BECKER'S
Hospital Review
BUSINESS & LEGAL ISSUES FOR HEALTH SYSTEM LEADERSHIP

6 Takeaways on Healthcare Cybersecurity from the 2017 HIMSS Forum

Written by Martin Luethi, PhD, Strata Decision Technology | February 20, 2017

Cybersecurity has quickly jumped to the top of everyone's list relative to risk for every organization, and healthcare providers are scrambling to get really smart really fast.

That's why on a Sunday in Orlando, Florida, a few hundred healthcare professionals from provider, vendor and government organizations jammed into a room for the first HIMSS Cybersecurity Forum, one day ahead of the HIMSS 2017 conference.

The session provided an excellent snapshot of the current state of cybersecurity in healthcare with a well-rounded picture of the efforts, challenges, threats and risks. Presenters and panelists included CISOs and CIOs from Intermountain, Boston Children's Hospital, Texas Health Resources, UPMC, Sutter Health, UVHN, Indiana University Health, and NIST.

The fact that cybersecurity has now a separate day-long forum certainly shows that it has become, or still is, a major concern for many healthcare organizations. It is even more surprising that this forum was not created years ago.

Here are few key takeaways and trends discussed during the sessions:

1. **Attacks are on the rise.** Like in other industries, the number of attacks has risen dramatically over the past few years. Although many events are rather broad and unsophisticated malware, phishing and ransomware attacks, targeted social engineering has been increasing. Emails mimicking people and companies known to a recipient have become very common, among them also a tactic called whaling,' which targets C-level executives specifically. While the presented case study of a denial of service and hacking attempt against Boston Children's Hospital by Anonymous in 2014 is an exception, it showed in an astounding manner that healthcare organizations are not immune to very targeted attacks by hackers.

2. **Healthcare lags other industries.** Although most healthcare organizations have improved and evolved their security posture over the last few years, institutions are still far behind other industries, most notably compared to finance or defense organizations. The loose protection of endpoints, the lack of funds, mergers and acquisitions and an industry that is not aligned were cited as some of the reasons. In healthcare, threat information sharing attempts are still in their infancy. Some speakers also criticized the focus on assets and infrastructure versus the actual data. The perimeter in today's IT environment can't be as clearly defined any longer. Cloud services, remote and mobile access have blurred this line considerably.

3. **Security is a business problem.** In many organizations, security is still considered to be an IT problem that requires a technical solution. However, most security issues have their root in non-IT causes, namely in people and process issues. It was emphasized that it is key to build a solid culture of security with strong executive support. IT and organizational strategy need to go hand in hand with security planning. If security is detached from other efforts it will not be effective or successful.

4. **Cloud can be more secure.** Most speakers agreed that a well-managed and planned out cloud infrastructure can be more secure than a more traditional on-premise data center approach, especially for smaller organizations. The reasons are simple: Cloud providers have generally more sophisticated physical, technical and administrative controls in place and access to more skilled resources. It was cautioned that such an approach should be well-thought-out and standards need to be in place.

5. **Know your risks and prioritize your spending.** Healthcare organizations should invest more in information security — so-called 'check-box compliance' alone will not improve their security posture. Reoccurring third party risk assessments are key to understanding where risks truly are, and alternating with internal assessments can keep costs reasonable. The effectiveness of controls needs to be tested but cannot encompass the entire catalog of controls. Data-driven continuous learning will provide

Continued on page 2

the best results.

6. Good hygiene and standards. Good principles and controls can reduce a large share of an organization's risk. Having strong processes around these principles and engraining them in an organization will be most effective. NIST's Cybersecurity Framework is a popular example and is, compared to other NIST standards, relatively simple. It provides a framework for organizations to assess and improve their ability to prevent, detect and respond to cyberattacks. Another popular framework is HITRUST, although a show of hands during the forum only showed a few organization use HITRUST.

There is a lot of work left to make healthcare organizations and their data more secure. Organizations need to work together to share and exchange knowledge on this topic. The good news is that HIMSS recently launched a Cybersecurity Community, which provides a monthly forum for participants to share best practices and advance the state of cybersecurity in healthcare. The number of members increased from 200 last September to over 1,000 in February. This shows that there is clearly a need for more coordination and willingness to learn from other organizations. And this is clearly a case where all of us are smarter than any of us — collaboration is needed.