AICPA

FVS Eye on Fraud

The AICPA Forensic and Valuation Services quarterly report on fraud trends and topics

The moving target: Cybercrime in health care and why it's time for organizations to take action

Issued by the AICPA FLS Fraud Task Force
Lead Author: Marc W. Courey, CPA/CFF, JD, LLM, CFE, CICA, CCEP, CIA

In July 2018, a regional health care provider based in Missouri shut down its electronic health record (EHR) system — housing the digital equivalent of a patient's paper-based health chart — to recover from a malicious ransomware attack. Hackers had successfully encrypted patient records, causing officials to restrict staff access for an extended period.[1]

Fortunately for the health care provider, an incident-response plan was already in place, enabling staff to act quickly once the ransomware attack was discovered. While an outside forensics firm decrypted patient files and initiated recovery efforts, medical staff were able to continue providing general care to patients; they sent intensive cases, such as trauma and stroke patients, to other facilities to ensure their continued care. Grateful patients went so far as to visit the medical center's social media platforms to leave glowing feedback on how well staff responded to the attack.

Winter 2019, Issue 1

Inside this issue

Practice tips 3–4
Real cyberattacks in the health care space 5–6
Real-life case study 8

Continued on page 2

[1] Jessica Davis, "Update: Ransomware attack on Cass Regional shuts down EHR," Healthcare IT News, July 11, 2018, accessed December 2018, https://www.healthcareitnews.com/news/update-ransomware-attack-cass-regional-shuts-down-ehr.

Compared to other industries, health care is a rich target for fraudsters, who can potentially extort huge sums of money from the sector.

This situation is, of course, somewhat of an anomaly — the cybersecurity story with a somewhat happy ending. In most cases, however, there is no happy ending. One look at the headlines over the past few years will tell you just how quickly cybercrime has evolved into a real and dangerous global threat, and health care is far from the only targeted industry. Large and, presumably, technology-sophisticated corporations, such as Target and Equifax, have fallen prey to data breaches that caused reputational damage and tangible harm to the victims caught in the crosshairs.

The costs that a cyberattack incur can be astronomical. These costs include forensic investigations into the attack in addition to damages resulting from the breach of intellectual property, money, or personal and financial data. By 2021, costs related to cybercrime are projected to hit $6 trillion annually.[2] That eye-opening number explains why an overwhelming 86% of American companies increased their cybersecurity spending last year.[3]

It's clear that leaders and C-suite executives all over the globe must put cybersecurity at the top of their priority list. But for health care leadership teams, the issue is even more dire. Why?

A moving target

Compared to other industries, health care is a rich target for fraudsters, who can potentially extort huge sums of money from the sector. The United States spends more on health care than any other country. In 2017, Americans dished out a staggering $3.5 trillion in health care expenses, equivalent to about $10,739 per person.[4] Health care organizations have a lot at risk — in its 2017 Cost of Data Breach Study, sponsored by IBM Security, the Ponemon Institute reported that, at $380 per record, health care had the highest per-capita cost associated with data breaches.[5]

Dollars spent represent only one side of the story. In this digital age, availability of information is everything, making the health care sector a gold mine for hackers. Health care requires the routine exchange of highly sensitive information, including patients' names, birth dates, Social Security numbers, and other personally identifiable details. On the dark web, personal medical records and other health-related information are highly sought. Hackers use patient diagnoses and prescription data for extortion and leverage addresses and insurance information in fraudulent billing schemes.

Continued on page 3

[2] Susan Schaibly, "Files for Ransom," *NetworkWorld*, September 2005, networkworld.com/article/2314306/lan-wan/files-for-ransom.html.

[3] "Cyberfraud – Current issues and trends," AICPA FVS Eye on Fraud, Summer 2018, Issue 3 (Available via AICPA Forensic & Valuation Services Online Professional Library).

[4] Thales, 2018 Data Threat Report – Global Edition, p. 6, accessed December 2018, http://go.thalesesecurity.com/rs/480-LWA-970/images/2018-Data-Threat-Report-Global-Edition-ar.pdf.

[5] 2017 Cost of Data Breach Study: Global Overview, Ponemon Institute and IBM Security, June 2017, accessed December 2018, https://www.ibm.com/downloads/cas/ZYKLN2E3

Ransomware, spread through phishing emails or infected web pages, holds dual appeal for fraudsters. On one hand, it can serve as the smokescreen for concealing misappropriated information, with patients and their health care providers none the wiser. On the other hand, the very nature of health care services makes the loss of EHRs, even for a short time, extremely detrimental — increasing the likelihood that the provider will pay the ransom.

In 2016, multiple hospitals in Lincolnshire, England, canceled hundreds of planned operations, outpatient appointments, and diagnostic procedures after they were affected by the overall attack on the National Health Service (NHS) network, further illustrating the broad impact these types of attacks can have on the health care industry.

Regulatory bodies are stepping in

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 requires health care organizations to have information-security programs that properly safeguard patients' protected health information (PHI). For instance, the HIPAA Security Rule requires anyone who transmits PHI over an open network to first encrypt the information, including emails, text messages, faxes, and so on.[6] Because the transmission of unencrypted PHI is a reportable breach, the Office of Civil Rights (OCR) can dole out hefty penalties to organizations that don't comply.

Many health care organizations are still confused about their exact responsibilities under HIPAA, especially as they relate to cybersecurity. This confusion arises from the fact that many haven't taken the appropriate steps to secure the areas within their organization most vulnerable to attack: people, processes, and technology.

The people factor

In 2018, the consulting firm Accenture published a report exploring why employees are the weak link in health care organizations' cybersecurity.[7] The firm surveyed 900 health care providers and payer organizations across the U.S. and Canada. Among its findings were some surprises, such as the fact that

Continued on page 4

[6] "Does the Security Rule allow for sending electronic PHI (e-PHI) in email or over the Internet? If so, what protections must be applied?," HHS, July 26, 2013, accessed June 14, 2018. https://www.hhs.gov/hipaa/for-professionals/faq/2006/does-the-security-rule-allow-for-sending-electronic-phi-in-an-email/index.html

[7] John Schoew, "Losing the Cybersecurity Culture War," Accenture, February 20, 2018, accessed January 2019, https://www.accenture.com/us-en/blogs/blogs-losing-cybersecurity-culture-war.

Practice tips

Your client health care organizations can't afford to overlook cybercrime. CPAs, in concert with other knowledgeable professionals, can help clients patch obvious vulnerabilities, implement best practices, embrace continuous staff training, and develop better communications. You can also help your clients answer the tough security question: How do we balance necessary access to and availability of information against the critical need for our organization to protect itself, its employees, and its patients — the very reason for its existence — from cybercrime?

CPAs can, and should, speak with clients about how the right tools and software can go a long way toward enhancing their cybersecurity program. CPAs can also be a trusted voice of reason to help clients remember that no tool or technology can replace comprehensive staff training and solid risk-management processes, which comprise the following actions:

- Automate. Automation can help organizations defend themselves against critical aspects of today's threat landscape; CPAs can help clients evaluate automation options. One trend in the automation of cybersecurity involves intelligent agents that operate at endpoints (desktops, laptops, servers, mobile devices, and so forth) and identify, report, and stop suspicious activity without human intervention. Over time, these agents will be able to promptly respond to and halt improper activity from cyber sources (such as ransomware) or human sources (such as employees who copy unauthorized information).

- Train. Although automation can be valuable to your client's cybersecurity program, it's important for your client to recognize that its people constitute both a significant risk and an important asset in the organization's cybersecurity strategy. CPAs can help clients remember that if they invest in ongoing, comprehensive training, their employees will be able to spot and prevent attacks, such as ransomware camouflaged as an email attachment, or phishing emails that divert users to an imposter site to capture login credentials.

Continued on page 4

21% of respondents keep their username and password written down next to their computer.[8] In a separate survey, conducted by Kickstand Communications for secure-file-sharing services firm Biscom, 87% of health care workers admitted to using nonsecure email to transmit sensitive data and information, a violation of the HIPAA Security Rule that requires senders to encrypt PHI before sending it over open networks.[9] According to the same survey, health care employees are 36% more likely to share sensitive data — such as patient and payment information — using nonsecure email than those working in the financial services industry, heavily regulated in its own right.

Based on this data alone, hackers have an open gateway for infecting health care organizations with phishing emails, among the most common attacks against internet users. All it takes is for one unsuspecting employee to click on an embedded link or download an attached file. Once they've taken the bait, the hacker attacks, infecting the employee's network and bringing critical, sensitive information to the forefront.

Bad security habits span industries, compromising employee and customer (or patient) data with drastic consequences. These habits are rarely the product of malicious intent; they're the result of poor (or nonexistent) education and training. Most health care workers don't have the cybersecurity knowledge to know what they need to be wary of.

The advent of social media has opened the door to widespread distribution of information. In matters large and small, we freely share minute-by-minute updates of our everyday lives with the entire world, all from the "comfort" of our news feeds. Many of us don't realize that we could be exposing ourselves and our organization to fraudsters, who are quick to capitalize. A health care employee might discuss their job on Facebook and post photos they took at work without recognizing they've accidentally disclosed confidential information. Although social media can be an effective method for health care professionals to share and receive information — such as notifying the public about outbreaks or hazards, or quickly locating current information on treatments or conditions — social media can also "go wrong" in health care settings. Since 2012, there have been at least 47 documented incidents of inappropriate social media use by assisted-living facilities. These include intentional misdeeds (such as posting pictures of residents' genitalia) and inadvertent disclosures (such as carelessly posting photos or names of residents without permission)[10].

Practice tips (continued)

- Insure. Given the difficulty of responding to and recovering from a cyberattack, insurance should be a component of every organization's risk-management strategy. Purchasing cybercrime policies can be challenging; CPAs can help clients understand both the importance of having insurance and what types of coverage are available to their organization.

Process breakdowns

In 2017, the OCR performed its second in a series of HIPAA compliance audits. It discovered that nearly all health care organizations it audited — a whopping 94% — had substandard risk-management plans.[11] Not having a comprehensive plan to prevent and respond to a cybersecurity incident can cut millions of dollars from a health care organization's bottom line.

A risk-management plan requires sound operational processes and procedures; most organizations don't have the right ones in place to manage cyberthreats effectively. Take offboarding, for

Continued on page 5

[8] "1 in 5 health employees willing to sell confidential data: 7 survey insights," Julie Spitzer, Becker's Hospital Review, March 2, 2018, accessed December 2018, https://www.beckershospitalreview.com/cybersecurity/1-in-5-health-employees-willing-to-sell-confidential-data-7-survey-insights.html.

[9] Fred Donovan, "Most healthcare Workers Admit to Non-Secure Healthcare Data Sharing," HealthITSecurity.com, May 21, 2018, accessed December 2018, https://healthitsecurity.com/news/most-healthcare-workers-admit-to-non-secure-healthcare-data-sharing.

[10] Charles Ornstein, "Inappropriate Social Media Posts by Nursing Home Workers, Detailed," Pro Publica, December 21, 2015, accessed December 2018, https://www.propublica.org/article/inappropriate-social-media-posts-by-nursing-home-workers-detailed

[11] "Noncompliance with HIPPA Costs Healthcare Organizations Dearly," HIPAA Journal, December 13, 2017, accessed December 2018, https://www.hipaajournal.com/noncompliance-with-hipaa-costs/.

instance. Once an employee has left the organization, whether voluntarily or involuntarily, many organizations fail to properly timely shut down the former employee's access to email or critical internal technologies. Health care organizations must introduce some basic processes to remedy this.

A good basic process example, related to instances of PHI being faxed to nonmedical recipients, can be learned from Saskatchewan Health Authority's implementation of a new process for outbound faxes in which doctor's names and their fax numbers were chosen from a centrally maintained list. This process minimized the risk of entering incorrect fax numbers and the subsequent missending of sensitive information.

In addition to operational breakdowns, many health care organizations lack a strong process to regularly review access to information, tools, and platforms. Consider an employee who, working on a particular patient's case, had access to a specific application or database needed for that case. When the employee moves on to another case, that access should be promptly removed; too often, this does not happen.

Process breakdowns also apply to the protection of important documents. Though many organizations are moving toward electronic charting systems, facilities remain — often in rural or underserved communities with fewer resources — that still rely on paper records. Some of these facilities have no process for disposing of confidential information. Printed PHI records, once thrown into the trash or recycling bin, are at risk of compromise, both before and after leaving the facility. For instance, when one Missouri hospital moved to a new campus while its old campus was being prepared for demolition, it left behind paper documents containing information on more than 300,000 patients.

Gaps in tools and technology

Like so many other industries, health care is evolving through new technologies, such as artificial intelligence (AI) and the Internet of things (IoT). IoMT devices [12], in particular, are one of the most buzzed-about advancements in health care today — the market for these products is projected to reach $136.8 billion worldwide by 2021.[13] These devices and applications collate data that are provided to health care IT systems through online networks; like

From the headlines: Real cyberattacks in the health care space

- Technology access gone wrong. In July 2018, the Oklahoma Veterans Affairs (VA) department reported that approximately 50 VA employees were granted access to patient records in 2 facilities via their personal mobile devices. This level of "bring-your-own-device" access temporarily permitted employees to give medications during a roughly 6-hour network outage. The concern here is that access was granted despite the department's failure to use mobile-device management software to secure employees' devices.[14]

- Unsecured database leads to exploitation. Last year, a German cybersecurity and IT enthusiast discovered an online health care database that was public due to a misconfiguration. This exposed the personal information and health records of 2.3 million Mexican patients via the internet, including their full name, gender, identity codes, insurance policy numbers, date of birth, home address, and their disability or migrant status.[15]

- No organization is immune. Reuters reported in July 2018 that a major cyberattack on Singapore's government health database enabled hackers to steal the personal information of about 1.5 million people, including the prime minister.[16]

Continued on page 6

[12] Internet of Medical Things (IoMT) devices include developed and emerging technologies that can provide ways to monitor health indicators, monitor medical device operation, or provide control to medical devices, all in real-time through internet connectivity. Examples of such devices include sensors which measure blood pressure, glucose, or other body functions or therapy delivery devices such as insulin or drug delivery pumps.

[13] Bernard Marr, "Why The Internet of Medical Things (IoMT) Will Start To Transform Healthcare in 2018," Forbes, January 25, 2018, accessed December 2018, https://www.forbes.com/sites/bernardmarr/2018/01/25/why-the-internet-of-medical-things-iomt-will-start-to-transform-healthcare-in-2018/#7de9f64f4a3c.

[14] Marianne Kolbasuk McGee, "Should Staff Ever Use Personal Devices to Access Patient Data?," Bank Info Security, August 14, 2018, accessed December 2018, https://www.bankinfosecurity.com/should-staff-ever-use-personal-devices-to-access-patient-health-data-a-11346.

[15] Bob Diachenko, "Millions of health records exposed to public in Mexico," PharmaPhorum, December 14, 2018, accessed December 2018, https://pharmaphorum.com/news/health-records-publically-exposed/.

[16] Jack Kim, Aradhana Aravindan, "Singapore's worst cyberattack steals personal data of 1.5 million including PM," Reuters, July 20, 2018, accessed December 2018, https://in.reuters.com/article/singapore-cyberattack/singapores-worst-cyberattack-steals-personal-data-of-1-5-million-including-pm-idINKBN1KA14L.

any new technology, the full capabilities and security limitations of these products aren't yet fully known. These types of tools are typically developed fairly quickly, with security issues often unaddressed. Risks that are routinely managed in other industries can pose unique risks in the health care environment.

Another cybersecurity pitfall health care organizations run into ties back to email encryption. Even though it's a HIPAA Security Rule, some organizations fail to provide employees with the tools to properly encrypt PHI before they transmit it over an open network. Organizations continue to struggle with PHI encryption, and not just in email. At rest and in transit, encryption protects organizations from low-tech attacks.

Because so many organizations have no risk-management plan, other aspects of their technology infrastructure miss the mark on cybersecurity, most notably through antiquated security systems. Health care organizations may be susceptible to tunnel vision, prioritizing patient care and delivery over investing in current cybersecurity technology. What they fail to realize is inadequate security puts not only the organization at risk, it can harm patients as well. With today's integrated health care delivery models, losing even a portion of an organization's systems due to a cybersecurity incident can easily trigger mandatory delays in delivering critical care to patients. Another looming risk centers on potential breaches of current and future IoMT devices. In its 2017 survey, the Ponemon Institute found that most respondents related to health care organizations and medical-device manufacturing believed a device they used or manufactured would be attacked within the next year.

Ransomware: the prevalent attack[17]

Cybersecurity attacks come in myriad forms, but the one that runs most rampant in health care organizations is ransomware. In fact, the industry accounted for 45% of all ransomware attacks in 2017.[18]

What does ransomware look like? It usually comes as malicious software (also known as "malware") that prevents a user from accessing their computer system, network, or critical data until they pay a ransom to the hacker who deployed it. Given the sheer volume of sensitive information that permeates health care organizations, ransomware is an ultra dangerous threat.

Imagine that a health care provider — such as a hospital or clinic — gets hit with ransomware. The attack would likely prevent staff access to any patient records until they pay the ransom. The waterfall effects of this type of breach are monumental, affecting the organization's ability to provide care and damaging its reputation, operations, financials, and, potentially, the future of its business.

The risk of not taking action

Health care is at risk of falling far behind other industries in cybersecurity; major health care data breaches in recent years underscore this weakness. Organizations that fail to address the vulnerabilities outlined previously are taking an undeniable risk. What would happen to an organization's financial stability

Continued on page 7

From the headlines: Real cyberattacks in the health care space (continued)

- Missing devices cause data breaches. By April 2018, Data Breach Today tallied 18 incidents in which unencrypted laptops and other devices were lost or stolen, affecting about 68,000 individuals.[19]
- Ransomware wreaks havoc. In 2016, Hollywood Presbyterian Medical Center reported a ransomware attack that affected its administrative functions. The center determined that the fastest, most efficient way to restore its systems was to pay the 40-bitcoin ransom, then worth some $17,000.[20]

[17] Learn more: "Ransomware," AICPA FVS Eye on Fraud, Fall 2018, Issue 4 (Available via AICPA Forensic and Valuation Services Online Professional Library).

[18] Rajiv Leventhal, "Report: Healthcare Accounted for 45% of All Ransomware Attacks in 2017," Healthcare Informatics, February 22, 2018, accessed December 2018, https://www.hcinnovationgroup.com/cybersecurity/news/13029850/report-healthcare-accounted-for-45-of-all-ransomware-attacks-in-2017.

[19] Marianne Kolbasuk McGee, "Health Data Breach Tally Spikes in Recent Weeks," Data Breach Today, April 17, 2018, accessed December 2018, https://www.databreachtoday.com/health-data-breach-tally-spikes-in-recent-weeks-a-10816.

[20] Richard Winton, "Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating," Los Angeles Times, February 18, 2016, accessed December 2018, https://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html.

if an employee, with no cybersecurity training or education, unknowingly wires money to a fraudster? The ability to perform diagnostics, deliver patient care, and access key records can be lost in an instant if an organization fails to secure its treatment systems or invest in the right cybersecurity technology. If a breach goes public, an organization must notify its patients, regulators, vendors, and other stakeholders, resulting in regulatory and reputational damage that can be far costlier than an actual financial loss.

The question becomes: What can health care providers do now to prevent cybercrime? It starts with addressing the three essential business areas discussed above:

1.Educate, train, and communicate with medical staff regularly about cybersecurity

Start by implementing some basic best practices. Require employees to create passwords that adhere to a specific complexity standard and introduce rules for changing them periodically. Organizations can also invest in single-sign-on password-management systems, enabling staff to create complicated and unpredictable passwords without having to remember them.

Train employees to spot malicious emails and educate them on why they must pay attention to email content. Ensure they understand the need for encryption and give them the tools they need to protect PHI. Remember: education is not a once-and-done practice; it's essential to create an ongoing cybersecurity culture within the organization, routinely educating employees on cyber risks. Let the staff know that you will test their knowledge and vigilance by periodically sending suspicious emails or shady requests for patient information to see how many employees engage with them.

The cyber landscape is constantly changing, making continuous communication all the more critical. Remind your staff that their ability to protect their patients is on the line when cybersecurity isn't considered at every turn. Combat the "out of sight, out of mind" mindset that puts many health care organizations at risk.

2.Processes are key — take steps to make them airtight

The entire organization — from the board or directors to medical staff to administrative staff — needs to adopt cybersecurity and risk-management processes. Employees need to follow established processes. For instance, they cannot authorize payments above a set amount without first taking certain security-focused steps. Drive home the fact that processes are there to protect the organization and its patients.

Consider the document-management process, for example. With the prevalence of EHRs, organizations often overlook paper records, but these documents are easily and frequently compromised. Minimize this risk by hiring a shredding service, which can provide secured paper-disposal stations.

Another easily overlooked risk stems from trusted third-party relationships, such as with vendors or partners. These relationships can involve frequent communication and implicit trust in them with no verification of their cybersecurity protocols. A frequent example concerns the adoption of Microsoft Office 365, particularly related to email. For organizations that previously didn't have, or didn't allow, staff to access email through the internet, Microsoft's "standard" implementation allows remote email access without the security precautions afforded by two-factor authentication. Phished credentials can then expose staff email accounts to unauthorized parties, who can access PHI contained in the body of emails or in attachments. One third-party patient database, which included remote access, used a simple user ID and password common to all of the provider's customers. Once this flaw was discovered, all health care organizations that used this application — and their patients' PHI — were vulnerable.

3.Focus on technology as a part of the cyber fraud solution — not the "Silver Bullet"

Technology has fundamentally changed our world, allowing us to connect and communicate like never before.

Many health care organizations are moving toward implementing more adaptive types of security to better protect themselves and their patients from fraud. Processes that antivirus software used to handle are being replaced by AI-based tools that recognize the behavior of programs and employees and quietly halt careless practices. For instance, if a medical staff member is stealing and copying data, an adaptive security program could automatically detect and suspend this activity until further review — preventing fraud before it happens.

Continued on page 8

The AICPA's Cybersecurity Resource Center provides the following resources to practitioners to help assess risk and provide information on risk-management programs:

- AICPA Cybersecurity Resource Center
- Cybersecurity Fundamentals for Finance and Accounting Professionals Certificate
- Cybersecurity Readiness Assessments
- Cybersecurity Advisory Services: Readiness Assessment Deep Dive

Real-Life case study: When it comes to cybersecurity, process is everything

A health care facility subcontractor (whose contract was about to end) moved a patient database to his personal laptop, an inappropriate action that was nevertheless possible on the facility's network. Had the subcontractor copied — but not moved — the database, the facility might never have been alerted to his data theft.

When the subcontractor returned his rental car, he left his laptop and unencrypted external hard drive in the trunk. Both contained the database. Not only had the subcontractor removed the

database without authorization, but it also was outside of his control for days while the car-rental company located, boxed, and shipped the laptop and external hard drive to him.

Unauthorized activity can be circumvented with consistent, established processes for safeguarding access to information, tools, and platforms. This real-life scenario illustrates why process is everything when it comes to cybersecurity in the health care space.