Trustee Insights

CYBERSECURITY

The Board's Role in Cybersecurity (Part Two)

Enhance your knowledge of cyber issues and risks

To read part one, The Board's Role in Cybersecurity

BY REBECCA VESELY

When speaking to hospital executives at a cybersecurity forum, longtime law enforcement official M. K. Palmore had a straightforward message: Please engage law enforcement before disaster strikes.

Palmore was the head of the Federal Bureau of Investigation's (FBI) San Francisco cybersecurity branch and is well known in the cybersecurity field. He led a team of more than 60 personnel who conduct investigations into computer network intrusions and other cyber crimes.

Palmore stressed that cyber criminals are smart, difficult to catch and tend to go for easy targets. "The path of least resistance is always the route they will go," Palmore told the hospital executives.

The governing boards of hospitals and health systems can take proactive steps to ensure that their facilities are not the easy target, Palmore and others said at the forum.

TRUSTEE TALKING POINTS

- Board members don't need to be computer security experts to fulfill their role — but they should listen to them.
- A proactive board takes steps to make sure the hospital or health system is not an easy target for cyber criminals.
- Establishing a relationship with local law enforcement reduces the threat of an attack and speeds response time.
- Law enforcement cyber experts can offer the board an impartial assessment on the organization's vulnerabilities and risks.

The first step is getting up to speed on the risks and vulnerabilities to the organization. Inviting FBI agents to assess vulnerabilities is one way to do this. Board members do not have to be computer security experts themselves — but they should listen closely to those who are.

John Riggi, a 28-year veteran of the FBI and former colleague of Palmore's, joined the American Hospital Association in February 2018 to help hospitals and health systems reduce their cyber risks and vulnerabilities. He is also a bridge between hospitals and law enforcement for better coordination in advance, during and after cyber attacks.

Riggi agreed that hospitals and health systems should establish

pre-existing, trusted relationships with their local offices of the FBI and U.S. Secret Service regarding cybersecurity issues before a cyber attack strikes. A governing board should direct leadership to formalize an incident response plan with local and regional law enforcement, similar to natural disaster scenarios. There are 56 FBI field offices across the United States; each one has a cyber task force, which includes other federal and state law enforcement agencies working closely with the private sector to reduce cyber threats and speed response time to any attacks.

"Hospitals should have a specific point of contact at the FBI identified in the incident response plan," Riggi explained. "In some instances, the FBI will participate in a tabletop incident response exercise with the hospital to evaluate risks."

Build Relationships Up Front

Generally, the FBI's main contact would be the chief information officer (CIO) of a health care organization. However, CIOs typically need a green light from legal and leadership to first reach out to an FBI field office, Riggi said. Boards can decide to make establishing a relationship with the FBI and other law enforcement agencies a priority, setting things in motion.

The advantage of having a pre-established relationship with the FBI is that, when a cyber breach happens, there is already a plan in place, and a certain level of trust has been established. Additionally, law enforcement agents would be familiar with the organization's data systems and protocols; and the hospital will understand the nature of the FBI's response and the agency's capabilities.

"I have been involved in many crisis situations where time was lost because FBI assistance was delayed while the authorization to engage with the FBI was going through the organization's legal department," Riggi said.

He likened this unfortunate scenario to a homeowner whose house is on fire calling his lawyer while the firefighters wait outside for legal approval to turn on the hoses.

The questions that a hospital's governing board, leadership and legal team can answer before any incident include: whether patient information will be accessible to law enforcement; which databases will be available for review; and whether the hospital will or should require a legal process from the FBI to conduct computer forensic reviews.

While establishing relationships with law enforcement ahead of cyber incidents is becoming routine, many hospitals and health systems do not have these in place yet, Riggi said.

"These relationships are becoming more common, but we still have a long way to go," Riggi said.

Law enforcement cyber experts can offer boards an impartial assessment on vulnerabilities and risks unique to the organization. Understanding these risks is an important aspect to the board's oversight role in information security, Riggi said.

"The board should view cyber risk as an enterprise risk issue and understand the nature, capability and intent of their cyber adversaries based upon a current strategic cyber risk profile," he said. "Next, boards should assess their internal security capabilities to defend against the identified cyber adversaries and risk they present."

Understanding these capabilities can lead to discussions about how much risk to hand off to outside vendors.

"The board can then consider outsourcing risk to a reputable service provider, understanding the human talent and capabilities of that vendor, which may be better postured to mitigate the identified cyber risk," he said.

Understand Vendor Security

More hospitals and health systems are choosing to move electronic health records (EHRs), billing functions, human resources services and other activities to cloud-based services rather than hosting them on site. Vendors are responding to this trend by offering more cloud-based services.

Jim Hewitt, executive vice president of solutions at AllScripts, said at the Health 2.0 conference in October 2018 that the company's recent announcement that it will offer a pure cloud EHR was in response to demand from the field.

"A good chunk of our customers are converting to the hosting cloud," Hewitt said. "Fewer and fewer are taking on on-premises solutions. It's dwindling quickly."

Governing boards may play a role in not only approving vendor agreements for cloud-based hosting services but also understanding the shared risks and rewards to cloud solutions, said Riggi.

"It's not a panacea to cyber risk," Riggi said of the cloud. "When you put data in the cloud, the hospital is still responsible for configuring the security around that data." Amazon (or another cloud services provider) might be secure in their infrastructure, but the hospital may have to select and implement the desired level of security controls.

Questions boards should ask about a cloud strategy should include: "What is the cyber risk of this solution, and how is that risk being mitigated?" Riggi said.

He and other experts remind organizations that cloud-based services are not immune to cyber attacks. For instance, in 2017, Nuance Communications, a voice vendor that integrates its medical dictation application with EHRs, was one of 2,000 victims of the NotPetya ransomware attack. Also in 2017, the malware attack known as Operation Cloud Hopper targeted cloud-based providers rather than company servers.

In certain cases, a bad actor gains illegal access to the software company's distribution system and replaces a legitimate software update with malware. When a customer — such as a hospital — downloads the update, the malware could infect its system.

Ways to minimize the risk to this type of attack include rolling out updates in small batches so an attack can be contained. Additionally, software updates can be first sent to so-called "safe sandboxes" — where they are verified before being released to the whole system, according to Symantec, a global cybersecurity company.

Keep Up with Developments

To be sure, governing board members don't need to be cybersecurity experts to fulfill their important role in reducing risk of cyber attacks, Riggi said.

"You don't have to be a tech expert to understand cyber risk," he said. "Boards should not be intimidated by the technology. It is incumbent upon the technical leaders to understand the risk and be able to explain it to the board in a nontechnical manner through the lens of strategic and enterprise risk."

Overall, Riggi said he is "tremendously encouraged" by the active engagement of boards of both large and small hospitals across the nation on cybersecurity issues.

"Hospital boards are really beginning to view cyber risk as an enterprise risk issue," he said. "They are devoting more resources to the issue, and there are many doing really great work mitigating the risk — protecting data and, most importantly, ensuring safe and uninterrupted delivery of care. Bottom line: doing great work protecting patients."

TRUSTEE TAKEAWAYS

To fulfill its duty to protect the organization's data systems and its patients, a governing board should:

- Ask leadership to explain cyber risk and internal security capabilities in a nontechnical and strategic manner.
- Direct leadership to formalize an incident response plan with local and regional law enforcement, including an FBI field office.
- Seek guidance from cybersecurity experts to understand the organization's strategic cyber risk profile — and how much risk should be outsourced to a reputable service provider.
- Take appropriate precautions when weighing the move to a cloud-based provider and understand new responsibilities in terms of safeguarding data in the cloud.

Rebecca Vesely *is a contributing writer to* Trustee Insights.