THE CYBERSECURITY WAR IN HEALTHCARE

KONICA MINOLTA

MedCity News

Since the HITECH Act passed in 2009, the push to digitize patient medical records has grown exponentially. Micky Tripathi, the head of the Office of the National Coordinator for Health IT, noted at the ViVE conference in March 2023 that 97% of hospitals have adopted certfied electronic health records (EHRs). Add to that medical devices connected to the Internet of Things, cloud-based software companies that have moved into healthcare, clinical and patient facing apps, and wearables. Health systems have made patient data more accessible than ever before, but one common thread is that security and equally important, training is often an afterthought – less than 11% of healthcare IT teams identified cybersecurity investment as a high priority. In the past few years, hospitals have suffered an onslaught of ransomware attacks. Why? Because they work. A 2022 report from Cynerio and the Ponemon Institute on Intent of Things (IoT) and Internet of Medical Things (IoMT) found that 47% of hospitals pay when their data is held for ransom by cybercriminals. The widespread attacks and implications for national security has led to a series of proposals to increase and add more consistency to patient data protection.

The 2022 Healthcare Data Breach Report published in the HIPAA Journal documented 707 data breaches of 51.9 million records. Despite a 113% decline from 2021, it was the second highest number of breaches to date. Hacking/IT incidents caused the majority of data breaches (84.6%). Business Associates accounted for the largest portion of data breaches, followed closely by hospitals. The U.S. Department of Health's Office of Civil Rights website also offers a window into the most recent breaches with a breakdown by size, scope, and organizations impacted.

OneTouchPoint, a marketing and software services company, suffered the worst healthcare data breach of 2022, affecting more than 4 million people across 37 organizations. An unauthorized party accessed several servers. The breach underscored the risk posed by healthcare business associates.

The cost of a data breach can hit hospitals hard, particularly as they struggle to recover from the height of the Covid-19 pandemic and replace staff who have resigned over burnout and other reasons. According to data from IBM, the average cost of a healthcare data breach is a whopping $10.1 million in 2022 – a 42% increase over 2020.

It used to be that one of the biggest security risks facing hospitals was physicians and other healthcare staff using their own devices for patient consults, or uploading patient data onto these devices and accidentally leaving them on a train or in a taxi. But in recent years, malware and ransomware attacks have become the dominant concern.

A recent Wall Street Journal article noted that the CIO mantra for 2023 is trust no one. That would be a good watchword for the unsuspecting hospital staff who open an email from someone who appears to be a colleague but which unleashes a Phishing attack putting hundreds of patients' data at risk. Training is critical to prevent or at least minimize the impact of these attacks. Among best practice guidelines advocated by CISA are:

- Avoid using weak passwords
- Use two factor authentication with remote access tools
- Don't run unsupported software
- Use continuous compliance and security monitoring tools, such as Security Information and Event Management (SIEM) to thwart attacks

IT roles

During the pandemic, CIOs had to oversee the adoption, implementation or expansion of telehealth tools and build partnerships with service providers. Navigating this gauntlet of responsibilities during a time of so much uncertainty has helped reaffirm the importance of their role.

The chief information security officer (CISO) started to become prominent in the past seven years at medium to large sized health systems. The HITECH Act requires institutions to designate a security representative or officer. That role could also be designated to a chief compliance officer, for example. But one trend has been the rise of more specific roles making individuals responsible for cloud architecture or digital infrastructure at the vice president level at the larger health systems.

At some of the small hospitals in critical access rural facilities, they may only have one person who is responsible for security and that's where the real challenge is. The majority of care delivered in this country are the small rural hospitals and they are the ones that are most exposed. A survey by CyberMDX and Philips revealed that 48% of respondents said their hospitals had to shut down due to a cyberattack. If a person with a health emergency has to be diverted to a provider 3- minutes away from their local hospital because it's incapacitated over a cyberattack, it could be a matter of life and death.

Health systems can prepare for a cybersecurity attack by putting in place a security incident response plan, according to a report by the U.S. Sen Mark Warner (D-VA). They need to determine the scope of the data breach to identify networks, systems, and applications affected by the attack. Then determine the origin and whether the attack has ended. They also need to ascertain how the attack occurred. They should also contact the FBI or U.S. Secret Service Field Office.

Risk factors

One reason healthcare organizations find it challenging to deal with ransomware attacks is that legacy systems are not designed to resist cyberattacks. Another factor is that patient safety risks are not fully understood. Complicating matters, there is a longstanding shortage in the cybersecurity workforce across not only healthcare but other sectors as well.

One concerning trend impacting hospitals over the past two years is Insurance companies are toughening their stance on the terms hospitals must meet to be insured. Carter Groome, First Health Advisory CEO, said they may require their hospital customers to implement certain tools or implement a system to avoid losing their coverage.

"Right now, 12% of hospitals are not insured," Groome said. "What happens if that number continues to rise? Will insurers move out of the sector as a whole? Where will that leave healthcare if there are no Federal protections?

With ransomware attacks a constant threat, cyber insurance costs are rising and applications can be increasingly burdensome to fill out. Another development that Groome and his colleagues are watching closely is insurance companies that may implement an "Act of war rule" as opposed to an Act of God rule. For ransomware attacks committed at the behest or support of a nation state, insurance companies may balk at making cyber payouts to those institutions, justifying their position by saying they do not cover acts of war.

Litigation over insurance companies that decline to cover these costs have produced at least one win. Merck successfully sued its cyber insurer Ace America in the wake of a 2017 NotPetya ransomware attack when the insurer balked at covering the cost of the attack. It's an issue that will continue to be a concern for healthcare in-house counsel.

Another risk is created by health systems' reliance on third parties to provide analytics data on patients who interact with their hospital websites. Third-party web analytic tools software installed on provider websites, including patient portals, may expose patient data. ECRI, a consultancy organization supporting the healthcare and medtech industry, issued an alert in Ocober 2022 on the risks of hospitals working with third parties or business associates to track patient data.

Among ECRI's recommendations:

- Develop policies governing the use of third-party web analytic tools
- Review usage agreements of web analytic tools to determine how any collected data may be used
- Do not install third-party web analytic tools on websites containing patient information, such as patient portals, without a BAA in place
- Consider indirect indications of a medical treatment or conditions that may be inferred from browsing websites, such as searching for a doctor or viewing an online medical library

Connected devices

During the pandemic, remote patient monitoring through connected devices attracted a great deal of interest because they could help clinicians keep an eye on high risk patients without requiring them to come into the hospital. Their use was also reimbursed by CMS as part of the public health emergency. In September 2021, the Federal Trade Commission reminded device makers that collect or use patient health information that they must comply with the Health Breach Notification Rule. The rule says device makers must notify patients when their health data is breached. The omnibus spending bill passed last year also included provisions adopted from the Patch Act proposal introduced into the House of Representatives but which never came up for a vote. They require manufacturers to regularly update the software of their connected devices to reduce the risk of data breaches.

Another interesting facet of cybersecurity and connected devices is how hospitals are dealing with the cybersecurity needs of these devices. The Insecurity of Connected Devices in Healthcare, based on data provided by 517 healthcare experts in leadership positions at hospitals and health systems such as CIOs, CISOs, CTOs and more. At least one Internet of Things (IoT)/IoMT was involved in 88% of ransomware attacks, according to the report. One of the most interesting findings from the Cynerio/Ponemon Institute is that there is no clear, consistent ownership or accountability for protecting connected devices in different hospitals and health systems. Although the CIO or CTO was most commonly named as responsible for cybersecurity of IoT and IoMT devices (18%), at other institutions it was the CISO (14%) or operational management (14%). The majority of respondents (21%) said they spend $1 million to $2.5 million in IoT/IoMT cybersecurity. Respondents said that one factor that would affect that investment spend is new regulations (41%) but the majority (45%) said a serious hack of their medical devices would spur more investment.

Next steps

To address the shortage of cybersecurity experts in healthcare, Warner has made a couple of proposals. He noted that Congress could establish a workforce development program that focuses on healthcare cybersecurity. This program could be tailored to prepare cybersecurity professionals to confront cyber threats that are specific to the healthcare environment and would leverage community colleges and professional certification programs to develop a skilled workforce.

Warner has also advocated for creating a set of minimum standards for cyber hygiene in healthcare. "Flexible and adaptable best practices are needed as the threats healthcare organizations face are often evolving," the report noted. He likened the development of cyber hygiene standards to other programs hospitals have enacted such as preventing the spread of hospital-acquired infections and the maintenance of emergency and standby power systems.

It's also imperative for providers to implement an active defense strategy to conduct vulnerability assessments, behavioral monitoring, threat detection and intelligent security.

Outlook

The pandemic has left hospitals and health systems in a vulnerable position. It's impractical for the smallest providers to shoulder the cost of cybersecurity expenses on their own. As the healthcare industry works to develop effective countermeasures to prevent these attacks or deflect them, it is critical for stakeholders across software, providers and government agencies to formulate a strategy that is practical and effective for providers, regardless of resources or size.

Despite a dip in ransomware attacks in 2022, the need to be vigilant and constantly assess and improve security measures will remain as cybercriminals will keep trying to succeed in penetrating hospitals' inner sanctums to obtain patient data.

Best practices

There are several things hospitals and health systems can do to protect themselves against ransomware attacks and data breaches. Although they are not a guarantee, they reflect industry best practices. One panel highlighted the need Lisa Pino, Director for Office for Civil Rights, a department within HHS, offered some guidance for how hospitals can improve their cybersecurity posture.

- Maintain offline, encrypted backups of data and regularly test their backups
- Conduct regular scans to identify and address vulnerabilities, especially those on connected devices, to limit the attack surface
- Regular patches and updates of software and operating systems
- Train employees regarding phishing and other common IT attacks

At the ViVE 2023 conference, panelists discussing cybersecurity at health systems and life science companies recommended providing this training in frequent but short, digestible segments of 4-5 minutes. That way, the subject matter doesn't become overwhelming, is better retained and easily fits into employee workflows.