HIPAA Security Shopping List (HIPAA on the Job)

by Margret Amatayakul, MBA, RHIA, CHPS, FHIMSS

Many information security officials are barraged with requests for the latest security tools. Such shopping lists often do not reflect a structured plan or a true risk analysis to justify their cost or human resource requirements. This column describes some of the latest tools, how you can evaluate their effectiveness for your organization, and how you can integrate policy and technology to achieve a balance of cost and benefit from security controls.

Security Expenditures: A Bare Necessity

For healthcare, the rationale for security expenditures is primarily the HIPAA security rule compliance deadline of April 21, 2005. But in general, there is more Internet use, more malicious code more often (e.g., viruses and worms), and more publicity about privacy and security issues. This leads to more interruption of information technology services and constant—and costly — emergency security activity. As a result, many new security "appliances" are being developed and marketed.

Checking out the Options

Many of the new security tools provide excellent support and significant value. But some are also highly sophisticated, requiring specialized skills and knowledge for implementation and use. For example, a security event management (SEM) appliance is a central repository that collects and correlates security event and alarm information from multivendor, heterogeneous security tools, such as intrusion detection systems and vulnerability assessment tools. SEM appliances were created because these other tools were producing so much data that it was impossible for humans to process it all.

While SEM helps process the data, it is only useful if you have the many intrusion detection systems, vulnerability assessment, and other tools that capture system security event data. But if the organization has done a good job of providing antivirus coverage, has hardened its servers to reflect organizational needs, is disciplined about applying vendor security patches, and adopts a layered approach to internal and external firewalls, SEM may not be necessary.

Consideration must also be given as to whether the organization has sufficient staff resources to handle the new, highly sophisticated tools. Having an intrusion prevention system (IPS) may sound like a way around adding staff resources for constantly quarantining files targeted by an intrusion detection system (IDS), but if the organization cannot anticipate its incoming mail sources, it is possible that staff will spend just as much if not more time attempting to rectify problems associated with blocked mail.

Another set of tools include low-priced devices that filter content, help you avoid spam, and make users aware of social engineering—the use of nontechnology or low-technology means to gain access to and attack a system (such as impersonation, tricks, bribes, blackmail). Even if the cost of these devices does not seem like a great expenditure, the human resources that must be applied to properly implement, manage, and keep them up to date may be enormous.

In addition to skill and staff requirements, policy must support the technology. For example, it does no good to have sophisticated audit trail pattern analysis tools if executive management will not act on their findings. Similarly, robust access control systems with "break-the-glass" capability for emergency access procedures will not be effective if roles are not assigned properly and users are free to misuse their privileges.

Finding the Right Fit

Most importantly, all potential security tools should be evaluated in light of a risk analysis and how they fit into an overall security architecture. In fact, it is probably a better approach to conduct a risk analysis and then look for tools to solve the problems identified, rather than to take a list of desired tools and attempt to decide which ones fit.

While it is true that healthcare information systems are becoming more vulnerable and threats greater, an organization must weigh the likelihood that a threat will actually exploit a vulnerability against the cost of controls designed to thwart the threat or plug the gap.

Many security experts suggest that an actual return on investment (ROI) analysis be conducted as part of the risk analysis. As with the security tools themselves, caution should be applied here. Some security tools should be cost justified, but other tools may have to be acquired no matter what.

The Meta Group suggests that for information security "not every expense is an 'investment.'"[1] Because of regulations, it may be necessary to incur an expense, even though there may not be high degree of risk. For example, audit control is a HIPAA standard. If a system containing protected health information does not include audit trail capability and you have no other means of recording and examining system activity, whether there is high risk or not, you will need to incur the expense of implementing some form of hardware, software, or procedural mechanisms to achieve audit controls.

Alternatively, HIPAA is very nonproscriptive and supportive of the risk analysis process. Therefore, there may be tools that clearly save money, help avoid cost, or improve productivity. For example, security identity management (SIM) is a set or suite of tools bundled together that support various access control, authorization, user account administration, automated password reset, password synchronization or even single sign-on, and termination of account procedures.

In a large organization, especially an integrated delivery network, SIM tools may yield a positive ROI. For a smaller organization where there is one primary application and low work force turnover, SIM tools probably could not be cost justified, nor are they an expense that the regulation would require.

Enterprise security management is another example of a new suite of tools that can be just right or overkill. These suites provide configuration management (i.e., change control), security policy management, security patch management, and remote device management.

Trying It on for Size

Finally, tools must be implemented in a manner that fits their environment. There must be an overarching plan that rests on executive management support and risk analysis; is policy driven; engages the user community; addresses application needs, operations, and physical security as well as technology; is properly implemented with training; and includes a feedback mechanism for ongoing compliance assurance. "Policy and Technology Integration Pyramid" illustrates this general security program.

Within the technology, a layered approach ensures networks are segmented into secure domains. "Technology Layers for a Security Program", below, illustrates a layered approach to security and fits the tools described in this column to the applicable layer.

Note

1. Scholtz, Tom, Chris Byrnes, and Carsten Casper. "Information Security ROI: Not Every Expense Is an 'Investment.'" Tech Update. September 10, 2003. Available online at http://techupdate.zdnet.com/techupdate.

References

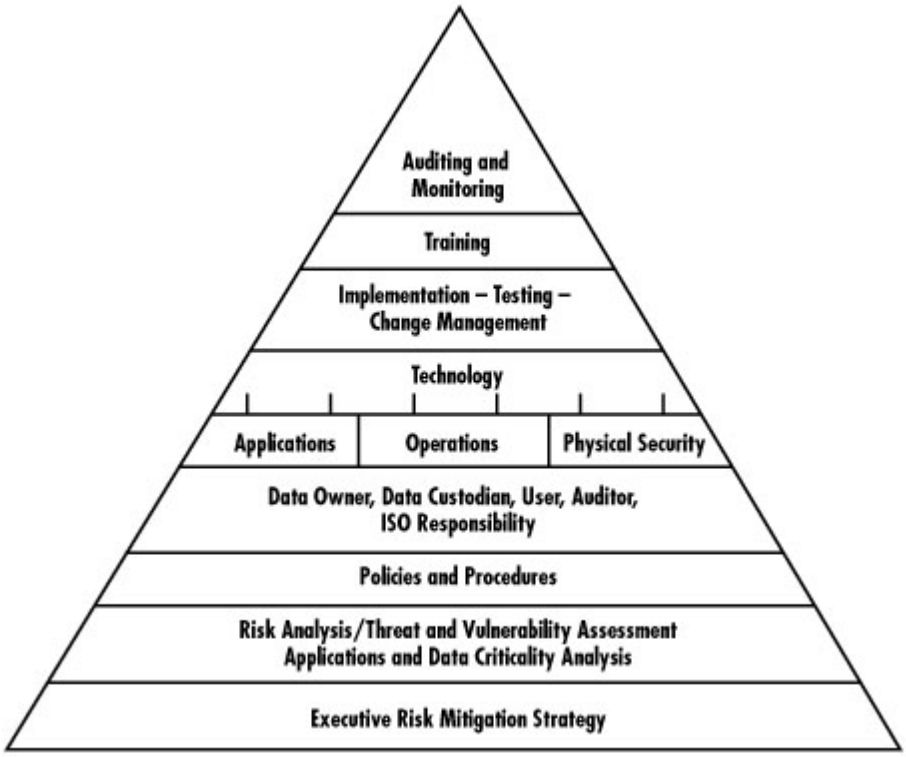
Amatayakul, Margret. *Implementing the Electronic Health Record: A Practical Guide for Professionals and Organizations*. Chicago: AHIMA, forthcoming.

Amatayakul, Margret, and S. S. Lazarus. *Complete Guide to HIPAA Security Risk Analysis: A Step-by-Step Approach*. New York: Brownstone, 2004.

NIST SP 800-53, First Draft. "Recommended Security Controls for Federal Information Systems." Available online at http://csrc.nist.gov/publications/nistpubs/index.html.

Technology Layers for a Security Program
Perimeter
Firewalls
Virtual Private Network
Wireless Network Encryption
Network
Antivirus Tools
Intrusion Detection/Prevention Systems
Vulnerability Assessment
Network Partitioning
Host
Platform Hardening
Application
Security Event Management/Security Information Management Tools
Data
Enterprise Security Management
Security Identity Management
Public Key Infrastructure

Policy and Technology Integration Pyramid



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

Article citation:
Amatayakul, Margret. "The HIPAA Security Shopping List." *Journal of AHIMA* 75, no.5 (May 2004): 58-59.