March 1998

ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

MANAGEMENT OF RISKS IN INFORMATION SYSTEMS: PRACTICES OF SUCCESSFUL ORGANIZATIONS

Recent break-ins to U.S. government and university computer systems demonstrate just how vulnerable even the most sophisticated organizations can be to technological assaults. While the new attacks caused no apparent damage to information or to the systems, these incidents are unfortunate reminders that the potential exists for severe damage. Systems are at risk from fraud, user errors, accidents and natural disasters, as well as from sabotage and other malicious acts.

It is a fact of life that organizations are becoming increasingly dependent on interconnected information systems to conduct business and to provide information and services to their customers. While the vulnerabilities of systems are getting increasing attention, many organizations have not adopted systematic, thorough practices for evaluating system vulnerabilities and for reducing risk. Recently, the General Accounting Office (GAO) studied organizations that had successfully adopted superior security programs. This bulletin describes some of the good practices that GAO identified and disseminated to help other organizations, especially federal organizations, to improve their information security.

The GAO Study

For many years, the GAO had found weaknesses in the information systems of federal agencies. Many agencies had not instituted information security programs to establish controls for their systems and to monitor those controls for their effectiveness. To gain a broader understanding of how security programs can be successfully implemented, GAO studied the management practices of eight nonfederal organizations. The focus was on the management framework that the organizations had established rather than on specific controls that had been adopted.

The nonfederal organizations studied by the GAO manage the same types of risks as federal organizations. Both federal and nonfederal organizations are concerned with protecting the confidentiality, integrity and availability of information. Secure information systems are essential to providing high-quality services to customers, avoiding fraud and disclosure of sensitive information, promoting efficient business operations, and complying with laws and regulations. All of the organizations studied had reoriented their security programs to make them visible, integral components of their business operations.

The GAO findings have been published in an exposure draft executive guide entitled *Information Security Management, Learning from Leading Organizations.* The GAO discussed its findings with several government organizations concerned with federal security policies, including NIST. After reviewing the comments received on the exposure draft, GAO plans to issue a final version of the executive guide.

Risk Management

Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk. Managers analyze risks for many aspects of their business; they consider alternatives and implement plans to maximize returns on their investments. A risk management process for information

Continued on page 2

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. **Bulletins are issued on an as-needed basis** and are available from ITL Publications, National Institute of Standards and Technology, Room 562, Building 820, Gaithersburg, MD 20899, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and address to this office.

Bulletins issued since May 1996:

- *The World Wide Web: Managing Security Risks*, May 1996
- *Information Security Policies for Changing Information Technology Environments*, June 1996
- *Implementation Issues for Cryptography*, August 1996
- *Generally Accepted System Security Principles (GSSPs): Guidance On Securing Information Technology (IT) Systems*, October 1996
- *Federal Computer Incident Response Capability (FEDCIRC)*, November 1996
- *Security Issues for Telecommuting*, January 1997
- *Advanced Encryption Standard*, February 1997
- *Audit Trails*, March 1997
- *Security Considerations in Computer Support and Operations*, April 1997
- *Public Key Infrastructure Technology*, July 1997
- *Cryptography Standards and Supporting Infrastructures: A Status Report*, September 1997
- *Internet Electronic Mail*, November 1997
- *Information Security and the World Wide Web (WWW)*, February 1998

systems enables managers and their organizations to build an in-depth knowledge about their systems and how they are interrelated.

Risk management is a vital element of a comprehensive information security program. Several NIST publications deal with this topic, including the following:

NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook

NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems (both documents are available at http://csrc.nist.gov, click on "Publications")

Five Principles of Risk Management

The GAO identified five principles of risk management, which had been adopted by the organizations studied:

- Assess risk and determine needs
- Establish a central management focus
- Implement appropriate policies and related controls
- Promote awareness
- Monitor and evaluate policy and control effectiveness

Who we are

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today.

The successful organizations applied these principles by linking them into a cycle of activity that enabled the organizations to address risks on an ongoing basis. The success of security programs depended upon the recognition and understanding of the senior executives that their information systems were subject to risks and that these risks affected their business operations. After assessing risks of their business operations, the organizations established policies and selected controls. They emphasized increased awareness of users to the policies and controls. They monitored the effectiveness of the policies and controls and used the results to determine if modifications of policies and controls were needed. Central security management offices coordinated this cycle of activities.

All organizations studied said that risk considerations and related cost-benefit tradeoffs were a primary focus of their security programs. Security was not an end in itself, but a set of policies and controls designed to support business operations.

Sixteen Successful Practices

The GAO found that there were general practices associated with each risk management principle and that these practices were common to the organizations studied.

- Principle: Assess risk and determine needs.
  - Practice 1. Recognize information resources as essential organizational assets that must be protected. The efforts of high-level executives to understand and manage risks helped to ensure that security was taken seriously at lower levels in the organization and that security programs had adequate resources. Security specialists kept managers at all levels informed of emerging security issues. For some organizations, the high-level interest was driven by an incident that demonstrated system vulnerabilities. Some organizations were exploring new ways to improve operational efficiency and services to customers through information technology and were concerned about the security of these new systems.
  - Practice 2. Develop practical risk assessment procedures that link security to business needs. While the organizations explored a variety of risk management methodologies, they were generally satisfied with relatively simple risk assessment practices that could be adopted by different organizational units and that involved both technical people and those with knowledge of business operations. In one organization, simple automated checklists were used. Another organization established standard procedures for requesting and granting new network connections, requiring documentation of the business need for the connection and the risks associated with it. None of the organizations tried to quantify the risks precisely because of the difficulty of identifying such data.
  - Practice 3. Hold program and business managers accountable. The organizations studied felt that business managers should be held accountable for managing the information security risks associated with their operations, just as they are held accountable for other business risks. Security specialists in these organizations had an advisory role, including keeping management informed about risks. Similarly, program managers in federal agencies are also considered to be in the best position to determine which of their information resources are the most sensitive and to assess the impact of security problems.
  - Practice 4. Manage risk on a continuing basis. The organizations studied emphasized continuous attention to security. The continuity of attention helped to ensure that controls were appropriate and effective, and that individuals who used and maintained information systems complied with the organizational policies. For federal organizations, the Office of Management and Budget has developed policies that promote a risk-based approach. These policies have been issued in Circular A130, Appendix III, Security of Federal Automated Information Resources.

- Principle: Establish a central management focal point.
  - Practice 5. Designate a central group to carry out key activities. Central security groups served as catalysts for ensuring that information security risks are considered in planned and ongoing operations. These groups provided advice and expertise to all organizational levels and kept managers informed about security issues. They developed organization-wide policies and guidance; educated users about information security risks; researched potential threats, vulnerabilities and control techniques; tested controls; assessed risks; and identified needed policies.
  - Practice 6. Provide the central group with ready and independent access to senior executives. The organizations studied knew that security concerns could be at odds with the desires of business managers and system developers to develop new computer applications quickly and to avoid controls which might impede efficiency and convenience. Elevating security concerns to higher management levels helped to ensure that the risks were understood and taken into account when decisions were made.
  - Practice 7. Designate dedicated funding and staff. Unlike many federal agencies, the organizations studied defined budgets which enabled them to plan and set goals for information security programs. The budgets covered central staff salaries, training, and security software and hardware. In these organizations, information security responsibilities had been clearly defined for the groups carrying out the security programs, and dedicated staff resources had been provided to carry out these responsibilities.
  - Practice 8. Enhance staff professionalism and technical skills. The organizations studied had taken steps to provide personnel involved in information security programs with the skills and knowledge that they needed. Staff expertise was updated frequently to keep skills and knowledge current. Staff members attended technical conferences and specialized courses, connected with other professionals in the field, and reviewed technical literature and bulletins. Special training courses were provided for system administrators who are the first line of defense against security intrusions and often in the best position to notice unusual activities. Because of the strong demand for security professionals, these organizations made special efforts to attract and keep expert staff members.

- Principle: Implement appropriate policies and related controls.
  - Practice 9. Link policies to business risks. The organizations studied stressed the importance of up-to-date policies that made sense to users and others who were expected to understand them. A current and comprehensive set of policies is a key element in an effective security program. These policies must be adjusted on a continuing basis to respond to newly identified risks. The policies of the organizations studied paid particular attention to user behavior. In today's interconnected network environment, users can accidentally disclose sensitive information to many people through electronic mail or introduce damaging viruses that are then transmitted to other computers in the organization's networks.
  - Practice 10. Distinguish between policies and guidelines. Policies generally outlined fundamental requirements that managers considered to be mandatory, while guidelines contained more detailed rules for implementing the policies. By distinguishing between the two, the organizations studied were able to emphasize the most important elements of information security while providing flexibility to unit managers in implementing policies.
  - Practice 11. Support policies through the central security group. The organizations studied had central security management groups responsible for writing policies in partnership with other organizational officials. The central groups provided explanations, guidance, and support to the various units in the organization. This practice encouraged business managers to support centrally developed policies that addressed organizational needs and were practical to implement.

- Principle: Promote awareness.
  - Practice 12. Continually educate users and others on risks and related policies. The central security management groups worked to improve everyone's understanding of the risks associated with information systems and of the policies and controls in place. They encouraged compliance with policies and awareness on the part of users of the risks involved in disclosing sensitive information or passwords.
  - Practice 13. Use attention-getting and user-friendly techniques. The techniques used included intranet Web sites that explained policies, standards, procedures, alerts and special notices; awareness videos with messages from top managers about the security program; interactive presentations by security staff with various user groups; security awareness days; and products with security-related slogans.

ITL Bulletins Via E-Mail

We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message to listproc@nist.gov with the message **subscribe itl-bulletin**, and your proper name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message **HELP**. To have the bulletin sent to an e-mail address other than the From address, contact the ITL editor @ 301-975-2832.

- Principle: Monitor and evaluate policy and control effectiveness.
  - Practice 14. Monitor factors that affect risk and indicate security effectiveness. The organizations studied directly tested the effectiveness of their controls. Most organizations relied primarily on auditors to carry out this function. This enabled the security organizations to maintain their role as advisors. The central security management groups kept track of audit findings and the organization's progress in implementing corrective actions. In some cases, the central security management groups conducted their own tests, and some organizations allowed designated individuals to try to penetrate systems. The testing of controls enabled the organizations to identify unknown vulnerabilities and to eliminate or reduce them. All of the organizations monitored compliance with policies, mostly through informal feedback to the central security group from system administrators. All of the organizations kept summary records of actual security incidents to measure the types of violations and the damage suffered from the incidents. The records were valuable input for risk assessments and budget decisions. Many of the organizations expressed an interest in developing better techniques to measure the benefits and costs of security policies and controls.
  - Practice 15. Use results to direct future efforts and hold managers accountable. Organization officials said that monitoring encourages compliance with information security policies, but the full benefits of monitoring are not achieved unless results are used to improve the security program. Results can be used to hold managers accountable for their information security responsibilities.
  - Practice 16. Be alert to new monitoring tools and techniques. Security managers of the organizations studied said that they continually looked for new tools to test the security of their systems. They found current professional literature and involvement with professional organizations useful in learning about the latest monitoring tools and research efforts.

GAO's Guidance for Federal Organizations

Federal agencies are encouraged to develop an information security program that follows the general principles and practices outlined in the draft executive guide. By instituting this management framework, agencies can strengthen the security of their information systems, facilitate the development and improvement of systems, and take advantage of technology advances.

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Building 820/562
Gaithersburg, MD 20899

Official Business
Penalty for Private Use $300

Address Service Requested

BULK RATE
POSTAGE & FEES
PAID
NIST
PERMIT NUMBER G195