COVER STORY

REPRINT February 2018

hfm

healthcare financial management association hfma.org

Chetan Parikh

safeguarding ePHI

a non-techie guide for healthcare leaders

The increasing sophistication of cyberattackers' techniques makes it high time for healthcare organizations to up their game in protecting patients' electronic protected health information (ePHI).

Cyberattackers who covet a significant financial return see a goldmine in the healthcare industry. The industry is under siege by profit-minded hackers, with the all-too-frequent result that healthcare organizations of all types are becoming compromised by sophisticated cyberattacks.

Given that health care is the largest part of the U.S. economy. safeguarding ePHI is considered a matter of national security, with severe consequences for organizations at which PHI protections are compromised by data breaches.

Consider the recent $115 million settlement for Anthem's 2015 data breach.[a] In addition to the financial penalty, Anthem must implement changes in its security system, provide credit monitoring services to data breach victims for at least two years, and cover out-of-pocket expenses that victims incurred due to the data breach.

Hackers target healthcare organizations for several reasons, the first of which is to gain access to the aforementioned goldmine of information.

Healthcare records include personal, financial, and medical information. A patient's record can be the ultimate cheat sheet for hackers because most of the identifiable personal information is permanent (e.g., Social Security number). These data offer value to hackers for many years to come. Hackers can leverage the data for crimes such as identity theft, financial fraud, tax misdemeanors, insurance fraud, and others.

Patient identity theft is not the only risk posed by a cyberattack. Healthcare organizations cannot afford a disruption in business continuity, and physicians and nurses depend on data to perform time-sensitive and life-saving procedures. When access to critical data and IT systems is prevented by hackers, patients' lives may be endangered.

AT A GLANCE

> Hackers are getting better than ever at pirating electronic protected health information, with records selling for a premium on the black market.

> Healthcare organizations have not invested adequate time or money in ensuring patient information is secure.

> By employing strategies for protecting such information, healthcare organizations can save the high financial and reputational costs that come from data breaches.

[a] Snell, E., "$115M Settlement Proposed in Anthem Data Breach Case," Health IT Security, June 26, 2017.

Unfortunately, for various reasons, hackers are having an easier time penetrating the networks of healthcare organizations.

Why Health Care Is Increasingly Vulnerable to Cyberattacks

The first reason the industry is facing a rising threat is that hackers are getting smarter. With growing hospital support of electronic health records (EHRs) for owned and independent physician practices, a whole new area of exposure has been opened. However, the healthcare industry has been slower to digitize than other industries, and healthcare organizations therefore may not be as knowledgeable about security as they should be. At the same time, cybercrimes and hackers have become more sophisticated.

This combination sets up healthcare organizations as ideal targets. For instance, various types of malware have evolved to become more complex. Ransomware has come a long way from variations that simply prevented users from accessing their files to those that use sophisticated encryption capabilities. In addition, even amateur hackers have low-cost access to tools that can make them experts in ransomware.

Complicating the situation is the fact that healthcare organizations tend to underinvest in cybersecurity. Hospitals often remain dependent on legacy IT infrastructure, running outdated on-site systems that leave them vulnerable to attack. This point is reinforced by findings of a recent study conducted by HIMSS and Symantec, which notes that healthcare organizations are underspending on cybersecurity programs, with less than 6 percent of their IT budgets, on average, allocated to cybersecurity.[b] In comparison, cybersecurity constitutes approximately 16 percent of the federal IT budget for 2016 and 15 percent of the average financial institution's budget. This discrepancy belies the fact that in the black market, healthcare data are 50 times more highly valued than financial data: According to the cyber division of the FBI, electronic medical records sell for $50 per chart on the black market, while a stolen Social Security number or credit card number will sell for $1.[c]

And the situation is likely to get worse, as shown in these statistics: By December of 2017, the U.S. healthcare industry was among the leaders in number of records compromised, with 27.9 percent of the total records coming from the industry. [d]

The Petya attack of 2017 infected companies in more than 150 countries across several industries, including many healthcare organizations in the United States.[e] As many as 80 percent of healthcare providers and insurers have had their IT compromised by cyberattacks, according to a 2017 survey conducted by KPMG International.[f] And a 2016 report from cybersecurity company NTTSecurity notes that 88 percent of all ransomware attacks in the second quarter of that year had been focused on the healthcare industry.[g]

Indeed, the healthcare industry was the most attacked industry during 2016.[h]

In short, problems such as malware, phishing, ransomware, and others are only going to get

[b] Cybersecurity in Healthcare: Why It's Not Enough; Why It Can't Wait, HIMSS Media, 2016.

[c] FBI Cyber Division, "Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain," private industry notification, April 8, 2014.

[d] Identity Theft Resource Center, Data Breach Reports, Dec. 27, 2017.

[e] Landi, H., "PA Health System, IT Vendor Affected by Petya Attack," *Healthcare Informatics*, June 28, 2017.

[f] KPMG, Healthcare Cybersecurity Execs Cite Surge in System Breaches, Data Loss Since 2015: KPMG Survey," July 31, 2017.

[g] Kern, C., "Healthcare Continues to Be Top Cyber Security Target," Health IT Outcomes, Sept. 16, 2016.

[h] Morgan. S., "Healthcare Industry Is the Bullseye for Hackers in 2017," CSO Online, Oct. 28, 2016.

worse if adequate cybersecurity is not in place. Healthcare leaders need to have appropriate policies, solutions, and processes—and the overall mindset—to defend against them.

Top 10 Practices for Defending Against Cyberattacks

With hackers at the ready, now is the time for healthcare organizations to prepare themselves. Below are 10 business and technical considerations organizations should address to mitigate the risk, and damage, of a cyberattack.

Regularly perform audits of existing security infrastructure. In today's digital age, ePHI faces a growing number of security threats from all quarters. An audit plays a key role in reviewing security controls and measures, uncovering potential threats before they spiral into larger issues, and identifying opportunities to strengthen enterprisewide security. Hospital security audits should accomplish the following:

> Highlight existing privacy risks and data security threats and the policies, controls, and procedures in place to deal with those risks.
> Ascertain whether protective procedures are being consistently and diligently followed by the respective teams.
> Provide reports of both emerging and existing cyber risks to the hospital, as well as recommendations to mitigate them.
> Ensure that all cybersecurity regulations are being met.
> Monitor the effectiveness of training sessions and analyze data on metrics such as repeat offenders.

Establish a cybersecurity strategy. This strategy should revolve around following three key elements. First, from the results of audits, organizations should keep an eye on all identified gaps and their severity. This approach should be clearly laid out in thorough and detailed policies. Second, organizations should provide defense at every network access point, to protect all types of sensitive data. Healthcare organizations should take a proactive approach, continuously scanning to detect patterns that suggest an intrusion. Finally, organizations should implement effective controls, processes, and rapid-response mechanisms to establish a culture of vigilance, instill good habits regarding digital security, and expedite action when a breach occurs. Continuous, enterprisewide training on cybersecurity is a wise investment, because users are the weakest link in a healthcare cybersecurity chain.

Adopt a culture of full transparency in communication. A lack of communication, or poor communication, between upper management and IT about the importance of cybersecurity can lead to significant damage to a hospital's bottom line and public image if a breach occurs.[i] There are also other stakeholders involved in securing a network, including vendors, suppliers, and contractors. Transparent communication is the key to success. To be able to improve cybersecurity communication, an organization must ensure the following conditions exist:

> Cross-functional teams are communicating risks effectively, and awareness of security risks has been spread to people in areas other than IT, such as engineering, administration, marketing, and others.
> The IT team understands how to translate technical details of security risks into information that can be easily comprehended and digested by upper management.
> Team leaders and members charged with execution agree on a set of objectives so that key success metrics are clear to all stakeholders and everyone understands the importance of critical applications and sensitive data sets.

[i] Ponemon Institute and Websense, *Exposing the Cybersecurity Cracks: A Global Perspective*, April 2014.

Encrypt data at every stage. A 2014 study found that unencrypted and unauthenticated communication among medical devices not only exposed the devices to hacking but also provided direct access to electronic medical records such as ePHI.[j] The same study stated that not all vendors do enough to secure these devices before providing them to hospitals. Thus, hospitals should continuously evaluate such vendors to ensure devices are secure. Encryption should be enabled for all sensitive data, and robust encryption capabilities should be supported by the applicable software. If legacy applications and storage are not going to be replaced, encryption solutions should be used to manage this crucial function.

Implement data-centric protection of valuable data. No matter how many cybersecurity measures an organization implements to stop a breach, a sophisticated hacker may be able to get through. Healthcare organizations should execute data-centric protection for their most valuable data and applications so even if hackers get in, the information captured will not disrupt business continuity.

The starting point for any leader is to determine what data are most valuable to the hospital and then to assess the business risk of a breach of that data. One such vulnerability might be the loss of ePHI by a negligent nurse who did not comply with regulations. Once the organization has identified the most important information data assets and prioritized them, it's time to incorporate protective measures across the data lifecycle. Organizations also should adopt and rigorously follow cybersecurity frameworks such as that of the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce.

Implement real-time threat intelligence and protection. With increasing new threats, healthcare organizations should use threat intelligence to secure unexpected application, data, and user behaviors. Four strategies are as follows:

> Employ round-the-clock monitoring and real-time notification to rapidly isolate dubious activities.

> Review patch and configuration management to make sure standardized tools are in place.

> Enhance testing, response, and protection abilities for network at-risk areas.

> Ensure firewall, intrusion detection and protection system, antivirus, and associated security technologies are updated.

Test data backup and disaster recovery capability. Healthcare organizations can't afford to lose their critical business data. It is essential to keep in place a recovery solution and a backup that protects critical data from all threats. These systems should be tested on an ongoing basis to ensure the organization can isolate a cyberattack and recover fully from its effects. Organizations should invest in preparedness with multiple backups, disaster recovery mechanisms, and business continuity plans, and by keeping systems updated, upgraded, and patched to minimize the chance or impact of a cyberattack.

Deploy anti-ransomware/phishing malware solutions. Healthcare organizations should implement solutions that can detect, isolate, and support recovery from phishing, ransomware, or malware threats. Data loss prevention is a vital element in any cybersecurity infrastructure because of its ability to prevent data breaches.

Establish multitiered authentication and account access management policies. Because users are the weak link in the security chain, hospitals should limit data access to those whose job requires it. Best practices include:

[j] Zetter, K., "It's Insanely Easy to Hack Hospital Equipment," *Wired*, April 25, 2014.

- > Evaluating options for multifactorial authentication of ePHI access and elevated privileges
- > Automating with alerts for all access to ePHI and other sensitive data
- > Implementing modern technologies like provisioning workflow and single sign-on, or reducing sign-on across all applications
- > Actively auditing file access and multiple controls for privileged accounts

Adopt cloud-based technology. Cloud technology beats traditional on-site systems in storage, scalability, ease of data access, flexibility, investment, and data security. Consider this statistic: Of all the breaches affecting more than 1 million patient records in 2015, only one involved a breach of cloud services.[k] Cloud-based software leverages advanced technologies for data security, network protection, and identity and access management. It includes a range of services such as advanced authentication, penetration and vulnerability testing, real-time threat monitoring, network behavior analysis, and security-alert analysis. In short, cloud-based software offers top-notch security, virtually zero downtime, faster data-recovery mechanisms, and 100 percent availability of data.

The Cost-Benefit Analysis of a Secure Network

The average total cost of a data breach in the United States has reached $7.35 million, a significant percentage of which is due to business disruption.[l] Adding to that is the cost of the regulatory compliance breach: HIPAA settlement fines, on average, amount to about $1.1 million, and this figure is only increasing as the Department of Health & Human Services becomes more aggressive in enforcing HIPAA regulations, according to a 2012 study by Protenus.[m] Clearly, a data breach will result in negative cash flow, damaging both the financial viability and reputation of the hospital. However, investing in cybersecurity can translate to substantial cost savings over time. Technologies such as security intelligence, advanced identity and access governance, and encryption deliver organizational cost savings of $2.8 million, $2.4 million, and $1 million, respectively.[n]

Given the growing sophistication of hackers, it's high time for healthcare organizations to secure their networks. Investigating and adopting sensible practices for the protection of ePHI can go a long way to ensuring an organization avoids the high cost of a breach. ■

[k] van Deursen, N., "2015 Was the Year of the Health Care Data Breach, but Cloud Sails Around the Storm," Security Intelligence, Dec. 18, 2015.

[l] Ponemon Institute, *2017 Cost of Data Breach Study*, 2017.

[m] Protenus, "Cost of a Breach: A Business Case for Proactive Privacy Analytics."

[n] Accenture, Cost of Cyber Crime Study, 2017.

About the author

Chetan Parikh
is CEO, ezDI, Louisville, Ky.
(chetan@ezdi.us).

Reprinted from the February 2018 issue of *hfm* magazine. Copyright 2018, Healthcare Financial Management Association,
Three Westbrook Corporate Center, Suite 600, Westchester, IL 60154-5732. For more information, call 800-252-HFMA or visit hfma.org.