COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 20, Number 1. January 09, 2020 Security Threat Checklist for 2020

By Jane Anderson

Experts interviewed by *RPP* recommended a variety of strategies to stay ahead of evolving security threats in 2020:

- **Perform a risk assessment at least annually**. "Create, then execute, a plan to mitigate the identified risks, in a prioritized order," says Rebecca Herold, president of SIMBUS360 and CEO of The Privacy Professor. "Then, don't wait another two, five or 10 years to do another. Include all types of endpoints within the scope," including medical devices and employee-owned devices that are connected within the business ecosystem. Risk assessments should take place every year, and any time there has been a major change in operations.

- **Determine where your protected health information (PHI) is located**. Raj Mehta, life sciences and health care sector leader for Deloitte Cyber and partner in Deloitte & Touche LLP, says most organizations do not have a complete inventory of PHI data, since it doesn't all reside within central electronic health record systems. "What we have seen work is organizations at least conduct a risk analysis at the 'asset category' level where PHI may reside, and assess applicable risk scenarios—for example, PHI may reside in email systems, shared drives, medical devices and PHI applications." Herold adds that "health care organizations need to establish a PHI inventory, starting from their internal servers and data repositories, all the way out to their employee-owned endpoints, online servers and websites, and BA systems and devices. If organizations do not know where their data is located, they cannot control or protect it."

- **As part of their overall assessment of operations, health care entities should make certain that all their software is updated and current**, says attorney Patricia Shea, partner at K&L Gates LLP in Harrisburg, Pennsylvania. She notes, "I still find entities using software that is no longer supported. This is low-hanging fruit for bad actors. If a covered entity or business associate does not ensure that it has the fixes that have been established to protect data, it is asking for trouble. So if these entities are using equipment or software that is no longer supported and which likely has well-known weaknesses, it should not be surprising if the bad actors show up."

- **Oversee your business associates more closely**. Herold sees BAs and their subcontractors as one of the top HIPAA security issues for 2020, saying it's "still a huge vulnerability within health care organizations." She urges health care entities to take more time and effort to proactively ensure business associates and their subcontractors have sufficient security and privacy practices in place. "Start with requiring a recent (within six months, or since a major update in their organization was done—whichever has been most recent) risk assessment. Require them to sign monthly or bi-monthly security and privacy attestations. Ask for recent third-party audit results," she says.

- **Provide more frequent and varied information security and privacy training**. This should occur at least once per quarter, and possibly once per month, Herold says. "Make each training session comparatively short (e.g., 10 to 15 minutes per training), and send frequent reminders to keep awareness high—once every week or two. The message doesn't need to be long. It needs to be succinct, and related to the

recipients' daily work activities and own personal experiences." Harlow also backs what he calls "regular brief doses of 'micro-learning content,' with testing tied to training to confirm understanding and integration of the materials presented." This could include conducting tests with fake phishing emails and including training materials for those who open the emails or click on the links, Harlow adds.

- **Reemphasize the risks of not following procedure**, Shea says. "I see good people make mistakes because they think what they are doing is in the best interests of the entity or a project. They do not understand the risks they are accepting on behalf of the entity. Training and top-of-mind communications are essential. And remember, failure to follow procedures should not be tolerated. Entities spend a lot of time and money developing what they believe is best practice for them. Employees and workforce members who ignore that should understand that their actions may affect their future relationship with an entity."

- **Upgrade your security monitoring capabilities**, says Todd Thiemann, director of product marketing at Arctic Wolf Networks. "Security monitoring is essential because the bad guys will eventually slip through protective technology layers," he says. "Quickly locating and isolating a compromise can make the difference between a minor security event and a catastrophic breach."

- **Don't neglect the risks that are right in front of you**, says Richard Henderson, head of global threat intelligence for security firm Lastline Inc. "I think we spend a lot of time thinking about evil attackers from faraway lands trying to steal reams of sensitive information and nowhere near enough time thinking about what we're more likely to see," Henderson says. "Occam's razor applies just as much in health care as it does anywhere else: Is it more likely that a nation-state attack group is going to come after your organization, or is it more likely a device chock-full of unencrypted sensitive patient data gets lost or stolen? How likely would it be that you have staff that cut corners and don't properly destroy paper records or snoop on the records of friends, family, or a famous person who is seeking treatment?"

- **View security through a wide lens**. "One of the key impediments to managing HIPAA and other cybersecurity issues effectively is viewing them exclusively through a technology lens," says David Harlow, healthcare compliance counsel at Insulet Corporation. "For a health care entity this is an existential business issue, not merely an IT issue. Leadership and staffing, and budget support, need to be provided at a level, and in a manner, that can effectively mitigate data security threats."

- **Prepare for a ransomware attack**, Henderson says. "Start by asking yourself if you really believe you're ready to respond to that type of outage, and if you're not, start doing tabletop exercises with all your teams, not just security, and figure out exactly what your disaster recovery plans should be. If you feel like you're ready, then practice and prepare for it. Do mock scenarios and tests of outages. Practice restoring key systems. Check your backups. Make sure you have critical assets backed up in cold storage. And finally, make sure you have security technologies in place to not just stop the initial infection on that first computer, but tools that are able to detect and stop attacks from moving laterally across your environment and locking down other systems as they go."

- **Review all medical devices for appropriate protections** , says Roger Shindell, president and CEO of Carosh Compliance Solutions. Many Internet-of-Things devices in use have not had their factory security default settings changed, which makes them vulnerable to malware attacks, and hard-coded backdoors to devices provide uncontrolled access, he says.

- **Work with your organization's leadership to provide more resources for cybersecurity, particularly for training** , Shindell says.