WHITE PAPER

CDW PEOPLE WHO GET IT
HEALTHCARE

ENSURING THE SECURITY OF PATIENT DATA

Healthcare organizations must adopt up-to-date solutions and strategies to manage cyberthreats and protect sensitive information.

EXECUTIVE SUMMARY

Each year, healthcare organizations collect, store and share more patient data than they did the year before — the result of evolving bedside medical devices, clinician mobility tools and emerging Internet of Things use cases. More data means more potential jackpots for hackers, whose attack methods continue to evolve.

The cost of a data breach can be immense. Providers must alert patients and report the breach to the government, resulting in both a hit to the organization's reputation and the potential for steep fines.

Cybersecurity initiatives are also costly for organizations. Every dollar and hour spent on protecting data must come from some department's budget. To keep patient data safe without bursting IT budgets, hospitals must implement solutions that are both effective and efficient.

The deployment of robust security solutions and services requires a thoughtful, multilayered strategy that addresses both local and remote patient environments while it also keeps up with the maturation of IT systems and cyberthreats.

An Expanded Threat Landscape

When hackers lay their eyes on the sort of sensitive personal data collected and protected by hospitals and other healthcare organizations, they see dollar signs.

On the black market, a single credit card number might only fetch a price of 50 cents because there's a short window of time in which to exploit the compromised data before a financial institution recognizes the breach, invalidates the account and issues the victimized customer a new payment card.

Hospitals, however, collect information that can't be changed: Social Security numbers, birthdates, current and past addresses, next of kin. Because of its permanent nature, criminals can continue to exploit such compromised data for years, using the information to steal victims' identities for financial gain. Consequently, a single stolen record can command a price approaching $100. For obvious reasons, those circumstances mean that hospitals are a hugely attractive target for hackers.

According to the 2018 Healthcare Information and Management Systems Society (HIMSS) Cybersecurity Survey, 76 percent of healthcare organizations surveyed experienced a "significant security incident" in the 12 months prior — attacks that resulted from a wide variety of attack methods and motivations. The plurality of those incidents (38 percent) stemmed from online scam artists engaging in activities such as phishing and spear phishing. Negligent insiders — well-meaning personnel with trusted access who inadvertently trigger a data breach — accounted for 21 percent of incidents. Healthcare organizations face fines for breaches that don't involve external actors. Most hospital breaches result from healthcare insiders looking up information about family members, friends, neighbors and acquaintances without authorization. Meanwhile, hackers were responsible for 20 percent of breaches, and nation state actors, hacktivists, social engineers and malicious insiders each accounted for between 2 and 5 percent of breaches.

By a wide margin, email was the most common initial point of compromise for these incidents, with 62 percent of breaches resulting from a phishing email or similar attack. Attacks are also launched via organizational or third-party websites, hardware and software preloaded with malware, infected mobile or medical devices, and compromised cloud providers — but none of those attack vectors triggered more than 3.2 percent of the total number of breaches.

Nearly half (47 percent) of those attacks were caught within a day, while another 21 percent were sniffed out within a week. Still, roughly 4 percent of attacks took between a week and a month to catch, while 5 percent took between one and three months to detect. A handful of attacks weren't caught for four, seven or even 12 months.

Somewhat worryingly, only 41 percent of attacks were caught by organizations' internal security teams. Most were caught by other team members and third-party vendors, and 3 percent were discovered and reported by patients themselves.

Cyberattacks are such a problem for healthcare providers that the ECRI Institute ranks ransomware and other cybersecurity threats No. 1 in its "Top 10 Health Technology Hazards for 2018," above issues such as missed alarms, improper cleaning of equipment and radiation exposure from imaging tools.

"In a healthcare environment, a malware attack can significantly impact care delivery by rendering health IT systems unusable, by preventing access to patient data and records, and by affecting the functionality of networked medical devices," the report states. "Further, such attacks can disable third-party services, disrupt the supply chain for drugs and supplies, and affect building and infrastructure systems."

It is with good reason that the report calls out ransomware. Some experts say such attacks rose by roughly 89 percent in 2017, while other reports say it accounts for 85 percent of all malware in the healthcare industry.

Pinpointing Vulnerabilities

Last fall, the Department of Homeland Security issued a warning about a widespread vulnerability that exists in nearly all wireless networks. The vulnerability, dubbed KRACK (key reinstallation attacks), affected wireless networks encrypted using the Wi-Fi Protected Access 2 protocol, including those of many healthcare organizations.

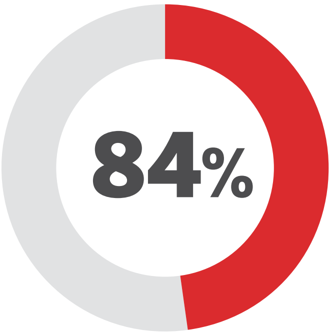
The warning underscored the necessity of healthcare IT leaders staying abreast of — and mitigating — known vulnerabilities. For healthcare organizations, sources of vulnerabilities come in a variety of forms:

- Many services within healthcare organizations require only single-factor authentication, making them an attractive target for brute-force attacks.
- Some medical applications transmit patient data in clear text, a format that is known to be susceptible to man-in-the-middle attacks.

Unsecured medical devices expand the potential attack surface, a problem that can be mitigated through network segregation, firewalls and port blocking.

- Outdated software and operating systems — especially those that are no longer supported by vendors — are ripe for attack.
- Third-party vendors that manage systems are also a source of risk. By targeting a smaller, external vendor that works with a healthcare system, hostile actors can effectively bypass all the larger organization's security controls and gain direct access to its networks.

According to CDW's Cybersecurity Insight Report, last year's WannaCry virus, a "virulent strain of ransomware," spread across organizations' networks by exploiting vulnerabilities in Windows computers, causing billions of dollars in damages and "crippling" healthcare facilities throughout Britain.



Percentage of healthcare organizations that increased their use of resources year over year to address cybersecurity concerns[1]

Part of the reason healthcare organizations are such frequent targets is because many medical devices use older technologies that are more vulnerable to attacks. In 2017, one publication even dubbed medical devices "the next security nightmare."

A report on cybercrime in healthcare, also published in 2017, takes an in-depth look at the factors contributing to the prevalence of attacks in the industry. It notes that hospitals and other healthcare organizations often prioritize operations and efficiency over cybersecurity, leading to a lack of safeguards protecting digital assets. Many organizations, the authors say, simply lack the proper staff to handle digital threats and implement basic protection measures, such as two-factor authentication and encryption.

When digital healthcare assets such as electronic health records are attainable, they prove to be irresistible to hackers due to the range of profit-making activities they enable. Criminals can use data stolen from EHR systems, the report notes, to not only procure prescription drugs, create fake identities and obtain medical insurance, but also to create birth certificates and file fraudulent tax returns.

HIPAA standards and other data safety regulations exist to help ensure organizations take steps to protect sensitive data against this growing array of cyberthreats. However, mere compliance is often not enough to keep patient data safe. Those standards and safety regulations should be seen as the bare minimum. To rise to the challenge of today's threat environment, healthcare providers must evolve and mature their security postures beyond what is required by external regulators.

The Cost of Cybersecurity in Healthcare

It is impossible to separate cybersecurity efforts from dollars-and-cents concerns. Healthcare organizations have limited resources available for technology, and at most organizations, cybersecurity only accounts for a small minority (4 to 7 percent) of total IT budgets.

After organizations suffer a major breach, it's usually a simple task to convince executives to beef up cybersecurity solutions. But for hospitals, clinics and other healthcare providers that have escaped major incidents, it can prove difficult to persuade stakeholders outside of the IT and IS departments to view cybersecurity as a top priority. Such individuals may believe that, because patient information has remained safe thus far, the existing tools and processes must be working.

One way to garner C-suite buy-in on the importance of data security is to frame it as an investment rather than a cost. For instance, when the new CIO of a medium-sized academic medical center convinced other executive leaders of the importance of security, they invested nearly $8 million on cybersecurity assessments, investments and remediation, including three new full-time staff. To convince them, he demonstrated the potential cost of a successful breach — not only fines and lawsuits, but a hit to the organization's reputation among patients and the larger community.

As it happens, the health center suffered a small breach about six months into the new CIO's tenure. The breach, which affected

HIPAA Enforcement: A Tutorial

The Health Insurance Portability and Accountability Act of 1996 established the first set of systemwide security standards for protecting health data. The Office for Civil Rights within the Department of Health and Human Services is tasked with investigating potential violations.

The office takes several steps to enforce the HIPAA privacy and security rules:

- OCR learns of potential violations from compliance reviews and complaints.
- If a complaint is accepted for investigation, OCR will notify the person who filed the complaint and the entity named in the complaint. Both parties then are asked to present information about the incident. Covered entities are required by law to cooperate with complaint investigations.
- If a complaint describes a potential criminal action, OCR may refer the case to the Justice Department.
- The office reviews the evidence presented, and if it determines that an organization was not in compliance, it will attempt to resolve the case through voluntary compliance, corrective action and/or a resolution agreement.
- If the entity does not take satisfactory action, OCR may impose civil money penalties.

Source: [1] HIMSS, "2018 HIMSS Cybersecurity Survey," March 2018 about 3,000 patients, was caused by an error rather than a hack. Because the organization could demonstrate its remediation plan, it suffered no fines.

When presented with broader industry numbers about the costs of cyberbreaches, most stakeholders will be forced to acknowledge that insufficient early investment in security could be costlier in the long term. A 2018 report about cyber claims notes that healthcare claims made up only 17 percent of total cyber claims in 2017, yet those claims accounted for 28 percent of total breach costs, which suggests that successful attacks on healthcare providers cost organizations more than breaches in other industries.

According to the report, on average, 1.6 million records were exposed in a healthcare breach. Breaches that exposed personally identifiable information were far more common (5.2 million records) than breaches that exposed protected health information (386,000 records).

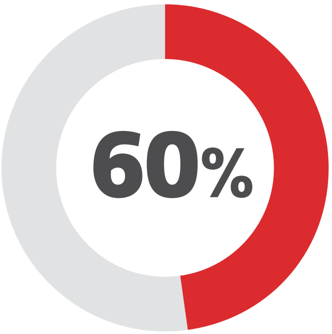
The industrywide numbers are even higher. In its 2017 report on cybercrime in healthcare Trend Micro estimates that cyberattacks against hospitals, clinics and doctors cost the U.S. healthcare industry a total of more than $6 billion each year, with an average breach costing a hospital $2.1 million.

Often, the headline-making dollar amount is far lower. For example, when Hollywood Presbyterian Medical Center suffered a ransomware attack in 2016, it was widely reported that the hospital paid the equivalent of $17,000 in cryptocurrency in order to regain access to its systems.

While this number may seem manageable, it fails to consider the lost productivity of clinicians or the resulting public relations fiasco. The hospital's network was down for more than a week, according to other reports. Officials struggled to maintain operations after losing access to email and some patient data, relying heavily on fax machines and telephones. The hospital transported some patients to other facilities, and the equipment necessary for such functions as CT scans, lab work and pharmacy needs was offline.

This is not to say that cost should not be a concern when considering cybersecurity solutions. While preventing a breach is typically more cost-effective than responding to a successful attack, the cost of effective cybersecurity systems remains a challenge.

Jigar Kadakia, chief information security and privacy officer at Partners HealthCare, addressed the economic challenges associated with cybersecurity at the joint HIMSS — College of Healthcare Information Management Executives (CHIME) cybersecurity forum in early 2018, saying that healthcare providers are often protecting their organizations "with fly swatters." He pointed out that the challenge is exacerbated by the fact that talented cybersecurity professionals are frequently able to command higher salaries in other sectors, forcing the industry to groom and manage homegrown talent.



Percentage of healthcare providers who consider a risk assessment to be their top consideration as a security investment[2]

Kadakia also said, however, that healthcare organizations can be convinced to loosen their purse strings when IT leaders make a compelling business case for cybersecurity investments.

"The financial people — the CFO and other folks — understand ROI," he said.

A Robust Support Infrastructure

Protecting patient data requires the deployment of security solutions and services that, in turn, require a multilayered strategy addressing both local and remote patient environments.

In some instances, this will mean adopting new and advanced cybersecurity technologies. But healthcare organizations can often improve their security posture simply by improving processes, training users and better integrating existing technologies.

Healthcare providers looking to safeguard patient data more effectively should consider the following actions:

Get Back to Basics — Advanced cybersecurity tools are wasted in IT environments where basic blocking and tackling steps are missed. For instance, in addition to implementing detailed firewall logging, organizations must also ensure that patch management is a part of their cybersecurity strategy. Password protection and access management are also critical.

Discussions with partners about cybersecurity strategies typically should begin with assessments of tools and tactics, such as firewalls, web and email security, and authentication controls (including two-factor authentication for remote access). Leaders must also prioritize policies around password management. When these relatively basic measures are lacking, it's nearly impossible for healthcare providers to take the next step in their cybersecurity evolution.

Segment Networks — Much of the challenge of safeguarding patient data is simply a matter of keeping sensitive information cordoned off from the rest of the network, making it more difficult for cyberattackers to reach it. Organizations that utilize network segmentation as a strategy deploy firewalls, routers and virtual LANs to restrict access to specific areas of their IT networks.

Segmentation also helps ensure that only those individuals who truly need it can access the disparate networks. For instance, many health organizations segment nonmedical systems, such as financial and human resources applications, onto separate networks from those that house patient data. In some cases, such a strategy can even save institutions money, as it allows organizations to rightsize their security investments.

Update Existing Tools — It's not enough to simply have cybersecurity systems in place. Organizations must also maintain and update these tools over time and ensure they have effective processes deployed to support them. For example, if a hospital installs an endpoint security tool but doesn't update that tool for three years, it likely won't be very effective at detecting and stopping newer, more advanced attacks.

Source: [2]Symantec, "Healthcare Cyber Security: Is That Light at the End of the Tunnel?" February 2018

Likewise, it's also important for hospitals to continually update processes, so when existing tools detect suspicious activities, IT employees are prepared and empowered to respond appropriately and immediately.

Assess and Train — Most data breaches in healthcare organizations begin with attacks on email. For instance, a recent report notes that slightly more than 64,000 patient records were exposed via email breaches in 2016, while in the fourth quarter of 2017 alone, 65,000 records were exposed in the same manner, a 467 percent increase overall. According to the HIMSS cybersecurity report, roughly 62 percent of healthcare organizations surveyed identified email as the most likely initial point of compromise.

While email security tools are important, hospitals and clinics must also make sure that employees are trained to sniff out phishing and spear phishing attempts. Some experts estimate advanced spear phishing attacks can cost businesses, on average, $140,000 per incident. Staff must learn to avoid clicking on suspicious links, inadvertently allowing malware onto the network. Phishing simulation and awareness campaigns can help healthcare cybersecurity managers better understand the current level of awareness among employees and provide targeted training as needed.

In a phishing simulation, IT or a third party sends faux phishing emails to employees and tracks who clicks on which links. Depending on how employees perform in the assessment, they can be directed to watch on-demand training videos or undergo more extensive educational programming.

Secure Productivity Tools — Security and productivity have not always gone hand in hand. The thinking goes: An organization could completely protect its network by clamping down on access but destroy employee productivity in the process. Conversely, a hospital could theoretically boost productivity by offering all employees unfettered access to all systems but create a veritable feeding frenzy for malicious actors.

However, some emerging cybersecurity tools can actually enhance clinician and staff productivity, rather than detract from it. For instance, secure messaging solutions emerged in response to clinicians sending each other text messages with patient updates using personal devices — a potential violation of HIPAA. Now that clinicians and other staff have access to secure messaging tools and services, they're using the technology to enhance communication, improve support and accelerate records access.

Similarly, single sign-on solutions emerged as a way to control access and identity management in healthcare settings. But they also simplify workflows and increase physician and nurse face time with patients.

Integrate and Improve — All too often, hospitals and other healthcare organizations have a number of effective, up-to-date cybersecurity tools at their disposal, but the systems lack integration, which hamstrings the effectiveness of the tools. This is an area where a third-party partner can help.

In a typical engagement, hospital IT administrators might feel confident in their tools but will ask a third-party solution architect to compare the cybersecurity environment to exemplary samples. During a cybersecurity gap analysis, the expert might find that existing firewall policies are not as effective as they could be or that password complexity standards should be raised to a higher level.

Machine Learning and Artificial Intelligence in Cybersecurity

Currently, machine learning and artificial intelligence help organizations better secure endpoints. The technologies can extend data security by analyzing behaviors across systems and keeping track of activities in vast data stores.

Jon Oltsik, a senior principal analyst at Enterprise Strategy Group, calls artificial intelligence in cybersecurity the real deal, but he says AI will serve mostly as "a helper app" for cybersecurity tools, rather than its own product category.

Oltsik cites ESG research:[3]

12% of enterprises have already deployed AI-based security analytics "extensively"; another 27 percent have such tools on a limited basis.

29% of cybersecurity professionals want to use AI-based security tools to accelerate incident detection, and 27 percent want to use these technologies to accelerate incident response.

24% of cybersecurity professionals want to use AI-based tools to better identify and communicate risk to their organizations. This would involve AI tools sorting through vulnerabilities, configuration errors and threat intelligence, then highlighting situations that call for immediate action.

22% of security professionals hope to use AI to gain a better understanding of cybersecurity situational awareness.

Source: [3]csconline.com, "Artificial intelligence and cybersecurity: The real deal," January 25, 2018

A third-party partner can also help busy healthcare IT managers stay abreast of evolving cybersecurity solutions and explore which emerging and next-generation tools can strengthen the organization's security posture.

Keeping patient data and IT systems safe calls for constant vigilence, regulatory knowledge, an educated staff and the right solutions and partners. In addition, leaders must balance effectiveness with both financial and operational efficiency.

CDW: A Security Partner That Gets IT

With decades of experience helping healthcare organizations with end-to-end IT security, CDW's solution architects are uniquely capable of helping hospitals protect patient data, secure their IT systems and launch an immediate response to any attacks.

Data Security — As mobility becomes even more entrenched and Internet of Things technologies emerge, healthcare organizations are creating more data every year. CDW can help hospitals and clinics deploy solutions, including tools to help with data loss prevention, encryption and endpoint protection to safeguard sensitive information.

Network Security — Today's networks require advanced security solutions, including next-generation firewalls and intrusion prevention systems, advanced threat detection, and network access control processes.

Mobile Security — Enterprise mobility management solutions must protect mobile devices, applications and content while still allowing users to be productive.

Cloud Security — Sensitive information no longer lives only on an organization's own machines. With data in the cloud, hospitals need to implement authentication, encryption and other security practices to prevent data loss. Specialized assessments from CDW can help organizations identify vulnerabilities.

Compliance — With broad experience assisting countless hospitals and care providers, CDW's solution architects have a wealth of knowledge about best practices for complying with HIPAA and other data security regulations.

The CDW Approach

ASSESS

Evaluate business objectives, technology environments, and processes; identify opportunities for performance improvements and cost savings.

DESIGN

Recommend relevant technologies and services, document technical architecture, deployment plans, "measures of success," budgets and timelines.

MANAGE

Proactively monitor systems to ensure technology is running as intended and provide support when and how you need it.

DEPLOY

Assist with product fulfillment, configuration, broad-scale implementation, integration and training.

Put your security to the test — request a free security scan at CDW.com/threatcheck or contact your CDW Healthcare account manager at 800.500.4239.

Explore Our Featured Partners:

COFENSE SOPHOS tigerconnect TREND MICRO

Visit CDW.com/healthcare or call your CDW Healthcare account manager at 800.500.4239.

CDW PEOPLE WHO GET IT HEALTHCARE