Quest for Managing Cyberthreats in Healthcare

Save to myBoK

By Susan Carey, MHI, RHIT, PMP, FAHIMA

So far 2017 is shaping up to be the year of fear in the realm of healthcare cybersecurity. There was a 61 percent increase in healthcare cyberattacks in 2016. This followed two years of steadily increasing cyberthreats in healthcare, including 93 major cyberattacks in 2016 resulting in compromised health records, reputational harm, and significant financial burden. Some of the largest attacks affecting the security of health records, according to an article in *Dark Reading*, were:[1]

- Newkirk Products—3.4 million records
- Banner Health—2.2 million records
- 21st Century Oncology—2.2 million records
- Valley Anesthesiology—880,000 records

Factors in Rise of Cybercrime in Healthcare

Why are cyberattacks increasing within the healthcare ecosystem? Why are cybercriminal adversaries turning toward the healthcare industry and away from other industries such as the financial industry? As evidenced by the numbers above, adversaries have more entry points than ever before, making healthcare entities an easy target for sophisticated hackers. Some of the healthcare entry points most susceptible to attacks are mobile, e-mail, third party cloud applications, medical device hijacking, and adware.

Industry experts believe that many healthcare organizations failed to adequately address the need to protect electronic patient data—or were simply unaware of the complexity of securing electronic health records (EHRs)—which made them a target for cybercrime.

Most healthcare IT shops have been spending capital budget on EHRs and operating systems to meet the requirements set forth in the 2009 HITECH Act. As a result, there was not enough capital or time to focus on protecting electronic patient data while simultaneously implementing an EHR. Now healthcare organizations find themselves way behind in implementing those security measures.

Organizations now have to place a concerted effort on budgeting for staff and resources to develop effective methods to prevent, detect, and mitigate risks as part of safeguarding electronic personal health data (ePHI) in response to ransomware and other types of cyberattacks. Security efforts and resources are being directed toward the most vulnerable areas of attack such as mobile devices, cloud infrastructure, and end-user behaviors. Also, additional security measures are being assessed in terms of managing the PHI maintained within EHRs.

<table>
<tr><th colspan="3">Project Management Plan</th></tr>
<tr><td colspan="3">This is a very basic project plan for ensuring cyber-responsibility within an organization. Full project management tools and techniques should be followed to manage this project. Industry experts are predicting that attacks will increase and that adversaries will launch smaller, more targeted threats. The impact of cyberattacks is far reaching within an organization and will harm the organization’s reputation. Cyber-responsibility must be a priority within every organization.</td></tr>
<tr><th>Component</th><th>Definition</th><th>Example</th></tr>
<tr><td>Goal</td><td>• Long-term aim (may not be achievable during the life of the project)
• General statement of intent
• Purpose of the project; why we are doing it</td><td>• Define and implement a cyber-responsibility plan that spans all levels and staff by the end of the fourth quarter.</td></tr>
</table>

	• Link to organizational strategic goal	
Objectives	• Short-term aim (must be achieved during the project period) • Something toward which work is directed • Position to be attained • Purpose to be achieved • Result to be obtained • Product/service to be created	• Educate the board on the risks related to cyberthreats • Develop an education/awareness plan for the organization • Conduct a risk assessment of the current network • Evaluate the current attack surface and expansion • Analyze attacker behavior • Analyze defender behavior • Define/list attack vectors
Scope	• Major deliverables/categories of work • Describe as a noun (what) • Include brief description of each • Represents what is included in the project	• Awareness/marketing initiative • Cybersecurity staffing plan • Training plan • Cybersecurity risk assessment • Cybersecurity preparedness assessment • Best practices for cybersecurity • Policies and procedures
Boundaries	• Features that must be included in the product or service being created • Stipulations that must be followed in planning or executing the project • Outlines special needs • Provided by stakeholders • Must be comprehensive and specific for project success	• Must include all organization stakeholders • Must include a proactive approach not just a recovery approach
Risks	• Unplanned events that may occur • Impact can be positive or negative • Represent inherent uncertainty on all projects	• Contract security professionals may not be available
Assumptions	• Factors considered to be true, real, or certain (without proof or demonstration) for the project to be successful • Are documented to ensure understanding by major stakeholders	• The budget for the project will be approved • Contract resources will be necessary
Constraints	• Limiting factors could affect project execution • May limit available project management options • Some may pose risks to the project	• Contract security professionals may not be available

High-level Schedule	• Time estimates the sponsor used to justify the project's approval • Provide ballpark estimates of project length at this stage • Show major deliverables and estimated duration • Use ranges of time	• Project approval by end of first quarter • Project funded by end of first quarter • Security professionals engaged by first week of second quarter
High-level Budget	• Costs used to justify the project's approval • Ballpark estimates • Known costs or best guess • Use ranges • Avoid wild guesses	• Contract security professionals at $200,000

HIM Should Lead Cybersecurity Efforts

Chief information officers (CIOs) are competing for the top talent pool in order to strengthen their security teams with shrinking budgets. General counsel and chief legal officers should be ensuring their organizations are covered by having insurance policies that include cybersecurity insurance, while chief privacy officers (CPOs) are immersing themselves in everything they must do to respond to a breach caused by a cyberattack. There is not a one-size-fits-all approach to cyber-responsibility. There are many stakeholders, the most important of which is the consumer whose data may be compromised. Cyber-responsibility is an organization-wide responsibility; not just of the CIO and CPO. Just as transitioning to ICD-10-CM/PCS was not just an HIM project, cyber-responsibility is not just an IT problem.

Organizations need to go back to the common theme of attack that starts with people, process, and technology. According to Fortified Health Security's 2016 Horizon Report, "As healthcare leaders, we must balance fighting these adversaries through advanced technical solutions with educating our employee populations about cyber-responsibility—all while maintaining an already strapped IT budget."[2]

Health information management (HIM) professionals sit dead center on this issue and should do all they can to educate themselves on it. HIM should take the lead in consumer advocacy, serving as liaisons between operations and IT. Additionally, they are the experts when it comes to release of information and the legality of what can be released. HIM professionals should be pushing for organizations to address cyber-responsibility as an organizational strategy.

Cyber-responsibility is complicated. Organizations should approach cyber-responsibility as a project with executive sponsorship. Executive sponsorship needs to be assigned to the CEO or the CFO as part of a project that should include educating the entity's board of directors. With IT budgets focused on EHR implementation and optimization, the board will need to be educated in order to make an informed decision on budget approval for cyber-responsibility. A project manager should be assigned and he or she should complete a project management plan. Remember, this is not just an IT problem and the project will touch all employees, from the board to the front line staff. The project management plan on page 41 is an example of how to begin a cyber-responsibility project.

Notes

[1] Sheridan, Kelly. "Major Cyberattacks on Healthcare Grew 63% in 2016." *Dark Reading*. December 22, 2016.

[2] Fortified Health Security. "Horizon Report: The State of Cybersecurity in Healthcare." 2016.

Susan Carey (susan.carey@nortonhealthcare.org) is the system director of HIM for Norton Healthcare.

Article citation:
Carey, Susan. "Quest for Managing Cyberthreats in Healthcare" *Journal of AHIMA* 88, no.5 (May 2017): 40-41,43.