Trustee Insights

CYBERSECURITY

Cybersecurity Awareness is a Board Responsibility

AHA Cybersecurity expert John Riggi discusses what trustees should know about their organization's cyberthreat plan

BY NIKHIL BAVISKAR

The frequency and severity of cyber-attacks on hospitals continues to mount as hackers become more sophisticated. Since hospitals and health systems are prime targets, trustees should familiarize themselves with their organization's plan to manage possible cyber intrusions. In recognition of October being Cybersecurity Awareness Month, John Riggi, national advisor for cybersecurity and risk for the American Hospital Association, spoke to Trustee Insights about this increasingly important topic. What Boards Should Know about Cybersecurity.

Nikhil Baviskar: *Board members must be attuned to a myriad of issues. What should they know about cybersecurity as it affects hospitals in 2023 and beyond?*

John Riggi: Boards should understand that cyber risk represents an enterprise risk to the organization and is primarily a risk to patient safety. For example, ransomware attacks which shut down computer networks and the internet connection with the outside world will result in physical impact to every function in the organization. We have seen repeatedly, unfortunately, hundreds of ransomware attacks on hospitals and health systems during the last several years, a significant disruption and delay to health care delivery.

Some of the initial effects of ransomware attacks include the loss of all network and Internet connected medical technology, which is used to deliver urgent health care such as diagnostic technology, imaging, radiology, lab, pharmacy, radiation oncology and chemotherapy. Unfortunately, in 2023 we are on pace to smash all previous records regarding data theft attacks and ransomware attacks against hospitals and health systems. The latest data from the HHS Office of Civil Rights (OCR), which tracks all required reporting of health care breaches, indicates there have been approximately 400 hacks resulting in the theft of the protected health information of 74 million individuals in the United States since the start of the year. "Hacks" mean external computer intrusions committed by foreign based bad actors, primarily criminal organizations, but also criminal organizations working in collusion with nation state intelligence services. These would include hostile nation states such as Russia, China, Iran and North Korea. For context, in 2022 we had hacks impacting 44 million individuals, and thus we have already surpassed last year's near record. We estimate that 25 % of the reported OCR breaches relate to ransomware attacks which were accompanied by data theft and extortion as part of the overall attack.

A ransomware attack delivers a bad guy's malware into an organization which results in the encryption of data and networks and causes those systems to shut down. It is very common that these ransomware gangs also simultaneously exfiltrate protected health information and hold the data for ransom, threatening to publish the stolen data on the internet and dark web if the ransom is not paid. This is known as the double layered extortion method. The hackers demand that the victim hospital or health system pay a ransom, generally in the millions of dollars, for the decryption key to unlock encrypted systems and in exchange for a "promise" not to publish the stolen patient data. Some organizations have improved their cybersecurity posture by installing "immutable" backups, which we strongly recommend. Immutable or unchangeable backups cannot be altered, deleted or encrypted by hackers and serve as a last line of defense to independently restore encrypted computer systems and data without having to pay a ransom for the decryption key. However, this would not necessarily solve the issue of the bad guys threatening to publicize or sell stolen patient information.

Some strategic cyber considerations trustees should know: Has the organization mapped its entire computer network, including connections with third-parties? Do they understand how expansive their network is? What are the internal and external clinical and operational dependencies on the availability of their computer networks? If they are hit with a ransomware attack, and are forced to shut down their networks, what would be the disruption to those internal and external functions that rely on the availability of network and internet connected technology?

For example, large health systems operate multiple hospitals, ambulatory clinics or other types of care centers, all of which may be connected to one overarching, system level computer network. When a large health system is targeted, the dependency and loss of the central corporate network "backbone" may result in a regional or multistate disruption to health care delivery health care— including the diversion of ambulances, patients and delayed surgeries. The diversion of ambulances and patients to surrounding hospitals will also create a regional strain to health care delivery services, which may create a regional risk to patient safety. Understanding what the direct and regional clinical impact would be if your organization is hit with a ransomware attack is key for effective cyber incident response planning. This planning should incorporate what I call "The 5 Rs" — Regional, Readiness, Response, Resiliency and Recovery capabilities.

There are three simple questions leaders should ask if the organization must shut down their network and internet connections:

1. What will work?
2. What won't work?
3. What's the plan?

These questions often are framed in the sense of the business continuity plan. Many think in terms of IT restoring lost technology and the network. But the IT department may not have control over the incident if the disruption is due to a ransomware attack or an attack on a mission-critical third party. We should also think in terms of not just business continuity, but what I call "clinical continuity." How do we continue to deliver care in the absence of technology - what is the plan? Do clinical downtime procedures extend far beyond manual charting for the electronic medical record? Downtime procedures are necessary for every piece of medical technology we rely on to deliver care.

The bottom-line question is: How do we continue to provide safe and quality care for patients in the absence of all technology?

What is the plan? Is the "plan" to simply divert patients or cancel surgeries? If you are the only hospital in a region or the only Level One trauma center in the state, there may be no practical, immediate diversion points. There are other factors, such as poor weather and distance, which will negatively impact the effective diversion of patients. A victim hospital may simply not have an alternative to divert ambulances or patients. Even for those organizations with the ability to divert, doing so may create delay and increase stress to the surrounding health care organizations.

So, a ransomware attack on one organization can actually be equivalent to a regional disaster. It may create in effect, what I call the ransomware blast radius. One organization is hit and there are disruptive health care delivery shock waves felt throughout the entire region.

Baviskar: *When I worked in the field, I saw first-hand how a third-party attack can affect the hospital's day to day processes.*

Riggi: Right, from a board's perspective, it's important to know: Who are our mission critical third-party providers? If the hackers hit that central node health care— What will be the impact to our organization?

Baviskar: *Aside from the resources your team puts out, what is another good way that board members can stay up to date with what is coming next?*

Riggi: On our website, we aggregate the threat data from multiple federal agencies and other sources. Our AHA cyber website is one of the only sites that displays data from all the government agencies in one location. We also provide unique resources and perspective on cyber threats, policy and advocacy matters and have a multitude of podcasts I have recorded with senior government officials and health care leaders. Another resource is www.stopransomware.gov. The HSCC, Health Sector Coordinating Council, www.healthsectorcouncil.org. Whenever there's significant threat intelligence, that information will be published in AHA Today and when particularly serious, will be disseminated to all members via a special cyber alert.

In order to stay abreast of new developments, an effective cyber governance structure is essential. One way to stay up on cybersecurity is to ensure it is treated as an enterprise risk issue and ranked in the risk register. Many organizations rank cyber as their number one risk issue or at least within the top three. I also recommend the full board receive a cyber threat briefing at least once a year. It is also helpful to bring in outside experts to brief the board on the latest national threat picture. Creating a governance subcommittee on cyber is important. This can help in developing key cyber metrics for the organization. This committee should meet at least quarterly with the CIO and CISO and get the latest threat updates, discuss strategy, review the latest risk assessments, phishing tests and vulnerability management statistics. I think the board should also understand that cyber risk will affect the organization when it comes to mergers and acquisitions and overall business strategy.

Baviskar: *That is a helpful concern to bring up. It is something that may not be top of mind during the acquisition process.*

Riggi: Cyber should be included as a risk issue as part of every merger and acquisition. Cyber due diligence is as an important component of overall due diligence health care — I would say just as important as financial due diligence. For example, organizations should ask health care — "What is the cyber risk if we acquire this entity and how well-postured are they to prevent and recover from a cyber-attack? If they have a poor cybersecurity posture, the responsibility for that risk transfers to the acquiring entity, which then creates a huge financial, legal, regulatory, reputational and patient safety risk for the acquiring entity. Bringing the new organization to an acceptable level of cyber risk exposure may require a significant investment of millions of dollars, which could outweigh or eliminate the financial benefit of the transaction.

Baviskar: *Would there be any legal risk to a board of directors for some type of a cyber-attack?*

Riggi: For the financial services sector in New York, state law requires every financial entity operating in the state of New York, including insurance companies and banks, to have a board member that is knowledgeable about cybersecurity. We have yet to see the same responsibility placed on health care boards, but the organization may face legal and regulatory risk exposure if cyber is not a priority. Ultimately, my personal opinion is that boards will serve themselves and the organization well by receiving regular cybersecurity briefings and providing guidance in return. Having a robust and interdisciplinary engagement on the issue of cybersecurity is important for the board and all functions and the organization health care — so collectively they may understand the nature of cyber risk, the risk exposure and the impact the organization and each function faces. This will assist organizations defend against and prepare for cyber-attacks, bearing in mind that no organization, including the federal government, can completely eliminate all cyber-attacks.

Baviskar: *What are your overall takeaways for trustees reading this interview?*

Riggi: First, I would approach cyber risk in a very strategic manner. It is important to rank cybersecurity as an enterprise risk issue and understand what the organizational exposure to cyber risk is. What would be the impact of a cyber-attack to the functions of the organization, especially patient care? Board members should ask broad questions and set the requirement that the technical leaders responsible for cybersecurity translate how technical cyber risk transforms to strategic business risk along with financial, legal, regulatory and again, most importantly, patient safety risk.

Also, make sure to ask the big questions. Who has access to our data? Who has access to our networks? Who are the mission critical third parties we depend upon? Are we receiving frequent cyber updates? Do we understand what is being presented to us? What is the action plan to help mitigate the risk to prevent an attack? I hate to use this cliché, but it's not a matter of if, but when.

One of my other recommendations relates to emergency management planning. I often see a tremendous gap between emergency management planning and cyber incident response planning. Emergency management teams are highly effective in preparing for fires, floods, mass casualty attacks and other hazards. Ultimately, I recommend that we integrate the cyber-incident response plan with emergency management plans and treat a cyber-attack as another hazard which emergency management teams plan for on an internal and on a regional basis.

We all must understand that there is no competitive advantage when it comes to cyber risk. To defend one is to defend all. Sharing intelligence amongst health care colleagues is vitally important for the common defense. If you prevent a high impact ransomware attack, you're preventing an act of cyber terrorism. During a hospital ransomware attack, there is a broad threat to the entire community as a result of the victim hospital not being available to handle medical emergencies, resulting in the diversion of ambulances and patients. The cyber terrorist's intent is to cause disruption to health care delivery, which represents a direct risk to patient and community safety. In large part due to our advocacy, the federal government now officially classifies ransomware attacks on hospitals as threat to life crimes. For example, if, as the result of ransomware attack, a hospital is forced to divert ambulances carrying heart attack or stroke patients to another facility an hour away, it increases the risk of a negative outcome or death.

But by working together and with the federal government we can help defend against and minimize the impact of these cyber-attacks health care — to help protect patients and the nation. *One team, one fight.*

Nikhil Baviskar *(nbaviskar@aha.org) is program manager, trustee services, at the American Hospital Association.*

Please note that the views of interviewees do not always reflect the views of the AHA.