Trustee Insights

CYBERSECURITY

The Board's Role in Cybersecurity (Part One)

Help protect your organization from the expanding risks and vulnerabilities of cyberattacks

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

BY REBECCA VESELY

In May 2017, more than 200,000 vulnerable computer systems in 150 countries, including those of Britain's National Health Service, were hit with a crippling cyberattack that ultimately cost $8 billion. Ambulances carrying trauma patients were diverted, and surgeries were canceled.

Known as WannaCry, the attack fell under the category of ransomware. A computer virus found its way into protected systems by exploiting an old, unpatched vulnerability in Microsoft Windows. WannaCry then encrypted the PC's files, locking out users until they made a ransom payment.

The WannaCry virus was later traced to North Korean hackers working on behalf of the North Korean government, whose crimes the U.S. Justice Department recently described as "staggering and offensive."

WannaCry is just one high-profile example of the many cyberattacks on hospitals and health systems today. It is illustrative in that it shows how bad actors, including hostile nation states, can exploit vulnerabilities to wreak havoc on organizations and potentially jeopardize patient safety and care delivery.

But WannaCry also shows that, with proper planning and investment, risk can be mitigated, said John Riggi, senior advisor for cyber-

TRUSTEE TALKING POINTS

- Hospitals and health systems are prime targets for cyber adversaries because of the broad and highly valuable information data sets they possess.
- The main cyber threats faced by health care organizations are constantly evolving and gaining in sophistication. Complacency is not an option.
- Computer intrusions, email compromise, ransomware attacks, data extortion and crypto hijacking are among the most common cyber threats.
- Elevating information security staff to positions of sufficient authority, status and independence can help mitigate the threats.

security at the American Hospital Association (AHA).

"The impact on American hospitals and health systems was far less serious, which speaks to the tremendous efforts the field has made to improve cybersecurity and build incidence response capabilities," Riggi told members of Congress in July.

Riggi is a 28-year veteran of the Federal Bureau of Investigation (FBI), and joined the AHA in February 2018 to help hospitals and health systems reduce their cyber risks and vulnerabilities. He is also a bridge to law enforcement for better coordination in advance, during and after cyberattacks.

"The threats are constantly evolving and dynamic in nature," Riggi said in an interview. "And generally, cyber adversaries have the upper hand. They are on offense, and we are constantly on defense."

Making Cybersecurity a Priority

Health care is unique among economic sectors in its breadth and depth of valuable information. These include personally identifiable information such as Social Security numbers; financial information (e.g., credit card numbers and bank accounts); protected health information of citizens, including high-profile targets; business intelligence; intellectual property (e.g., medical research); and national security information related to emergency preparedness.

"Each one of these data sets is heavily targeted by cyber adversaries," said Riggi. "Hospitals and health systems are the only organizations that may possess *all* these data sets in combination, making them exponentially valuable."

The average cost of a lost or stolen health record is $408 per record, compared to a stolen record that is not health care related, whose cost is $148 per record, according to the Ponemon Institute, an independent information security research firm.

Because the information held by hospitals and health systems is a lucrative target for cyber thieves, hospital executives and boards need to be paying even more attention to the threat than those in other sectors of the economy, Riggi said.

However, engagement on the

CYBERSECURITY CULTURE QUESTIONS

Five questions board members should ask to ensure cybersecurity is being addressed internally:

1. Do we have at least one person on staff dedicated full time to information security?
2. Is the reporting structure of information security officers sufficiently prominent within the organization to provide sufficient status, authority and independence for effective functioning?
3. Does the board have a risk committee, and is that committee briefed regularly on evolving cybersecurity risks?
4. Do we have an incident response plan that includes contingencies for various cyber scenarios, such as ransomware, and how secure are our backups?
5. Does the board receive regular briefings and updates on the strategic cyber risk profile, and on how risks are being mitigated?

issue can be a problem. In its 2018 study on global megatrends in cybersecurity, the Ponemon Institute found that only 36 percent of information technology (IT) security professionals say senior leadership is engaged on cybersecurity as a strategic priority (across all business sectors). And 68 percent of respondents said their board of directors is not being briefed on the risks and prevention tactics for cyberattacks.

Types of Threats to Hospitals

An important aspect of engagement is being aware and up to date on the latest threats. For hospitals and health systems, the most significant and common threats include external computer intrusions, said Riggi.

Among the most common attack vectors to penetrate a computer network is by means of phishing emails, where cyber adversaries tempt hospital personnel to click on links or attachments in emails that in turn release a malicious virus into the computer system. More recent attacks include so-called "spear phishing" schemes, where targeted personnel are identified by name (and even hobbies or interest gleaned from their social media accounts) to entice them to open email and click on links.

Many hospitals are educating their workforces on how to spot phishing and spear phishing emails. The Texas Hospital Association (THA) works with its 500 member hospitals on phishing awareness training for personnel. Hospitals participating in the program have averaged a 60 percent reduction in click rates after completing the training, according to the THA. The training can be useful especially to the 75 percent of Texas hospitals that are small in size and may not have a large information security team on staff, noted THA officials.

As in WannaCry, ransomware is a serious threat to hospitals. Unpatched medical devices were a main attack vector in the WannaCry incident, and they remain a prime cybersecurity threat to hospitals, said Riggi.

"One of the basic questions hospital board members should ask is, 'Do we have an accurate and current inventory of our medical devices, and what are the cyber vulnerabilities of those devices critical for life support?'" said Riggi. "Medical device security is an ongoing and tremendous challenge."

A large hospital system can map more than 100,000 medical devices within its network, he said. Some of these devices are connected or disconnected to networks without the knowledge of the IT department, thereby reducing the ability to patch cyber-threat risks to those devices.

"Once you understand the network of medical devices, the questions are how are the medical device networks structured or segmented," Riggi said. "This is important because medical devices generally carry many vulnerabilities, which could present risk to the entire network."

Interoperability — the sharing of data and patient records across trusted parties — creates challenges to cybersecurity as well, Riggi said. Points of vulnerability can occur in sharing of data with insurers and electronic health record (EHR) vendors. In January, about 1,500 medical practices were locked out of their cloud-based EHRs in the SamSam ransomware attack on Allscripts.

"Strategic level or embedded threats can often be overlooked," Riggi said. "An example is a value-based payment model, where a majority of the clinical operations depend on sharing information throughout the continuum of care. Hospital boards should be aware that there is potential cyber risk as EHRs and patient information are shared between the provider and others."

So-called "crypto hijacking" is a threat that has emerged in the

past year. It refers to cyber criminals who penetrate a computer network for the purpose of co-opting its computing resources to engage in lucrative cryptocurrency mining. This type of cyberattack can drain energy and potentially disrupt clinical and business operations. Mining costs can far exceed the worth of a single bitcoin, so getting someone else to pay for the electricity and computing power to make digital currency becomes attractive to bad actors.

Adversaries and Responsibilities

As in the case of WannaCry, many cyber adversaries are based overseas in hostile or rogue nation states. As stated previously, the high monetary value of information possessed by health care organizations makes them a target of organized crime groups and others who have financial motivation to steal these data.

Nation states themselves pose significant threats to health systems, Riggi said, including China, Russia, Iran and North Korea. Of potential intelligence value to these nations are the health records of high-level military or government personnel, along with innovative medical research, he said. The term *hacktivist* refers to people who conduct cyberattacks that are politically or ideologically motivated. But these threats are not as common as those motivated for financial gain.

The Security Rule under the Health Insurance Portability and Accountability Act (HIPAA) means that hospitals and health systems can face penalties for failing to keep patient records private. The Office for Civil Rights at the Department of Health and Human Services (HHS) enforces the Security Rule, tracks violations and can refer complaints to the Justice Department for investigation.

> "Boards should elevate the issue of cyber risk as an enterprise risk management issue. And they should ensure they receive regular briefings and updates on the cyber risk profile, and that adequate steps are being taken to mitigate the risk."
>
> **John Riggi,** senior advisor for cybersecurity at the American Hospital Association

However, Riggi said, a cyber breach doesn't necessarily mean a HIPAA compliance failure, and health organizations should receive support and resources from the government.

"In fact, an aggressive regulatory approach can be counterproductive and hinder valued cooperation by the victims of a cyberattack with other parts of the government," he told members of Congress in testimony in July. "Instead, successful attacks should be fully investigated, and the lessons learned should be widely disseminated to prevent similar attacks in the future."

Understanding the Board's Role

A hospital's governing board plays an important role in curbing cybersecurity risk. Addressing cybersecurity first means making it a priority.

"Boards should elevate the issue of cyber risk as an enterprise risk management issue," Riggi said, on par and in the context of patient safety and care delivery. "And they should ensure they receive regular briefings and updates on the cyber risk profile, and that adequate steps are being taken to mitigate the risk."

In terms of resource allocation, boards should ask leadership whether there is at least one person dedicated full time to information security, Riggi advised. "That is not feasible for all hospitals, as some are simply too small," he cautioned. "But they should look at the resources dedicated to information security in terms of the overall budget — and personnel. Sometimes outsourcing the security function to a trusted and competent third-party firm makes the most sense for hospitals."

The reporting structure of information security leaders is another area where boards can weigh in, he said. A chief information security officer (CISO) can sometimes be buried under layers of management, rendering that person ineffective. Some CISOs report to the chief information officer, others to the chief compliance officer, and others to the CEO. In any case, the CISO should

hold a position that provides sufficient authority, status and independence within the overall organization.

"The lower the organizational priority emphasis on cybersecurity, the lower the quality of information security professional you will attract. And if the organization which does not prioritize cybersecurity happens to have a high caliber information security person, that person will be difficult to retain. They are in high demand," Riggi said.

Additionally, the governing board should have a risk or audit committee that oversees information security and is part of the governing structure, he advised. The risk or audit committee holds regular meetings to review cyber risk assessments and prioritize the cyber threats and risk mitigation objectives and expenditures.

Finally, boards should know their facility's continuity of operations plan and ask plenty of questions about it, Riggi said. This includes the status of backup servers in case of a ransomware attack. Are the backups maintained offline? Are they segmented? Has the restoration time been tested? What is the security around the backup in terms of who has access to the servers, including vendors?

Although cyber risk can never be eliminated completely, the good news is that steps can be taken to reduce the risk substantially, Riggi said.

"Bad guys are thinking every day about how to compromise cybersecurity procedures and controls," Riggi said. "The best defense is understanding your strategic cyber risk profile, having a dynamic risk mitigation plan and, most importantly, instilling a 'patient safety' focused culture of cybersecurity."

In part 2: *getting your board up to speed on cybersecurity issues and risks*

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

TRUSTEE TAKEAWAYS

Governing boards have a critical role to play in terms of understanding and curtailing cybersecurity risks. Boards should:

- Understand that cyber risk is first and foremost a patient safety and care delivery risk issue.
- Know that health care is a prime target for cyber adversaries; the threat is ongoing and constantly changing.
- Keep cybersecurity front and center, receiving regular updates on risk and risk mitigation. Treat it as an enterprise risk issue.
- Understand that cyber risk can never be eliminated; it can only be mitigated. Proper planning can make cyberattacks less probable and less severe if they do occur.
- Uncover the vulnerabilities within the organization and take steps to mitigate that risk.