Securing Executive Support for Security (HIPAA on the Job)

Save to myBoK

by Margret Amatayakul, RHIA, CHPS, FHIMSS

Many information privacy officials (IPOs) and information security officials (ISOs) may be facing what seems like an uphill battle to gain support for security measures believed to be necessary to comply with the HIPAA security rule. There are a number of converging factors that can influence executive management and a number of steps IPOs and ISOs can take to help their cause.

Executive Support

Executive support is obviously needed for the assignment of resources for a security official and budget for security controls. Some executives may think compliance with the "mini-security rule" in the privacy rule is sufficient. They may also decide that with little evidence of privacy rule enforcement and without the occurrence of an adverse security incident that current security measures are sufficient. The key, however, is that without a risk analysis that matches threats and vulnerabilities in your environment to the actual risk executive management is willing to assume, it is impossible to determine whether current security measures are sufficient.

Executive management support is needed not only to assign the appropriate individual to the function of information security, but to:

- Define their risk position and establish a risk mitigation strategy
- Approve security controls and understand their residual risk
- Support ongoing security monitoring
- Create an environment of security awareness

External Influencers

An important business case can be made to support security by referencing the Sarbanes-Oxley Act (Public Law 107.204), but a connection may need to be made between securing electronic protected health information (EPHI) and what may be perceived as solely an accounting issue. Signed into law after the Enron and other public company accounting practice scandals, the act is controversial, only applies to publicly traded companies, and therefore directly affects only a certain segment of the healthcare industry. It requires an adequate internal control structure and procedures for financial accounting and reporting. Many industry observers, however, note that a secure information infrastructure is central to internal controls and that the act's principles will transfer to nonprofits as a standard of practice.

Another important factor for executive managers to consider is increasing risk of identity theft and other cyber crimes. These criminal acts frequently are not targeted at EPHI, but at the identity of patients, and possibly even the provider's own identity, for perpetrating other types of crimes such as writing illegal prescriptions. Many of the techniques used to carry out such crimes involve no technology or low technology and must be thwarted by continual awareness. With increasing issues surrounding health insurance and costs of drugs, heightened interest in electronic health records, and the finalization of the HIPAA National Provider Identifier expected this winter, healthcare may become an even easier target for cyber crimes in the future.

Internal Considerations

Having built a case for support, IPOs and ISOs also need to do their part. The best IPOs and ISOs will be passionate about privacy and security, but must be equally capable of using a strategic approach that is:

- Reasonable. Especially for general security professionals, it must be recognized that the traditional approach drawn from the US Department of Defense (DOD) does not work in healthcare. Some risk is unavoidable in order to provide proper healthcare to patients. In fact, recognizing that EPHI would be classified as "confidential" in the range of "top secret" to unclassified, and that systems would be rated C2 by DOD standards, may help put HIPAA security into perspective.[1] HIPAA supports a reasonable approach through its risk analysis requirement and addressable implementation specifications.
- Synergistic. There are many competing demands for executive attention and support. Coupling discussion of HIPAA security with other strategic initiatives will build awareness with executives and support integration of security. This should not diminish the importance of security, but rather it will make it an integral part of all internal control requirements. IPOs and ISOs should cultivate relationships with those responsible for other internal controls, such as in patient financial services, pharmacy, and HIM, and gather momentum for security through a well-planned and coordinated approach.
- Channeled. As much as IPOs and ISOs may want the HIPAA security rule to be on every executive's agenda, it may be necessary to work through channels within the organization. It can help to identify who or what has the most attention currently and channel security through them or their initiatives. Using corporate compliance, risk management, and an executive sponsor are also built-in channels to deploy for success.
- Documented. HIPAA requires documentation, so IPOs and ISOs should use this to their advantage. But rather than just applying documentation from the perspective of documentary evidence, documentation of threats and vulnerabilities, costs and benefits, and alternative control mechanisms may point to more cost-effective and efficient means of accomplishing the desired security. For example, if an intrusion detection system is on your "must-have" list, do the math and you may find that a more layered firewall configuration may be just as effective, with lower capital outlay and much less labor.

Pick Your Battles

There are many clichés that could apply to the position IPOs and ISOs find themselves in with respect to getting executive attention for HIPAA security rule compliance. "Pick your battles" may be apropos. Executives deal with strategy, which was originally a military term that meant the art of planning and directing large-scale military movements (e.g., a war). IPOs and ISOs deal with tactics, which, in the military sense, means the art of deploying forces and maneuvering them in battles.

In addition to providing perspective, these definitions recognize that both planning and maneuvering are art forms. IPOs and ISOs should cultivate the art of recognizing where they must be reasonable. Remember, just as the commander in chief plans the war, executives determine their risk position. While that in itself is not an easy task for healthcare executives, once defined, the IPO and ISO should rely on that as their benchmark for recommending controls—so long as the residual risk in those controls is clear.

Note

1. US Department of Defense. "Trusted Computer System Evaluation Criteria." DoD 5200.28-STD. 1985.

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

Article citation:
Amatayakul, Margret. "Securing Executive Support for Security." *Journal of AHIMA* 75, no.2 (February 2004): 54-55.