Holistic Approach to Network System Security

by Doug Nelson

Introduction

Information security concerns increase with expanded healthcare data access across wide area networks, increased storage on network devices, and greater use outside an organization's electronic borders. Today's information systems network architectures are changing rapidly, as are the methods for communication, storage, and viewing.

Each new method presents a unique challenge and raises the question of how information can be networked securely. If critical or confidential information is exchanged over a shared public data network such as the Internet or a frame relay network, organizations should consider who can see or gain access to such information. When an organization is networked through a wide area network, how can unauthorized users or intruders be detected, identified, and stopped? When confidential data are copied by centralized network storage back-up devices, organizations should consider how this information is handled after a backup. And when data is backed up for disaster recovery or migrated to an archival storage system, how will this data be securely restored and retrieved?

Defining the requirements for a network security solution is an intricate task. One piece of hardware, a suite of software, or a well-articulated security policy alone cannot provide complete and effective network security. Too often, information systems departments view network security through the single dimension of the electronic infrastructure. In fact, security is most effectively accomplished when organizations view it as an ongoing process that incorporates several interrelated areas of security.

This article describes a holistic approach to network security using closed loop corrective action. It presents a process that applies total quality management theory to the security domains of network technology, organizational policies, and the physical environment.

Closed Loop Corrective Action

The elements of an information system network security process fall into four phases.

1. Assessment or audit of the current security posture within an organization
2. Implementation of security methods and technology
3. .Measurement and monitoring of security methods/technology
4. Identification of security domains requiring corrective action

Figure 1 represents these four phases as a closed loop corrective action process.

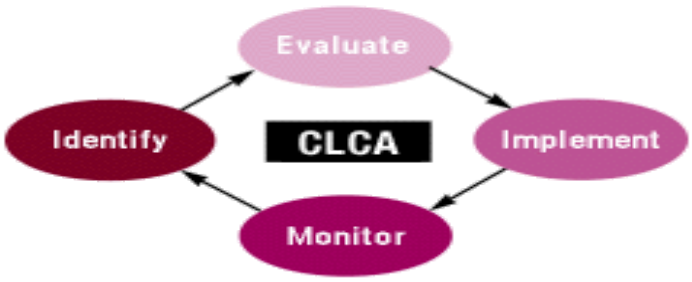
When an organization employs the process in all domains of information security, it can effectively avoid and abate the risks inherent in networked information systems.

Evaluation and Assessment Phase

In the initial phase of this holistic approach to security, an organization evaluates its posture from the perspective of the three domains of security: physical network operations, electronic network technology, and operational and legal policies.

Physical network operations
Quite often this dimension is referred to as the three Gs-gates, guards, and gun -- but it extends much further into the more subtle areas of the physical environment of a network. When assessing vulnerabilities, look for sabotage risks or equipment

Figure 1
Closed Loop Corrective Action



failure points in the areas where network equipment is located, such as wiring closets or communication demarcation areas. This is an area where many organizations leave their network and information exposed to potential infiltration. A wiring closet can be used by an intruder to gather privileged user information. All that an enterprising intruder has to do is find an unsecured wiring closet and hide a notebook-size network diagnostic analyzer that records all data traffic on a segment of a local area network. This includes system sign-on information such as user names and passwords. Later from a remote site or safe location, the intruder can use this information to access targeted systems.

An intruder posing as a confused end user can employ "social engineering" skills to get an organization's information systems help desk personnel to unwittingly give system access information. Of course, not all information theft occurs by sophisticated means; it can happen as easily as picking up printer output from a dumpster or taking system back-up tapes awaiting pickup or delivery from a building lobby.

An organization should evaluate the physical operations at its main site and at remote locations to expose weaknesses of all types, not only electronic vulnerabilities of the network.

Electronic network technology

An electronic map is the first step in evaluating a network for vulnerability. This permits penetration testing at potential host systems. The analysis should identify logical and physical network perimeters in addition to vulnerabilities inside and outside the network. Threats from inside the network are equal to or greater than threats from the outside; various studies estimate that 50 to 85 percent of all attacks take place from inside the network.

A thorough audit of the electronic technology should include all outside connections to the wide area network, including leased line facilities, frame relay connections, asynchronous transfer mode networks, switched dial modem, ISDN, and dedicated Internet connections. Many audits reveal that occasional users on departmental networks equip their workstations with modems and configure them for the convenience of remote dial-up access. This practice can leave a major opening for intruders to enter an organization's enterprise-wide network and can also act as a jump point to other organizations linked to the network.

Network services that can be accessed from the outside or between organizations like Web servers, e-mail, and file transfer programs all have unique vulnerabilities. Most information systems journals cover the latest network harassment or break-in techniques. The storylines are filled with exotic cyber-vernacular such as "denial of services attacks," "spamming," "SYN flood attacks," "hijacked-spoofed connections," "SATAN attack," and "ping of death." If an organization is planning to use the Internet for its many advantages, it would be prudent to audit the electronic aspects of its existing network connections and those of its business partners before proceeding with a network implementation.

Operational and legal policies

With the advent of computer-based patient records, many organizations are implementing effective information access controls and appropriate security policies. During an audit of these policies, emphasis is on the security of patient health information and rightly so. However, a complete audit should examine all the other legal and policy concerns of the organization's information systems infrastructure.

When many departments are connected via a common network infrastructure, the organization should review all policies pertaining to information security for conformance and consistency. It should review conformance with both criminal law and civil law. This review may bring additional liabilities to an organization in areas such as patient record information, theft and destruction of computer hardware, theft of software, copyright infringement, sabotage by computer, theft of data, theft of computer services, unauthorized modification of data, and misuse of e-mail.[1]

Implementation Phase

After an organization completes the evaluation phase, it should plan new procedures, technologies, and systems to address security deficiencies.

Physical network operations

All affected areas of an organization, not just the information systems department, should review the completed assessment of physical operational security. The requirements for heightened awareness of physical vulnerabilities in a network can include many departments in an organization. Physical security personnel should regularly check for unlocked wiring closet doors and suspicious equipment attached to network wiring locations. Organizations need to define procedures for securing information systems during emergency building evacuations like a fire alarm or bomb threat. Building plant operations personnel should be aware of the impact of electrical power outages on mission-critical systems and telecommunication networks. Human resources personnel should perform background checks on maintenance crews before they are permitted access to central information systems areas.

Electronic network technology

Effective measures for electronic security fall into five basic areas: user authentication, access control, encryption, intrusion detection, and audit logs. User authentication can occur at many points in the users' information access procedures, often by password on the host system. However, the network or attached devices can employ other methods to ensure that a user is authentic. An authentic user often carries a token-generating device that creates a constantly changing numeric value. When the user logs on to a network or system, the current value of the token is entered and compared to a narrow range of possible current values. If they match, this implies that the user logging on to the system knows a valid password and possesses a unique token-generating device. Biometric devices that validate the user, such as fingerprint match, voice wave recognition, and retina scanning are becoming more widely available.

Access control on a network, particularly a network that involves many local area network (LAN) segments or wide area network (WAN) connections, employs security devices commonly called firewalls. The most popular location for a firewall is where an organization's LAN connects to a public WAN like the Internet. Essentially, a firewall blocks certain users from gaining access to a network, or it controls the types of information the user has access to.

Configuring firewalls can be complex and arduous if an organization doesn't have a clear idea of what its network looks like or what it wants to secure. Firewall hardware technology falls into two basic categories-a proxy host CPU system and a packet filtering router/switch. Each method offers its own advantages and disadvantages; factors such as the number of simultaneous users, network speed, and the amount of data throughput help determine which technology to use. Organizations can use a combination of both technologies. The real key to either firewall technology is the flexibility of the software in the device and the speed at which it operates so that the firewall does not become a bottleneck on a network. Organizations should also consider the following factors in the implementation of a firewall: the methods it uses to generate audit logs or how it reports to logging devices. Besides audit logging, information security personnel should know how to use it effectively to detect intrusion attempts from outside and inside the network.

The authentication devices and access control features of a firewall can be part of an effective security system, but organizations should consider who can see data when it passes across a network. Cryptography is a method long used in the military, intelligence organizations, the financial sector, and now on the Internet to keep data private. When data is manipulated through a variety of mathematical algorithms, the result is unintelligible cipher text. When this manipulation, called encryption, is performed on data before it crosses a network perimeter on to a public data network, a hacker or network maintenance personnel sees the transmission as cipher text. Only the intended destination that holds the key to the mathematical algorithm can decrypt the information packets. In public networks, an organization can create a private sleeve over its information (Figure 2) and still have the convenience and ubiquity of public packet networks. This makes it very economical to share information with remote locations and business partners. More powerful encryption methods employ an additional feature that guarantees message integrity. It provides proof of who generated the information and that the message has not been modified since it left the originator.[2]

Operational and legal policies

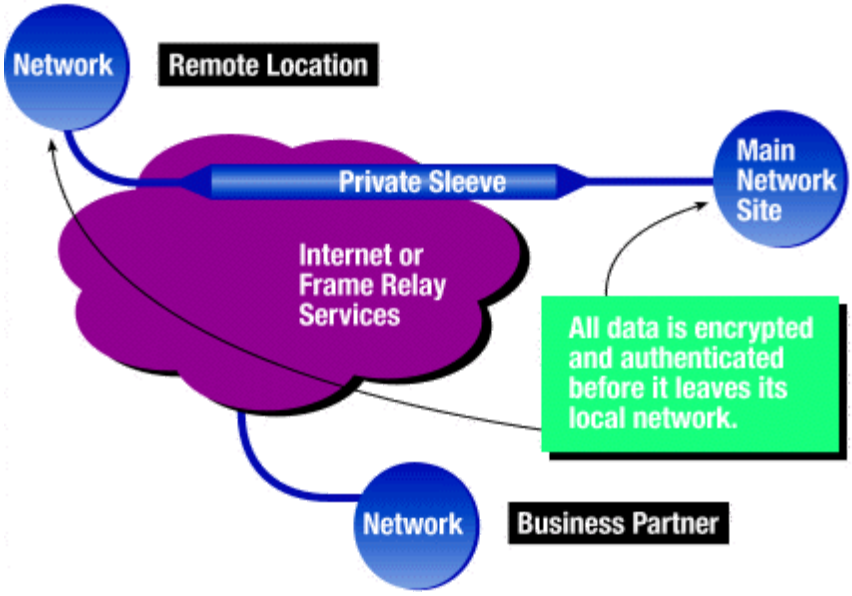
Operational and legal policies should address the shortcomings that the organization identified in the assessment phase. If an information security committee or council did not exist prior to the audit, the organization should establish one composed of managers and senior staff members who represent users and creators of information.[3]

The committee's task is to develop policies that define the organization's expectations of proper computer and network use and procedures for handling improper use. There should be a plan to educate users on the new policies and other aspects of computer network security.

Monitoring Phase

In the monitoring phase of the closed loop corrective action process, the organization observes all the implemented security improvements to ensure that they continue to adequately address security deficiencies. In addition, other key activities to this phase include keeping abreast of changes in network technologies, new laws or standards, intruder break-in techniques, and reported security breaches in other organizations.

Figure 2
Cryptography Over a Public or Private Wide Area Network



Electronic network technology

The primary elements in monitoring network security are audit logs and expert system-based intrusion detection devices. Both elements track down an intruder and provide the necessary proof or evidence for prosecution. Also, when an organization suspects that its system data have been compromised and information integrity is in question, up-to-date intrusion detection systems, together with properly maintained audit logs, can offer proof that only authorized users had access to the network.

Intrusion detection technology can be used in conjunction with firewall solutions or as a stand-alone device that remains connected in the background of a network. Using an intrusion detection system with a firewall router, organizations can detect network attacks by potential intruders in real time and abate them within seconds. Many freely distributed software tools exist for hackers. When they are applied against a targeted system, the tools help the hacker interrogate and probe that system for openings. Several available intrusion detection systems keep profiles of all known "signatures" of these attacks in order to recognize them while they are in progress. Once the attack has been identified, a shun is put in place to stop the intruder before he can finish the probing attack. Sometimes it is desirable to divert an intruder to a "safe" system area to keep him busy; this gives network security personnel time to trace the network connection or to see what the intruder may be looking for. The systems that use expert technology learn from each new attack technique and create new attack signatures. Organizations can use an intrusion detection system to stop attacks from both outside and inside their networks. When combined with audit logs, organizations selectively monitor network transactions from inside the organization for suspicious activity. If unauthorized connection attempts are made from within an organization, those activities are recorded and operations personnel notified in real time.

Identification Phase

In the fourth phase of the model, the organization identifies corrective actions. Here it identifies security areas and makes adjustments. The results of this part of the process are cycled back to the beginning phase.

Audit logs should be analyzed for events and trends that indicate unusual user behavior. Security personnel should back up logs regularly and safely store them. Electronic security technologies should always be current with the most reliable releases of hardware and software. Organizations need to keep current with legal requirements and reevaluate ineffective security policies.

Conclusion

Networks and information systems change continuously, thus it is important to have a security process that endures change. Organizations can achieve complete and effective network security by employing a holistic process and repeatedly assessing, implementing, monitoring, and identifying through a closed loop corrective action.

Notes

1. Adler, M. Peter, and Erika Koster. *Law and Computer Networks*. Minneapolis: Oppenheimer, Wolff and Donnelly, 1996, pp. 4-12.
2. Kaufman, C., R. Perlman, and M. Speciner. *Network Security-Private Communication in a Public World*. Englewood Cliffs, NJ: Prentice Hall, 1995, p. 52.
3. Miller, Dale. "Updating Information Security Policies." *In Confidence* 4, no. 6 (1996): 6.

References

Behar, Richard, Amy Kover, and Melanie Warner. "Who's reading your e-mail?" *Fortune Magazine*, February 3, 1997.

Doty, Ted, StorageTek Network Systems Group. "The Firewall Heresies." http://www.network.com/Corporate Area/Library/heresies.htm. 1996.

Scheier, Robert. "Lock the Damned Door!" *ComputerWorld*, February 10, 1997.

Sutterfield, Lee, and Todd Schell. "Security Posture Assessment." WheelGroup Corporation Web page, http://www.wheelgroup.com/securlib/SPA-whitepaper.doc.bin. July 14, 1996.

Doug Nelson *is a marketing representative with StorageTek of Houston, TX.*

Article citation:
Nelson, Doug. "A Holistic Approach to Network System Security." *Journal of AHIMA* 68, no.5 (1997): 20-24.
