Compliance Today - March 2018
Building a security program: It's not just IT

By Eric Hummel, MS CS, InfoSec

Eric Hummel (eric.hummel@qipsolutions.com) is Chief Technology Officer at QI Partners, LLC in Rockville, MD.

As the saying goes, "To a hammer, all problems look like a nail." Most healthcare companies start their Health Insurance Portability and Accountability Act (HIPAA) security program by assigning responsibility and accountability to a manager of Information Technology (IT). This creates a bias within the organization that security compliance is an IT issue. In reality, much of security does not directly involve IT. The result is that non-IT risk gets overlooked, and the IT team takes on a security enforcement duty that is both uncomfortable and ineffective.

The need for security compliance is not going away. It is rapidly taking on increased importance in all organizations. Losses are starting to become significant and threats are increasing. Security is an ongoing requirement for all organizations in the 21st century. A security program needs to be built for efficiency and longevity. It needs to manage risk in a way that also meets the compliance requirements of HIPAA and state laws. This makes the choice of an organizing principle for your security program much more important.

Managing risk

Merging the twin requirements of HIPAA compliance and the need to manage risk in medium or small healthcare organizations is challenging at best. The compliance side demands that a thoroughly documented program be in place that meets certain minimum requirements. The risk side of security needs to meet the real threats of ransomware and data breaches that harm reputation and bottom line. In many communities, expertise is neither affordable nor available to plan and lead in this complex situation. But, these are compatible requirements, particularly when managed as a single program.

Left searching for cost-effective options, organizations reflexively turn to their IT staff, assigning the Chief Information Officer (CIO) or an IT manager the new responsibility for security compliance. This person is proficient in technology and possibly technical data security, but they are rarely experienced in organizational risk management. Beyond having the added burden of planning, execution, and continuous monitoring of risk and compliance, they also must lead a program that encompasses workflows throughout the organization. Internal IT professionals should be focused on ensuring complex security aspects such as data loss prevention or security event and incident monitoring. However, things like business associate agreements and better staff background checks will likely be out of their experience range. Even though cybersecurity may seem like an IT issue on the surface, security compliance is process oriented, and risks come from all directions, not just IT.

Security is a risk management process, not an IT function. Like other business or medical risks, security should be viewed as a process to minimize potential losses by controlling sources of risk. IT is one source of risk, but there are many others that may be more important:

- Human error is a major source of risk that IT may be poorly suited to address.
- The physical layout and security features of a clinic can help or hinder security.

- Effective staff training is both needed and key to reducing human error.
- Clinical and operations staff are key stakeholders and have vast knowledge that is needed when planning for disaster or emergency operations.

These are all functions of security risk management.

Ultimately, all of these risks, whether IT, HR, clinical, financial, legal, or administrative, should be the concern of the entire organization.

Security Stakeholders

- Executive management
- Administrative operations
- Clinical staff
- Human Resources
- Information Technology
- Physical Plant
- Finance
- Risk and Compliance

If planned correctly, compliance will be the natural result of a comprehensive security program led by someone who understands both the risk management methodology required for security and the HIPAA compliance documentation requirements.