EM IT Insight

by Jill Barson Gilbert

Network Insecurity

Today, many environment, health, and safety (EH&S) professionals carry around portable notebook computers, allowing them immediate access to information anytime, anywhere—via wired or wireless networks, at home, in the office, in airports, and even on airplanes. However, with the increasing threat of corporate espionage and malicious computer "hacking," and the introduction of commercial software applications delivered via the Internet, concerns over the safety of corporate data are greater than ever. And human error remains one of the chief causes of network security problems![1] At a minimum, computer networks, large and small, need protection from unauthorized intruders and a method of tracking those that have access to the network and its data. How secure are your data when you connect to your corporate network?

NETWORK SECURITY THREATS

Networks are intended to facilitate information sharing. They include the Internet, intranets for internal users, and extranets that provide limited access to customers and partners outside the company. Keep in mind that the more parties that have access to your network, the more you should be concerned about security.

Although personal computers and computer networks have been in use for more than 20 years, the risk of cyber security attacks remains high. Though the number of actual incidents reported by information technology (IT) security professionals in 2003 equaled the number reported in 2002, attacks via the Internet are on the rise, according to the results of a 2003 survey of computer security conducted by the FBI.[2] Many of the organizations surveyed reported network attacks from both inside and outside the company. Despite these trends, however, the severity and financial impacts of computer security breaches declined for the first time last year since 1999. This indicates that companies have gained a certain degree of control over security and can mitigate the impacts of security breaches.

HEDGE YOUR BETS AGAINST SECURITY THREATS

Network security measures help protect corporate networks and data from unauthorized modification, destruction, or disclosure. They also assure that the network properly performs its critical functions without harmful side effects. Sound planning and implementation can help minimize the risk of network security breaches. In many ways, IT network security planning parallels EH&S emergency planning and response. Both types of planning employ like processes. They include (1) assessing and prioritizing risks, (2) identifying mitigation strategies, (3) developing and implementing management systems, and (4) auditing the management systems on a regular basis.

Assess and Prioritize Risks

Many trade groups, computer hardware and software manufacturers, and standards organizations are getting serious about IT

security. The American Chemistry Council, for example, recognizes information and cyber security as a critical component of a sound security management system. It is developing a code of management practices for information and cyber security within its Responsible Care program.[3] Also, the National Institute for Standards and Technology (NIST) publishes a risk management guide that can be applied to many types of organizations.[4]

To understand your network's potential security risks, you may need to conduct a network assessment. Much like a security vulnerability analysis of chemical operations or an EH&S risk assessment, a network security assessment should evaluate where failures are likely to occur, which failures would cause the most harm, and which risks should receive the highest priority for mitigation. If your IT staff already has security policies and procedures in place, you may need only to verify your network security measures rather than conduct a detailed examination. A network security assessment might include a security readiness review and a risk assessment. A security readiness review should cover the following domains: general business practices, the IT environment, system, network, firewall, applications and databases, and hardware "clients."[5] A risk assessment follows the review and uses data gathered in these domains to identify where failures are likely to occur, which would cause the most harm, and to set priorities for mitigation.

Threats, vulnerabilities, and business requirements change, but your commitment to security should be constant. You should periodically reassess your network security to provide comprehensive protection. The frequency of reassessment depends on the size of your organization and the complexity of your IT systems.

Identify Mitigation Strategies

Once you have identified specific security risks, you can develop a mitigation strategy. This might include the use of multiple or "layered" security technologies that provide better protection than a single technology; one security measure can protect the network where another measure fails.[6]

Nearly all of the respondents in the 2003 FBI survey employ four network security technologies:[2] (1) antivirus software like Computer Associates, Norton, or McAfee; (2) hardware and software firewalls; (3) software access control (e.g., user login); and (4) physical security measures, such as locked server rooms and antitheft devices. Nearly three-quarters use intrusion detection software to recognize attacks that firewalls often cannot detect, and to provide data to assist in mitigation if a network breach occurs. Only a few companies today use biometrics

technologies, such as voice, eye, or fingerprint recognition to protect their networks.

Develop and Implement Management Systems

Good management systems have the support of top management, are dynamic, and involve the right people and resources. Two types of network security management systems are network security policies and procedures and disaster recovery plans.

Network Security Policies and Procedures. Network security policies and procedures must be clearly written and communicated throughout the organization. They also must come with proper training for all users, and must be enforced throughout the organization, or they will not be effective.

Network security policies and procedures might address

- User login to the network — policies and procedures for secure in-office, home-office, and remote dial-in access.
- Internet use — policies, procedures, and guidelines on the types of Internet sites accessible by employees and contractors, or policies on data and software downloads to prevent inadvertent virus attacks.
- Company intranets and extranets — policies regarding access to internal and external Web sites by employees, contractors, suppliers, and vendors, as part of their day-to-day jobs.
- Physical security of the network — policies and procedures to protect the physical security of server rooms, servers and equipment, and desktop computers.
- Use of company computers — measures to restrict access to sensitive company data by unauthorized users.
- Use of a virtual private network (VPN) — policies regarding access to network via VPN, with or without authentication devices such as tokens.
- Use of wireless devices — policies regarding password protection, use of wireless devises in public places, etc.

Disaster Recovery Plans. A disaster recovery plan can help organizations recover electronic data quickly after unauthorized access or in the event of a natural disaster, such as a hurricane, flood, or earthquake. As in EH&S emergency planning, the goals of a disaster recovery plan are to evaluate and prevent vulnerabilities, minimize serious business disruption, and ensure effective and speedy recovery. The disaster recovery plan should be tested periodically, reviewed at least annually, and updated as appropriate. It should be available to the designated disaster response team, and copies should be maintained offsite, in case the site cannot be accessed.

A disaster recovery plan might address

- The range of potential disasters that might occur — natural disasters, network breaches and viruses, software issues, human error, unforeseen circumstances, and hardware failures.
- Consequences of disasters — length and extent of outage, corruption of software, damage to hardware, need to restore backed up data, impact on users.
- Safety of critical documents and records — availability of hard copy and electronic backup data, onsite and offsite data storage, availability of backup data, time frame to restore critical documents and records.
- Priorities for data processing systems and operations — identification of the most critical data and systems to be restored when the network is brought back from an outage.
- Recovery strategies and tactics — address who, what, when, where, and how to recover systems and data. Address internal and external resources needed for recovery, such as the response team, potential need for an offsite command center and equipment, backup server sites, and power generating equipment.
- Testing criteria and procedures — periodic drills and tests to ensure the disaster recovery plan works *before* a disaster occurs.

If your network and the data within it are important to your organization, you need to protect them. Most organizations lack adequate network security planning, citing that it does not generate profits. As a result, network security often is reactive rather than forward-looking. Spending the time to identify and put into practice effective network security safeguards can provide many benefits, including the ability to quickly recover following a security breach, minimize network downtime and business interruption, reduce financial impacts, and lessen stress within the organization.

REFERENCES

1. *Study: Human Error Causes Most Security Breaches*; Strategic Research Corp., March 20, 2003.
2. *Eighth Annual Computer Security Institute/FBI Computer Crime and Security Survey*; Federal Bureau of Investigations, 2003.
3. *Implementation Guide for Responsible Care Security Code of Management Practices, Site Security, and Verification*; American Chemistry Council, July 2002.
4. Stonebumer, G.; Goguen, A.; Feringa, A. *Risk Management Guide for Information Technology Systems*; NIST Special Publication 800-30; National Institute for Standards and Technology, October 2001.
5. See http://www.hp.com/hps/security/sc_readiness.html (accessed Jan. 2004).
6. Wells, M.; Thrower, W. *The Importance of Layered Security*; Symantec Corp., September 10, 2002; available at http://enterprisesecurity.symantec.com/article.cfm?articleid=769&EID=0 (accessed Feb. 2004).

About the Author

Jill Barson Gilbert, QEP, is president of Lexicon Systems, LLC. She helps organizations increase business value by designing and implementing EH&S management solutions that leverage technology. A respected author and speaker, Gilbert is past chair of A&WMA's Information Solutions Committee. She can be reached at *JBGilbert@Lexicon-Systems.com*.