Cybersecurity Awareness

Protect the privacy and security of your data

By Scott Wrobel and Debra Geroux, JD, CHC. CHPC

Celebrating the 20th year anniversary of October as National Cybersecurity Awareness Month, the Cybersecurity & Infrastructure Security Agency (CISA) announced a new enduring cybersecurity awareness program, Secure Our World. However, for the healthcare industry and its internal auditors, every day should focus on cybersecurity. Cybersecurity risks to your organization's operations and compliance and to your patients and their safety and privacy are real.

The federal government, through collaborative efforts of its various agencies, continues to follow threat actors and cybersecurity incidents. The agencies provide guidance to healthcare leaders and internal audit professionals on what they can do to avoid being the next big data breach.

Beginning October 28, 2020, a joint cybersecurity alert ("2020 Joint Alert") was issued by CISA, the Federal Bureau of Investigation (FBI) and the Department of Health and Human Services (HHS), and other federal agencies. Since then, they have provided additional joint alerts, public service announcements (PSAs), advisories and other guidance.

The communications warn of various cyberthreats and threat actors. This article provides further insight into who these threat actors are, how they are attacking the healthcare industry, and what you and your organization can do to mitigate the risks of a cyberattack.[1]

Privacy as an element of security

In addition to remaining vigilant for cybersecurity threats of all types, healthcare entities should also be familiar with their obligation to protect their patients' healthcare information, thanks in large part to the Health Insurance Portability Act of 1996 (HIPAA). Also, HIPAA was amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act and its related regulations that include the HIPAA Privacy, Security and Breach Notification Rules. The Act and its regulations are collectively referred to herein as *HIPAA*.[2]

Often overlooked are other laws and regulations that affect healthcare entities and the information that they maintain. For instance, every state in the U.S. has some level of data privacy legislation that is implicated when an individual's personal data is affected by a cyberattack.

In recent years, many states have strengthened the protections afforded personal information through comprehensive privacy laws, starting in 2018 with the California Consumer Privacy Act of 2018 (CCPA), as amended by the California Privacy Rights Act of 2020 (CPRA). To date, 11 additional states have enacted comprehensive privacy laws protecting personal information, including health information, with effective dates ranging from January 1, 2020 to July 1, 2026.[3]

Another state—Washington—has broadened the protection afforded consumer health data collected by entities that conduct business in the state that is not otherwise covered by HIPAA through the enactment of the My Health My Data Act. Adding to the burden are the various federal laws and regulations that have been enacted to address the growing cybersecurity attacks on critical industries and public entities.

[1] While the laws and regulations discussed in this article are focused on their application in the healthcare industry, many of the state and federal laws and regulations are applicable to a multitude of industries.

[2] 45 CFR Parts 160 and 164, Subparts A, C, D and E.

[3] In addition to California, the following states have enacted comprehensive privacy laws: Colorado, Connecticut, Delaware, Indiana, Iowa, Montana, Oregon, Tennessee, Texas, Utah and Virginia. See https://pro.bloomberglaw.com/brief/state-privacy-legislation-tracker/ for more detail.

Patients are increasingly suing healthcare organizations over data breaches.

Taking proactive measures to avoid a cyberattack will inevitably lessen a healthcare entity's anxiety over having to notify government regulators and avoid the costly expenses of mitigation, remediation and notification. Also, proactive measures can help avoid the costs associated with lawsuits that have been increasing in frequency over the years.

Cyberattacks by the numbers

This year was one of unprecedented cybersecurity incidents. Media accounts of significant cyberattacks have been on the rise, affecting a broad range of industries, including financial, legal, manufacturing, education, governmental and healthcare. These industries have been attacked because they have information that threat actors desire—such as patient data, financial information and proprietary information—that can be leveraged to carry out extortion campaigns.

The healthcare industry, which is largely based on digital platforms, unsurprisingly remains among the top industries that cybercriminals continue to target. According to the FBI's *2022 Internet Crime Report*, cybercrime losses were in excess of $10.2 billion for 2022, nearly doubling the total losses reported in 2021, which does not take into consideration the cybercrimes that are not reported to the FBI.

In its *Cost of a Breach Report 2023*, IBM shows that the average cost associated with a breach for healthcare entities is $10.93 million, an increase of 53.3 percent from 2020. However, other factors, such as the size of the breach (records affected), can drastically increase the costs of breach response. For example, IBM reports that the 2023 global average data breach cost across all industries is $4.35 million, although the costs associated with a "mega breach" (breaches involving 1 million to 60 million individuals) fell in all categories, ranging between a 3.8 percent decrease to a 26.5 percent decrease.

Why are cybersecurity incidents rising?

A number of reasons exist for the increase in cybersecurity incidents. Since the Covid-19 pandemic, remote work has increased, resulting in greater vulnerability to cyber incidents. According to a 2021 global industry study commissioned by Tenable, Inc., 74 percent of the organizations surveyed attributed at least one cyberattack to vulnerabilities in systems implemented during the Covid-19 pandemic, including:

- The lack of security visibility into remote workers' home networks
- Migration of business operations to the cloud

Similarly, the Ponemon Institute conducted an October 2020 study related to the risks of cybersecurity attacks due to increased remote work. The study revealed a significant reduction in the effectiveness of organizations' information technology (IT) security posture due to Covid-19, falling from 71 percent effectiveness pre-Covid to 44 percent due to Covid-related vulnerabilities.

In addition to the increased vulnerabilities—and increased accessibility for cybercriminals—the evolution of cybercriminals and the tactics they employ is also leading to the increase in cyberattacks. In the past, extortion was the primary tactic, and that is still the case.

The increased sophistication of cybercriminals means their effect is also elevated. In its 2020 Annual Report to Congress on Breaches of Unsecured Protected Health Information, the U.S. Department of Health and Human Services, Office of Civil Rights (HHS) reported a total of 656 large breach reports (those affecting 500 or more individuals) affecting over 37.6 million individuals.

As of July 31, 2023, HHS received 437 large breach reports, with the top three affecting nearly 26 million individuals. These three entities include a:

- Hospital system affecting over 11.2 million individuals
- Pharmacy services provider affecting over 5.8 million individuals
- Dental benefits administrator for state agencies and managed care organizations affecting more than 8.8 million individuals

Further review of the reported large breaches clearly indicates that hospitals and other healthcare providers are not the only ones vulnerable to an attack. Indeed, HIPAA breaches have been reported by state and federal agencies, including the Colorado Department of Health Care Policy & Financing (DHCPF) and the Centers for Medicare and Medicaid Services (CMS).

Many of these incidents, including the Colorado DHCPF and a breach reported by CMS, were the result of a global cybersecurity incident affecting Progress Software Corporation's MOVEIt file transfer program. The threat actor CL0P Ransomware Gang, a ransomware group known for using zero-day vulnerability campaigns, was able to exploit MOVEIt software vulnerabilities in May 2023.

According to KonBriefing Research, as of December 1, 2023, the MOVEit Transfer cyber incident has affected 2,591 organizations worldwide and between 77.7 - 82.5 million individuals. Given the widespread use of the MOVEit Transfer software, only time will tell the reach of the MOVEit cyber incident.

The reported incidents here are not isolated. As various government agencies warn, cyberthreats to the healthcare industry are a reality and will continue in the future.

The threat actors and how they gain access

Ransomware continues to be big business. Ransomware as a service (RaaS) has become a new business model for threat actors who create ransomware variants that increase the ease with which an individual can deploy an attack. The ransomware is packaged and ready for attack.

While the variations in ransomware are continuously changing, the underlying concepts remain constant, with BlackCat, Black Basta, Royal and Lockbit 3.0 topping the list of threat actors. As of the second quarter of 2023, these four accounted for nearly 50 percent of the market share. And, despite statements by certain ransomware operators that they would not be launching ransomware attacks on hospitals during the Covid pandemic, the threats continued and are still very much alive as evidenced by the incidents discussed above.

Measures to prevent an incident

With cyberattacks not diminishing, industries—and more notably, the healthcare industry—need to step up their efforts to be proactive. Knowing who the threat actors are and how they are attacking can greatly assist in avoiding these threats. Generally speaking, cyberattack deployment can be categorized into three specific vulnerabilities: human error, malicious attacks and system glitches, with malicious attacks leading the pack by more than 50 percent.

Knowing who the threat actors are and how they gain access is critical to reducing the vulnerabilities that can be leveraged to steal sensitive, protected and/or valuable information. Resources are available to keep abreast of these threats and how to avoid them.

CISA has developed various free resources and tools (see the sidebar on page 11) to assist in your cybersecurity efforts, including technical assistance, exercises, assessments and training resources. The topics include Indicators of Compromise, for example for LockBit 2.0 ransomware, that provide mitigations for specific threat actors that can be used to ensure the security of their IT environment. The predominant risk areas that must be addressed are device security, cloud security and human errors.

Device security

Healthcare providers need to be cognizant at all times of the data that may be available on or accessible from devices, including diagnostic and other medical devices, and secure them accordingly. Knowing what data you have and where it is maintained is the first step in the analysis.

You must ask yourself what a threat actor could glean if they gained access to or overtook proprietary diagnostic tools. For example, would threat actors be able to extract firmware and source code information, then sell it to competitors? Or more problematic, if threat actors could leverage control over devices, could they interfere with the proper functioning of the device?

The average cost associated with a breach for healthcare entities is $10.93 million.

Remote work has increased, resulting in greater vulnerability to cyber incidents.

Your inquiries about device insecurities are significant, as they can lead not only to financial damages, they also pose significant risks to patient health. All systems that can access devices containing information about patients and/or proprietary technology should be protected with multifactor authentication, and they should have both location tracking and remote wiping enabled. Your IT management team can be engaged to assist with these solutions.

Cloud security

Healthcare providers are increasingly using cloud storage for data, including for electronic medical records. While storing data in the cloud is convenient and cost effective, the data also needs to be secured. No sensitive information should be accessible without multifactor authentication.

Additionally, since these cloud vendors are business associates—an often-overlooked concept—you need to ensure that they are compliant with applicable privacy and security laws, including HIPAA and similar state laws, at all times.

Breaches of cloud and other electronic services providers, particularly Office 365 email accounts, are on the rise, as evidenced by the MOVEit global incident. Consequently, IT management teams must continually address security protocols used. Examples include:

- Multifactor authentication that requires users to have a second device to authenticate their identity
- Geoblocking enabled to stop any access from specific foreign countries
- Strong password policies to reduce the chances of compromise

The changes can be made at the organizational level to help mitigate the third and most dangerous vulnerability—human error.

Human error

With even the most effective security protocols in place, human error continues to negate an organization's best efforts. Phishing campaigns are still prevalent—where threat actors obtain information from a target that can be used to perpetrate some type of future scam. Phishing campaigns typically occur not only through email, but also through phone calls (vishing) or text messages (smishing).

Newer campaigns, such as malvertising—malware in online advertisements—are adding to the threat actors' capabilities of breaching an organization's security. The threat actors are using more sophisticated efforts that utilize targeted emails (spear phishing). The content of the emails is based upon data found on the dark web that they use to develop an attack plan and perform targeted and more effective attacks. Understanding how spear phishing and other campaigns work is key to learning how to avoid them.

More and more, employees are using their business email addresses in connection with their personal accounts on social media sites that have had data breaches (e.g., Evite, LinkedIn, Dropbox). Once compromised, that information goes up for sale on the dark web. Threat actors are utilizing the information they find on the dark web about these accounts to spear phish employees' corporate email accounts.

A spear phishing attack is launched when an employee clicks on a spear phishing email that appears to be from a known sender or organization. According to Symantec's 2019 Internet Security Threat Report, spear phishing attacks are the most prevalent infection vector, representing 65 percent of the known groups carrying out cyberattacks.

The heightened effectiveness of spear phishing is due in large part to the sophistication of the email, which often include personal details that the recipient would not expect a threat actor to know. The threat actor is able to obtain access to the recipient's account when he or she clicks on a link or opens an attachment in the email, thereby launching the attack.

Once in, the virus quickly downloads all of the recipient's email searching for other victims and sends out an email to the recipient's contacts purporting to be from the recipient and spreading the link to a malicious website. Often, the threat actor stays inside the recipient's account to catch responses to the sent emails. For example, the email string may read:

- Recipient: "Is this email really from you?"
- Hacker: "Yes, it is, you can click on the link."

Once the victim clicks the link, the whole process begins again in a new recipient's account.

Similar phishing campaigns have included emails containing invoices that appear to come from an executive within an organization asking for payment(s). Not knowing the invoice to be from a threat actor, the recipient pays the invoice directly to the threat actor's untraceable account. Still another popular phishing campaign involves stealing usernames and passwords, known as credential phishing. In these campaigns, the attacks can be from spear phishing or may be the result of a business email compromise.

The best way to combat any phishing attempt is to be vigilant against the known threats. Training is critical to avoiding a cyberattack. While knowing what the threats are is important, training on how to spot and avoid malicious emails should be done on a regular basis. Other proactive measures should include establishing strong policies about the use of corporate email addresses and accounts, informing users of the potential dangers of clicking on and engaging with content from unknown sources and known sources whose requests are inconsistent with standard procedure.

Likewise, employees should have a well-established protocol to follow regarding reporting potential threats to management and IT. Periodic training exercises are a simple way to ensure the workforce is aware of and can recognize threats. The use of table-top exercises and simulated phishing emails will enable management and IT to see how employees are reacting to potentially malicious/spoofed emails and alert them to any additional training employees may need.

Conclusion

Cybercriminals are not going away any time soon. Instead, they are only growing in their sophistication. Healthcare providers must remain vigilant in their efforts to avoid becoming the next victim.

Build a comprehensive cybersecurity program and appropriately train your workforce to have the essential preventive activities. Use the tools and resources that the federal government has developed to keep IT administrators up to date on the current threats and threat actors. Build relevant policies and review them regularly. Join lists from trusted sites, such as CISA and the FBI, to assist your organization in keeping abreast of the current landscape of cybersecurity.

While many attacks can be prevented with diligent IT management, such as patches in software and strong encryption practices, no patch exists for human error. You can only prevent human errors through regular training of your workforce. Maintain cybersecurity checklists and incident response plans to assist your organization in mitigating its risk and addressing an incident should it fall victim despite its best efforts. **NP**

Resources

- CISA
  - Official Alerts and Statements
  - Free Cybersecurity Resources and Tools
  - Resources against Ransomware
- FBI – Official Alerts and Statements

Scott Wrobel is a co-founder of N1 Discovery and has accumulated over 20 years of experience implementing technology solutions for clients facing a wide variety of situations. He specializes in complex technology investigations and data breaches, including high-profile digital forensic investigations involving theft of intellectual property, fraud, child exploitation and white-collar crimes. Scott can be reached at Scott.Wrobel@n1discovery.com.

Debra Geroux, JD, CHC. CHPC, is a Shareholder and a Co-Chair of Butzel Long's Health Care Industry Team and member of the firm's Cybersecurity and Privacy Specialty Team, Government & Internal Investigations Team, and Litigation and Dispute Resolution Team. She can be reached at Geroux@butzel.com.