE IN A GLOBAL ECONOMY

In a global economy, success for organizations will be driven by their ability to innovate, to become truly global in their reach, and by their use of technology. This use of technology, primarily the use of computer systems and Internet technology requires exceptional security. In a recent class of information security professionals, the students were asked how many felt secure using a credit card for an on-line purchase. The response was telling, only 25% of the students raised their hands.

For a company to be able to send and receive proprietary data on-line, to use electronic commerce to receive money, and deliver orders, whether over an Internet connection, or through a worldwide company Intranet, excellent security will be an absolute requirement. Security organizations within companies, to be effective, 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. The measurement tools of a security program are the risk assessment, and, especially, the Return on Investment numbers. In order for security management personnel to be able to keep up with a worldwide organization, it will have to use common processes and standardized procedures.

HOW MUCH IS TOO MUCH? -- THE INSIDER

In a data-driven company, the insider (employee) has access to a wide variety of information, and often few controls exist to control the employee. In recent 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. 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.

In assessing the value of proprietary company information, consider the Brown and Williamson employee Dr. Jeffrey S. Wigand, who took company information not for personal gain, but to disclose questionable marketing practices in the tobacco industry. What was the ultimate cost of this insider, not just to Brown and Williamson, but also to the entire tobacco industry? Here's what the Feb, 6, 1996 episode of 60 MINUTES, had to say:

"Tonight, Jeffrey Wigand, the scientist whose insistence on defying his former employer has led him to tell what he believes to be the truth about cigarettes. What is it that he believes to be the truth about cigarettes? And what is it that Brown & Williamson believes to be the truth about him? A story we set out to report six months ago has now turned into two stories: how cigarettes can destroy peoples' lives and how one cigarette company is trying to destroy the reputation of a man who refused to keep quiet about what he says he learned when he worked for them. The company is Brown & Williamson, America's third largest tobacco company. The man they set out to destroy is Dr. Jeffrey Wigand, their former three-hundred-thousand-dollar-a-year director of research. They employed prestigious law firms to sue him, a high-powered investigation firm to probe every nook and cranny of his life. And they hired a big-time public relations consultant to help them plant damaging stories about him in the Washington Post, the Wall Street Journal, and others. What Dr. Wigand told us in that original interview was that his former colleagues, executives of Brown & Williamson Tobacco, knew all along that their tobacco products, their cigarettes and pipe tobacco, contained additives that increased the danger of disease. And further, that they had long known that the nicotine in tobacco is an addictive drug, despite their public statements to the contrary, like the testimony before Congress of Dr. Wigand's former boss, B&W's Chief Executive Officer Thomas Sandefur."

Such is the power of the insider.

THE LINK BETWEEN PHYSICAL AND INFORMATION SECURITY MANAGEMENT

Only a few years ago, the security functions in an organization were split between two different individuals. One was the information security officer, usually residing up on the 7th floor, near the MIS Department. The other

was the physical security officer, using relegated to a back office, where he spent his day checking in guards and investigating petty theft. Since September 11th, all that has changed. In fact, one of the challenges to organization is how to integrate these two functions, which are now almost completely interdependent.

A growing trend is to empower the company CSO (Chief Security Officer) so that cyber security, physical security, personnel security and all other aspects of security can be rolled up into an enterprise-wide, holistic security program. He or she has a seat at the table now with the company's COO, CIO and CFO. And a centralized reporting structure under the corporate CSO positions information security as a risk management expenditure as opposed to the forgotten item on the IT budget. The CSO will need to drive a security strategy to protect both financial and practical corporate assets because you cannot secure your information or your information systems unless you also pay attention to the physical and personnel security of the corporation. The converse is also true you cannot protect your physical perimeter or workforce unless you have also secured the company's information systems.

RESULTS OF THE CSI/FBI 2002 COMPUTER CRIME & SECURITY SURVEY

The Computer Security Institute (CSI) with the participation of the Federal Bureau of Investigation (FBI) Computer Intrusion Squad's San Francisco office conducted the "2002 CSI/FBI Computer Crime and Security Survey". The survey was conducted in order to provide statistical data on state of computer crime and computer security, to quantify information losses and to further cooperation between law enforcement and organizations to report computer crimes. Based on responses from 503 security practitioners in U.S. corporations, government agencies, financial institutions, medical institution and universities, the findings of the "2002 CSI/FBI Computer Crime and Security Survey" indicate that computer crime and other information security breaches continue unabated and that the financial toll to U.S. corporations and government agencies is mounting. Two hundred and twenty-three (or 40%) of the organizations studied, which were able to quantify their losses, reported losses **over \$455.8 million dollars**. This figure represents a 21% increase in reported losses over the 2001 figure of \$377.8 million in losses.

The survey also reported that an overwhelming 90% of respondents said they experienced computer security breaches within the last twelve months. The problem of employees, "insiders" was underscored in several parts of the survey. For example, **89 respondents who could quantify their losses reported insider abuse of Net access at an annual cost of \$50 million dollars and 15 respondents who could quantify the loss reported unauthorized access at an annual loss of \$4.5 million.**

The number of organizations that cited their Internet connection as a frequent point of attack rose from 70% in 2001 to 74% in 2002. This represents more than a 150% increase over the initial 1997 figure of 47%. In 1997 internal systems have been considered to be the greater of problems. Now the threat of Internet connection vulnerability is more than twice the threat cited from internal systems. It is not that the threat from inside the perimeter has diminished; it is simply that the threat from outside, via Internet connections, has increased.

CRITICAL INFRASTRUCTURE PROTECTION IN A POST 9/11 ENVIRONMENT.

In mid-1996, the Clinton White House announced an Executive Order (Executive Order 13013) 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.....

Now that the U.S. is on a heightened state of alert, these eight critical infrastructure elements are again subject to risk assessments and vulnerability assessments to ensure that biological agents don't end up in public water supplies (6 – Water Supply Systems); or that ports and container cargo are more rigorously inspected to make sure a 'dirty bomb' doesn't arrive in a critical seaport (5 – Transportation). The eight critical infrastructures include:

1. Telecommunications
2. Electrical Power Systems
3. Gas and Oil Storage and Transportation
4. Banking and Finance
5. Transportation
6. Water Supply Systems
7. Emergency Services (medical., fire, police, rescue)
8. Continuity of Government

NEW LAWS REQUIRE RISK ASSESSMENT

After September 11th, legislators scrambled to write new legislation that addressed the new threat environment. These include The Port Security Act of 2001, the Public Health Security and Bioterrorism Preparedness and Response Act of 2002, (Public Law 107-188, 107th Congress), the Aviation and Transportation Security Act of 2001, Presidential Directives 1 and 2 on Homeland Security, as well as others too numerous to mention. These public laws and federal guidelines require risk and vulnerability assessment of every infrastructure element.

ELEMENTS OF RISK ASSESSMENT

A formal, quantitative risk assessment is the foundation and starting point of a good risk management program. Risk assessment 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.

The risk assessment process analyzes a set of five variables, and comes up with recommended actions based on the relationships of these variables to each other.

You need to ask these questions: 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 a threat to materialize? Fourth, if the threat occurs, what kind of loss could you have? 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:

1. **ASSETS** - whatever you're trying to protect. Assets can include databases, information, personnel, facilities, applications, computer hardware and software, and communications systems.

2. **THREATS** - Threats are events that could occur, and cannot ever be completely eliminated, although you can reduce the likelihood of occurrence, or mitigate its impact. Even stringent security cannot eliminate every threat. Threats include events such as hurricanes, earthquakes, viruses, hackers, data destruction, data modification, theft of data, theft of company property, fire, false alarms, bomb threats, sabotage, fraud, or embezzlement.
3. **VULNERABILITIES** - These are weaknesses in the organization which would create a condition allowing a threat to materialize and triggering a loss.
4. **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, and for physical security reviews, loss of life.
5. **SAFEGUARDS** - Safeguards are security controls which, when put in place, can eliminate, reduce or mitigate the impact of a threat occurrence.

RISK ASSESSMENT METHODOLOGY

The risk assessment process includes gathering information about the assets of the organization, including all information assets such as networks, data centers, computers, hardware, software, data/information; as well as physical assets, such as the personnel who staff the organization, the network users, the physical facility and dozens of other organizational resources. In addition, the risk assessment process includes finding sources for comprehensive threat data, which may be gathered from internal sources such as incident report data, intrusion detection software and/or threat data such as crime statistics, industry standards and benchmarking data, and historical data about what has happened in the organization previously.

Vulnerability assessment is a key component of the risk assessment. Vulnerability data can come from two sources – however, a combination of both is recommended. The first source is a survey to find the weaknesses in the organization, asking the organization's personnel a controlled set of questions that validate compliance with the organization's standards. The second source is technical vulnerability scanning reports that give very micro-level details about the weaknesses in the configuration of a network, produced by commercial products such as ISS and NetSolar from Cisco.

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.

STEPS IN A RISK ASSESSMENT

There are six basic steps in a risk assessment:

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

THE 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 result of the vulnerability assessment will present a detailed road map of all the existing weaknesses in the present system, including information of how widespread the problem is, and which individuals identified the weakness (vulnerability).

Surveying people who use the system under review is a critical part of the vulnerability assessment. While paper surveys are laborious and difficult to aggregate, automated questionnaires now exist which allow risk analysts to interview users electronically. Survey questions start 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 in 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, there may be other individuals in the organization who can make major contributions. According to the audit guidelines for risk assessment, the more people you interview, the more likely you are to find vulnerabilities. Individuals should not be asked to answer more than 50-100 questions that are directly related to their job. For example, a network user 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. A database administrator will answer a few general questions, but also more specific questions related to their job.

SURVEY 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 you ask questions that are not linked to standards, and discover major problems, the path will not exist to force compliance. Limiting the number of questions to ask 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 job. It is important to make sure that these individuals understand that the risk assessment is a scientific process, and that any data gathered in the risk assessment will be seen by only one individual (the risk analysis manager), and 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 you question, the better the chances that you will discover vulnerabilities.

It is unrealistic to think that people will answer more than fifty to one hundred questions. To avoid individuals having to answer questions that do not relate to their area, in a risk assessment, questions are divided into job categories, or what is called 'functional 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, such as facilities managers, the physical security officer, or a database administrator will answer questions that relate only to his/her particular area.

Questions start as control standards. The standard might be: "Passwords should be changed every month". You might cite a reference representing where this standard originated, for example, "Telecom Security Directive 3, p. 4, paragraph 5". The question statement asks the user how well they comply with this standard on a percentage scale from 0 to 100. The zero answer means the user never complies with the standard. Answer of 100 means the user complies with the standard one hundred percent of the time; and the user is encouraged to answer with any percentage in between.

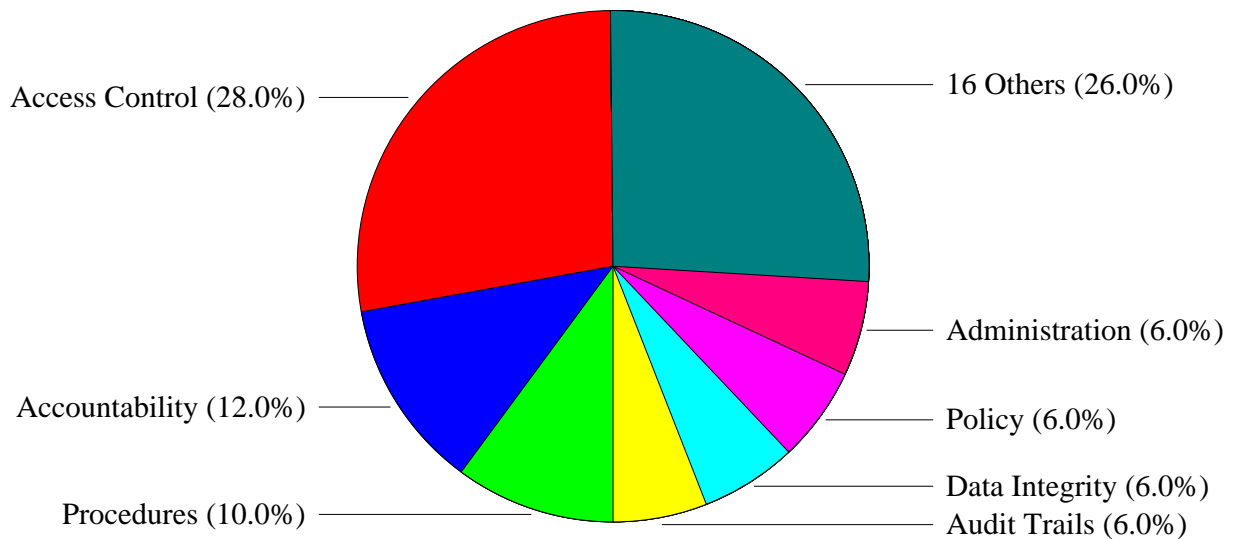
In addition, users should be allowed two additional options in answering. The first is the opportunity to answer 'not applicable', if the question doesn't apply to them; and secondly, to answer, "I don't know", if they don't know the answer. This question process also serves as a training exercise, and a security awareness process.

THE TECHNICAL VULNERABILITY ASSESSMENT

Technical vulnerability assessments use scanning tools to survey the actual network and report the technical weaknesses that are discovered. Products, such as NetSolar by Cisco, uses both passive analysis and active probing methods to identify security vulnerabilities, which may increase the efficiency of vulnerability identification and reducing false positive results. These technical assessments can differentiate between infrastructure devices (such as routers, switches, and firewalls) and host devices (user workstations or servers [such as e-mail servers such as Web servers. Technical vulnerability tools can find vulnerabilities in Network TCP/IP hosts, UNIX hosts, Windows NT hosts, web servers, mail servers, FTP servers, firewalls, routers and switches.

VULNERABILITY ASSESSMENT RESULTS

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, as illustrated in the chart below:



Vulnerabilities that are commonly discovered in risk assessments include:

- 50% of network users don't memorize passwords
- Users don't always log-off terminals
- Servers aren't located in a secured area
- Supervisors loan passwords to employees
- No clear separation of duties
- Uncompiled source code can reside on the system
- The disaster recovery plan has not been completed/updated.

ENROLLING THE ORGANIZATION IN RISK MANAGEMENT

Risk assessment is a management process and, by its nature, should involve the whole organization. Because the vulnerability discovery process will include questioning many different parts of the organization, it is vitally important to the eventual acceptance of the risk assessment findings, that different departments be involved in the initial setting up of the analysis. Mid-level 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 prior to 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

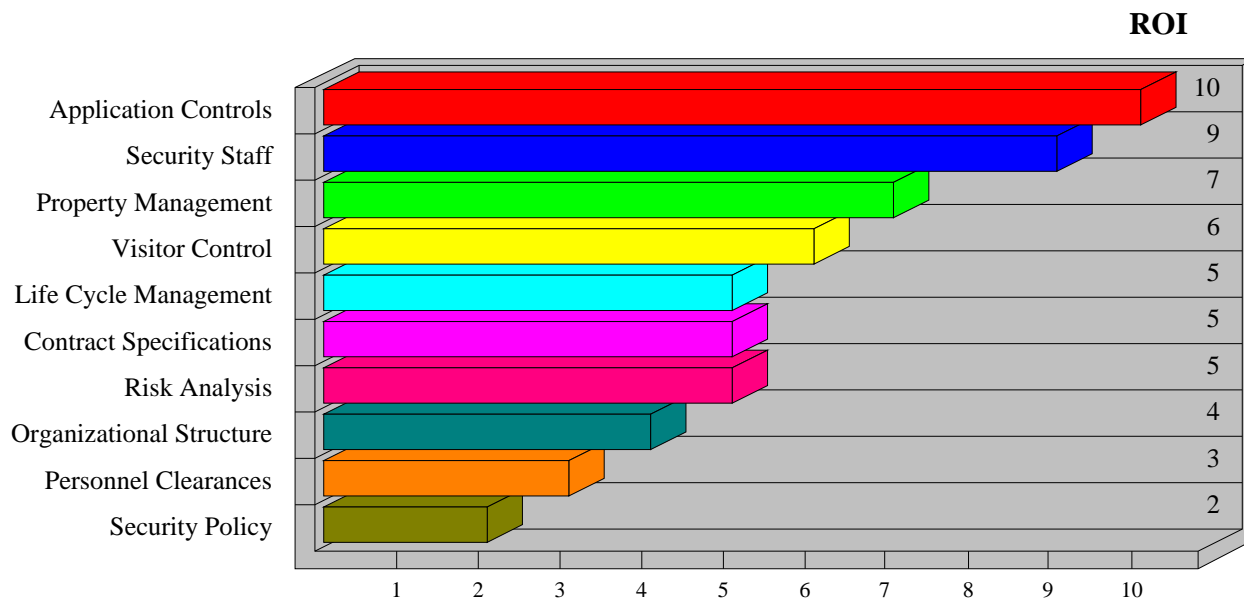
representatives from each department included in the analysis process. Team members will review questions, identify the correct standards for their areas, assist the risk analyst in arriving at current asset replacement values, and serve as administrative support for the surveys in their respective areas of responsibility.

THE COST BENEFIT ANALYSIS - ESTABLISHING 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. In reviewing the existing security controls, it's 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, completing implementation of an existing control to 100% is often the most cost effective solution.

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 strictly on initial cost, but also on the current threat exposure of the organization.

The accountability which is a built-in component of risk assessment is increasingly attractive to top level management, both in the federal sector, as well as 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. A typical Cost Benefit Analysis graph is shown below:



Return On Investment(ROI). Calculated in order of the 10 highest ROIs.

AUTOMATING THE RISK MANAGEMENT PROCESS

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

A manual risk assessment on a major computer network, including the personnel, the facilities, any remote sites, 1000 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 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 which will be included in the review.

In risk management of facilities and sites, additional considerations include the technical competence of the manager conducting the analysis. For large, multinational security 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 create a standard set of questions, and 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 THE AUTHOR:

Caroline R. Hamilton is President of RiskWatch, Inc., a company specializing in security and risk management software. She was a Charter member of the National Institute of Standards and Technology's Risk Management Model Builders Workshop from 1988 to 1995. From 1996-1998, she served on the working group to create a Defensive Information Warfare Risk Management Model, (DIWRM2) under the auspices of the Office of the Secretary of Defense. She is a member of the ASIS International's Council on Information Technology and Security, and is working with the U.S. Coast Guard and the Maritime Security Council to create new port and ship assessment software programs. Based in Annapolis, Maryland, she has written for the Computer Security Journal, the CSI Alert, Defense Electronics, InfoSecurity News, Access Control, Today's Facilities Manager, ISSA Password and many other publications.

