Creating a strong data security program

Support strategic initiatives with the right mix of technology.

By Ron Ropp and Becky Quammen

This article is part three of the Quammen three-part security series. Parts one and two were published in the July and October 2015 issues of *Health Management Technology*.

Security threats in healthcare are becoming more prevalent – and, therefore, worrisome. Consider the following: In 2014, more than 12 million healthcare records were breached. And the situation became even more dire in 2015, with more than 94 million records breached from the beginning of the year through June 26, according to the United States Department of Health and Human Services (HHS).[1]

With the threat front and center, healthcare organizations are ready to take action. In fact, 87 percent of healthcare professionals indicated that information security had become a critical business priority, according to results of the HIMSS 2015 Cybersecurity Survey,[2] which included responses from 297 healthcare professionals.

And it looks as if healthcare organizations are ready to move forward, purchasing and implementing the tools necessary to keep risk at bay. Indeed, 63 percent of organizations are planning to increase spending to offset data threats, according to a Harris Poll survey of 920 IT decision makers conducted on behalf of Vormetric, a data security solutions vendor. And 81 percent of the professionals surveyed in the HIMSS study believe more innovative and advanced tools are needed.

The challenge for you, as a healthcare leader, is to actually implement the technologies and tools that will support your strategic security initiatives. To do so, you need to ask the following questions:

- Is your security infrastructure current and keeping up with the evolving threat landscape, or is it static and in maintenance mode?
- Do you have the technology tools that will support the three "Ps"? That is, do you have technology in place that will enable your *people* to adequately implement security *policies* and follow established security *procedures*?
- Do you actually know what tools you have up and running – and what technologies might fill in the gaps?
- Are you considering the fact that many of your staff members bring their own technology into the mix? Do your security plans account for these "bring your own cloud" or "shadow IT" movements – both of which refer to technology, apps, and infrastructure that are being used within your organization outside of the IT department's sanctioned technologies? Are you protecting data that is potentially being stored by employees in Dropbox, Evernote, or iCloud?

By answering these questions, you can better determine what tools you need to support your strategic security initiatives, instead of simply buying the next big thing from each and every vendor that knocks on your door. In essence, you can create a security technology purchasing initiative that enables your organization to identify where your risk is greatest and then take action on the most pressing priorities, ultimately purchasing and implementing the tools that will offer you the greatest protection.

When creating such a program, you are likely to assess the viability of the following tools:

Security risk assessment technologies. Because your organization handles protected health information, you must regularly review the administrative, physical, and technical safeguards that you have in place to protect the security of the data. By conducting these risk assessments, you can identify potential weaknesses in your security policies, processes, and systems. Risk assessments can also help providers address vulnerabilities, potentially preventing data breaches or other adverse security events. In fact, the Office of the National Coordinator for Health IT, in collaboration with the HHS Office for Civil Rights and the HHS Office of the General Counsel, has developed a downloadable Security Risk Assessment Tool[3] to help guide organizations through the process.

Intrusion detection systems (IDS), intrusion prevention systems (IPS), and firewalls. Firewall and IDS technology has been around a long time,

Ron Ropp, Chief Technology and Security Officer, **Quammen Health Care Consultants**

Becky Quammen, CEO, **Quammen Health Care Consultants**

as have newer IPS tools that monitor and respond to threats. However, when purchasing these tools, it's important to remember that security incidents are no longer isolated events. The threats are advanced. Proactive security is required to maintain protection. No longer can you simply build a bigger and higher wall. The threats have been able to evolve faster than these systems that can identify them using "signatures." Newer next-generation IPS systems or firewalls (sometimes called NGIPS or NGFW) allow for more sophisticated prevention and response. The typical traits of a next-generation system are application awareness, network awareness, identity awareness, behavior awareness, and the ability to dynamically tune itself based upon the data it gathers.

Security information and event management (SIEM). You likely already have logging and monitoring of some sort in your various technologies in place. But do you have a way to gather this information centrally and manage the volumes of log and event data that exist? Does it give you actionable information? And are you looking at the right things? There are many vendors and tools that provide SIEM capability, but first it's important to determine your scope. Are you simply complying with a regulatory requirement or an enterprise implementation, and what are the critical things you want and need to know?

Mobile device management (MDM). These tools and software products are used to centrally manage your mobile devices. As BYOD and other mobility initiatives are more "the norm," do you have the platform that protects your organization? MDM systems typically implement administrative features on mobile devices that allow you to secure functions like email, applications, and Web browsing, and place potential restrictions on devices.

Encryption. Do you have tools in place to make it easy to encrypt email and other network systems transmitting data? Some phones and newer operating systems offer encryption by default for the entire device. Even better, do you have tools that examine content and automatically encrypt emails upon distribution, in addition to a strong policy on what can and cannot be sent? Have you conducted an inventory of your systems that communicate in house, and are they securely transmitting all information? Such a review should include file shares, the intranet, portals, etc.

The most important thing to remember is that you must always consider risk and security management as a core and ongoing function, and not a one-time event. Keeping information security tools in your annual budget is a requirement and should be accounted for continually as the threats become more sophisticated and the data more pervasive. **HMT**

REFERENCES

1. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

2. http://www.himss.org/2015-cybersecurity-survey

3. https://www.healthit.gov/providers-professionals/security-risk-assessment

Reprinted from November/December 2015

Health Management TECHNOLOGY™