Primer on Network Security

Save to myBoK

by Margret Amatayakul, RHIA, CHPS, FHIMSS

The lack of specificity in HIPAA's transmission security standard for "guarding against unauthorized access to electronic protected health information (EPHI) that is being transmitted over an electronic communications nework" may leave you a bit cold, especially the portion of the preamble that states, "Features...associated with a proposed requirement for 'Communications/network controls'...have been deleted since they are normally incorporated by telecommunications providers as part of network management and control functions that are included with the provision of network services."

While telecommunications providers and vendors of network devices do supply a lot of security features, how you construct your internal network has a lot to do with your ability to prevent external attacks from doing harm to EPHI that resides in your systems and to reduce internal threats to EPHI. Security depends on the type of systems deployed and the scope of connectivity required.

Know Your Environment: Network Security Scenarios

Mainframe Environment

Some providers may still have some legacy systems that deploy a mainframe computer and "dumb" terminals. These systems do not connect to the Internet and do not afford remote access as we know it today. In a mainframe environment, remote access essentially was how far you could string cable to connect your terminals. As such, little additional technical security was needed beyond access, authentication, audit, and integrity controls for data at rest.

Client-Server Environment

Most providers have adopted a client-server computing environment. Local area networks (LANs) manage access by client computers to data and applications held within server computers. A network operating system (NOS) runs the networked computers. The most common NOS platforms are Windows 2000, Windows NT, Novell, and UNIX.

Each computer or other peripheral device (for example, a printer) must have a network interface card (a NIC), or LAN adapter, to enhance the digital signals of data for transmission through the network cabling. Various types of cabling are used, including hardwire (copper cable that transmits electrical pulses or fiber-optic cable that transmits light pulses) or wireless (using radio or light waves). One or more wiring hubs, depending on the type and configuration of the network cabling (for example, Ethernet, token-ring), may be used to manage the cabling.

LANs can be self-contained within a facility, or they can connect to the Internet. Modems may be used to dial up to the Internet through the plain old telephone system (aka POTS), or a terminal adapter may be used to attach phones to an integrated services digital network (ISDN) line.

There are various ways to configure a LAN to reduce cost and heighten security. For example, some providers use "thin" clients with minimal or no processing and storage capability. As a LAN grows, a network management system may be necessary to monitor network activity, and network partitioning may be used to create discrete security zones. Still, if the LAN has no connection to the external world (either directly to the Internet or to other LANs that have such a connection), it is less vulnerable to external security threats.

Integrated healthcare delivery systems need to connect one LAN to another. A variety of communication links may be used, with distance, speed, volume, connection time (permanent or temporary), and cost contributing to the choice.

Until recently, most conservative providers preferred to use private frame relay, ISDN, or digital T1 lines leased from telephone companies. Bridges, routers, and switches are used to connect and disconnect remote users. Asynchronous transfer mode (or ATM) services permit transmission of video and digitized sound data. For greater distances (in wide area networks, or WANs), microwave or satellite services may be used. Digital subscriber line (DSL) and cable services may also be used, although these tend to be used by small offices or for connectivity from home. Again, your security threats are lower if you can be certain that there is no external connectivity within any of the components of your LAN or WAN— although today this is virtually impossible to ensure.

Browser-based Computing Environment

The Internet has brought not only convenient messaging and access to an amazing web of information, but it has also brought new technologies to information management. Many of these new technologies are finding their way into health-care computing.

An intranet is essentially a LAN (or WAN) that provides Internet-like services for authorized members of the work force and others. These services include access to internal e-mail and the means to provide secure e-mail with patients and business associates. The Internet's Standard Generalized Markup Language (SGML) and derivatives provide the ability to search for and share documents across any computing platform.

An intranet adopts this browser-based technology to help authorized users gain access quickly and easily to policies and procedures, training materials, and other resources that the organization may provide through its intranet. An extranet may extend such access to affiliates, business associates, and patients.

Finally, some providers are beginning to use a virtual private network (VPN) to transmit data through the Internet using a special protocol to create a proprietary tunnel.

From the Top Down: Network Security Layers

As greater connectivity occurs, even with trusted partners and most certainly via the Internet, providing transmission security is no longer just about having antivirus software and a firewall. Many security experts believe a layered approach is necessary to thwart unauthorized access, alteration of data, and denial-of-service attacks.

In a layered approach, your risk analysis determines exactly what controls are needed at each level:

- **Perimeter** is the outermost layer (the next layer out being the Internet or any other network with a different level of trust associated with it). Within the perimeter, the most common security controls include one or more firewalls and a set of strictly controlled servers managing other security functions located in a portion of the perimeter often referred to as the "demilitarized zone" (DMZ). Servers in the DMZ, such as e-mail servers, may contain software to protect against malicious code. An intrusion detection system can be added to detect intrusions that have circumvented or passed through the firewall or are occurring within the LAN behind the firewall. VPNs typically terminate within the perimeter layer.

- The **network** layer of security should have access controls and authentication services for both users and devices connected to the network. Other protections may include intrusion detection systems (IDSs), if they are not located within the perimeter layer, and network vulnerability assessment services that scan devices within the network for flaws and vulnerabilities that could be exploited by harmful traffic.

- The **host** layer of security focuses on individual devices such as workstations and network devices. Access controls, authentication measures, and IDSs can be applied here, although managing them at this level can be extremely time consuming, especially in a heterogeneous environment. Most providers reserve such controls for special-function servers. Modems are another source of vulnerability, permitting dial-up access from a workstation, even in some cases where there is hardwire connectivity. Downloads, instant messaging, and other unprotected connectivity are huge threats. A large organization may want a "war dialer" to identify open modem lines that normally should be off or are unauthorized. A similar tool should be used to detect rogue wireless access points in a wireless LAN. Another host-level

security function is “platform hardening” to ensure that unnecessary services, software, and users are removed from all platforms on which Web pages, databases, and other types of applications, data, or software reside.

- The **application** layer of security is where controls for data at rest are generally applied. Application-layer firewalls may also be installed on Web servers, e-mail servers, and other special devices to thwart internal attacks. Integrity controls in the form of data edits are not strictly security controls, but they could prevent keying errors from causing alteration or destruction of data.

- **Data**-layer security controls are the last line of defense. An important control here is contingency planning, including data redundancy and backup. Integrity controls ensure that data are not altered when stored or transmitted. Encryption is the strongest form of data security. Encryption for data at rest is an addressable implementation specification within HIPAA. Most providers will use encryption primarily when data are transmitted outside of a proprietary communication link.

Arranged like the layers of an onion, security layers protect against single points of failure in your network.

Margret Amatayakul*(margretcpr@aol.com) is president of Margret\A Consulting, LLC, an independent consulting firm based in schaumburg, IL.*

Article citation:
Amatayakul, Margret. "A Primer on Network Security." (HIPAA on the Job) *Journal of AHIMA* 75, no.3 (March 2004): 56-57.
