Laura Ramos Hegwer

managing cybersecurity threats

Healthcare organizations' vulnerability to cyberattacks makes it critically important that finance leaders take action to protect data privacy and security.

In 2016, several health systems faced seven-figure settlements because of potential HIPAA violations. The largest involved Downers Grove, Ill.-based Advocate Health Care, which agreed to settle with the Office for Civil Rights (OCR) for $5.55 million regarding three data breaches at its medical group in 2013, which compromised the protected health information of approximately 4 million people. The breaches resulted from four stolen desktop computers, a stolen laptop, and an issue with a business associate, according to the OCR resolution agreement.

While many breaches continue to result from lost or stolen devices—as well as simple employee negligence—other threats to data privacy and security have surfaced. Recently, the industry has seen an increase in "ransomware" attacks that restrict access to IT systems until money is paid, including the March 2016 attack on MedStar Health in Columbia, Md., which crippled the health system for days. In fact, a recent benchmark survey conducted by the Ponemon Institute and sponsored by ID Experts found that criminal attacks have surpassed employee negligence as the No. 1 cause of data breaches.

These types of breaches can have a significant financial impact on physician practices, hospitals, health systems, and health plans. The average cost of a data breach to a healthcare organization is more than $2.2 million, according to the Ponemon report.

Current Cybersecurity Threats

Over the next 12 months, keeping data safe will remain a challenge for healthcare organizations, says Douglas B. Fridsma, MD, PhD, FACP, FACMI,

AT A GLANCE

- Managing cybersecurity has become a priority for the C-suite.
- An enterprise risk management strategy should include proper privacy and security governance.
- Ongoing employee education on "cyberhygiene" is critical to help prevent data breaches.

Douglas B. Fridsma, MD, PhD, FACP, FACMI, is president and CEO, American Medical Informatics Association, Bethesda, Md.

Photo: American Medical Informatics Association

president and CEO, American Medical Informatics Association, Bethesda, Md.

"The problem is that many thieves now view health data as more valuable than financial data because it includes so much more information that can be potentially damaging," Fridsma says.

Complicating matters is the fact that a healthcare data breach can be much more difficult to remedy than a financial breach, such as a false credit card charge. "It is easy for a financial company to make someone whole after a potential breach," Fridsma says. "However, it is more challenging in the healthcare environment if sensitive health information is released or becomes public. Once that information is known, you cannot fix it."

Threats to data privacy and security are rising at a time when healthcare organizations are collecting a wider range of information on patients, adopting population health management strategies, and moving to new payment models. "As we start to move into shared-risk models, organizations want to have more detailed information so they can manage risk and target those patients who might benefit most from interventions," Fridsma says. "That data may include not only financial and health information, but social information as well, such as where someone lives or their socio-economic status. You add all those things together, and you start to get a very clear picture of who that person is. Such data could be very damaging if released."

Michael J. McCoy, MD, FACOG, a health IT expert who served as the first chief health information officer for the Office of the National Coordinator for Health Information Technology (ONC), says the value of stolen health records has dropped in recent months because so many have flooded the market. "In early 2016, a record was as much as $75 to $100 dollars on the dark web," he says, referring to an area of the internet not indexed by search engines. Because sites on the dark web have many privacy features, they often are used for illegal activity. "Now, [the price of a health record] is around $40 to $50. . . . They have hacked so many records that there is a surfeit of electronic medical records available, so the price has gone down," McCoy says.

Today's cybercriminals range from the ubiquitous "kid in the basement" hacker to organized crime syndicates and nation states. For example, the California Department of Insurance reported that the hackers behind the 2014 cyberattack on Anthem worked for a foreign government. "Ransomware is cheap and easy to purchase on the dark web or make yourself," says McCoy, who likens the crime to purse snatching. "When a petty criminal does it, it doesn't tend to attract a lot of attention unless the victim is someone highly visible. But if you have organized crime doing it, then that is a different issue." In fact, many recent ransomware attacks have been launched by organized crime, he says.

"Phishing" campaigns also are becoming much more sophisticated, McCoy says. "Spear

Four out of five acute and nonacute care providers have made information security a higher priority, according to the 2016 HIMSS Cybersecurity Survey. Yet many organizations' efforts continue to be obstructed by a lack of financial and human resources to promote cybersecurity.

phishing" strategies use an email that appears to be from an entity that is familiar to the recipient. That entity might be a person (e.g., the organization's CEO) or a company (e.g., a local fast food restaurant). In such attacks, cybercriminals use sophisticated social-engineering strategies to entice recipients to click on files that contain computer viruses like malware and ransomware. "Hackers are doing research and know who the CEO or CFO is in an organization and will spoof an email address that looks legitimate with a file they want people to open," he says.

Preparing for Cyberbattles

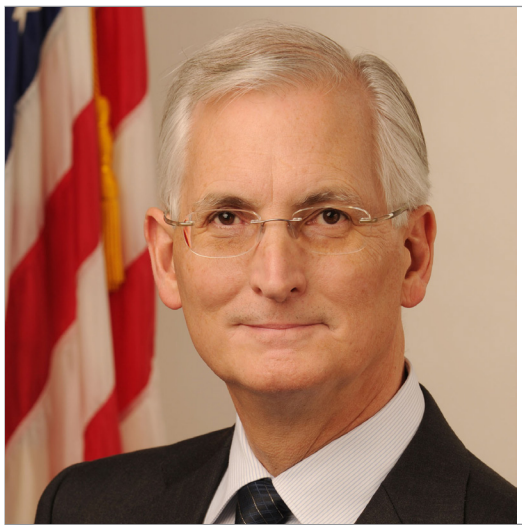
Most healthcare organizations are not adequately prepared to face today's breed of cybersecurity threats, McCoy says. This is especially true for physician practices that do not have the resources to invest in cybersecurity. McCoy also believes that many healthcare organizations, both large and small, do not have the resilience to recover properly from an attack. For example, ransomware can often lurk undetected in an organization's IT system for weeks or months before it activates and starts to do damage.

"If the organization does not have backups that go back far enough, they may not be able to recover," McCoy says. "From a business continuity perspective, that is a major issue for organizations, and the CFO has to be aware that it will cost money for the CIO to do what is needed." Necessary actions might include investing in network monitoring, an off-site data center, and data encryption.

Four out of five acute and nonacute care providers have made information security a higher priority, according to the *2016 HIMSS Cybersecurity Survey*.[a] Yet the survey also notes that many organizations' efforts continue to be obstructed by a lack of financial and human resources to promote cybersecurity.

"If CFOs are not shifting some of their budget toward cybersecurity, what they would pay later is probably a lot more than what they would pay now to beef up their security and education," McCoy

a. "2016 HIMSS Cybersecurity Survey," HIMSS.



Michael J. McCoy, MD, FACOG, a health IT expert who served as the first chief health information officer for the Office of the National Coordinator for Health Information Technology (ONC).

Photo: ONC

William "Buddy" Gillespie, HCISPP, ITILv3, is an HIT consultant based in York, Pa., and former CIO at WellSpan Health.

says, noting that, in addition to costly fines, many small organizations may not be able to afford costly identity-monitoring services for patients whose protected health information and financial data are compromised. "CFOs need to recognize the scope of the threat and the potential financial risk from any kind of breach," he says.

McCoy, who also served as the first chief medical information officer for Catholic Health East, believes C-suite leaders should consider cybersecurity in the same way they think about crisis management for disasters like tornadoes or even scandals. He recommends that organizations develop business continuity plans and consider their insurance coverage. According to the Ponemon Institute benchmark study, one-third

ONC, ASPR Leaders Offer Cybersecurity Advice

"We have seen the scope and number of cyberattacks in the healthcare industry increasing in the past several years," says Steve Curren, director for the Division of Resilience in the Office of the Assistant Secretary for Preparedness and Response (ASPR). "These attacks have the ability to cripple a healthcare organization's operations in a way that is very challenging to prepare for financially."

To help disseminate news on widespread threats to healthcare organizations that do not have the capital to invest in sophisticated monitoring systems, ASPR and Office of the National Coordinator for Health Information Technology (ONC) awarded a grant in late 2016 to support a national information sharing and analysis center.

Curren says his office also has been working collaboratively with healthcare organizations through the Health Care Industry Cybersecurity Task Force, established by the Cybersecurity Information Sharing Act of 2015. The task force includes 17 subject-matter experts from the private sector as well as four government members. The task force has been addressing the industry's level of preparedness and what health care might learn from other industries. "Eventually, they will provide recommendations on how the healthcare industry can better protect itself and what information we can share with healthcare industry partners so they can adopt the best cybersecurity practices and recommend a path forward for HHS [the U.S. Department of Health & Human Services] as we continue to address this issue," Curren says.

Today, more C-suite leaders recognize the vulnerabilities that their organizations face than they did just two years ago, says Lucia Savage, ONC's chief privacy officer. "People are not just looking at the capital required to do this correctly, which of course is a daunting number, but also the implications for their balance sheets when they fail to do it correctly," she says. "In the next few years, we will be getting much better cost estimates as

of healthcare organizations have purchased insurance to cover data breaches. But insurance is not enough on its own. An insurance company could sue a healthcare provider for not having adequate data security procedures, McCoy says. "CFOs need to make sure they have the appropriate reserves and insurance to handle that kind of concern," he says.

CFOs also should engage in serious conversations with the CIO or chief information security officer for the organization so they can allocate capital appropriately. These conversations may prompt the CFO and capital committee to make some difficult choices about funding cybersecurity instead of new equipment or services for the organization.

Developing a Strategy

Finance leaders should work with their IT, risk management, and compliance teams to analyze potential risks to the organization, says William "Buddy" Gillespie, HCISPP, ITILv3, a health IT consultant based in York, Pa., and former CIO at WellSpan Health. He suggests forming an enterprise work group with key leaders from these disciplines who can develop policies and procedures that form the backbone of an enterprise risk management strategy.

One key component of this strategy is proper privacy and security governance to help prevent attacks. Gillespie believes this governance starts at the board level, often in the compliance subcommittee. "Many board members are business owners who are dealing with their own

litigation ripens and organizations make disclosures on their SEC filings if they are publicly traded. That all elevates the conversation into the C-suite."

To prepare for ongoing cybersecurity challenges, Savage suggests healthcare leaders read the HHS resolution agreements on potential HIPAA violations.[a] She says the resolutions and corrective action plans show where organizations make mistakes. For example, many fail to perform more than one risk assessment or fail to follow up on the assessment's recommendations. Others focus their risk assessment on only one aspect of their information systems, such as their electronic health record. Savage also recommends following eight core security preventive techniques, published by the Department of Homeland Security and the Federal Bureau of Investigation.[b]

In September, ONC and OCR published a new security risk assessment tool, available at healthit.gov, especially for small practices and healthcare organizations. "It's a diagnostic tool for providers to identify where they need to make changes in their policies and procedures or their trainings to improve their workforce's preparedness and response to cybersecurity," Savage says.

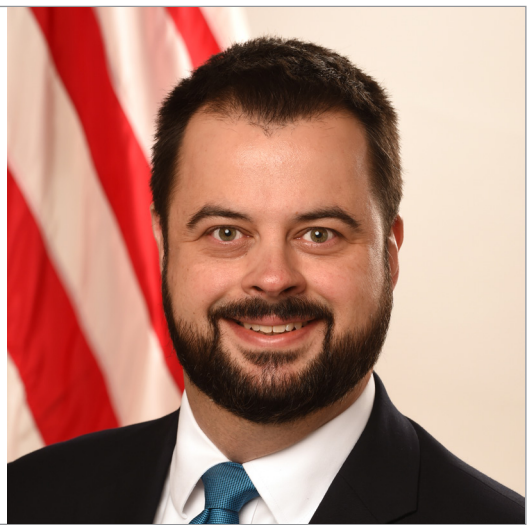
Curren says one of the best strategies to prevent breaches is robust employee education at every affiliate in an organization. "A system is only as strong as its weakest link," he says. "Malicious cyberactors can get in through one [information] system in a smaller organization and perhaps make their way to a bigger organization. So we can't say that there are only certain organizations we need to protect. We really need to protect the whole system, and large organizations may need to assist the smaller organizations to do that."

a. "Resolution Agreements and Civil Money Penalties," U.S. Department of Health & Human Services.
b. "Executive Summary of Grizzly Steppe Findings from Homeland Security Assistant Secretary for Public Affairs Todd Breasseale," U.S. Department of Homeland Security," Dec. 30, 2016.

Simple things like encouraging employees to create strong, unique passwords and disabling unused accounts can help address some of the most common ways that cybercriminals try to breach systems.

cybersecurity threats, so they can relate to the issues," he says. Gillespie recommends that the subcommittee report to the board monthly about potential threats, new regulations, and investments needed for cyber-protection. Cultivating this level of board buy-in can help elevate the importance of privacy and security across the enterprise.

Employee education also is critical to an organization's risk management strategy. During OCR's audits of health systems, the office looks for policies and procedures that give staff the tools they need to prevent and manage breaches, based on the premise that privacy and security are owned by every employee, Gillespie says. He suggests staff members need to be taught not only how to avert potential threats but also how to report potential breaches within the organization—and he recommends conducting such training annually.



Steve Curren, director for the Division of Resilience in the Office of the Assistant Secretary for Preparedness and Response (ASPR) (quoted in the sidebar on pages 36-37).

Photo: ASPR

Lessons Learned

The cybersecurity experts offer the following advice to finance leaders who want to keep their information systems and protected health information secure.

Teach employees about "cyberhygiene." Phishing is one of the greatest threats. Fridsma underscores the need for staff to understand the importance of sound email practices. For example, staff should be directed not to click links in emails from addresses they do not recognize or that require passwords or sensitive information to be entered. Simple things like encouraging employees to create strong, unique passwords and disabling unused accounts also can help address some of the most common ways that cybercriminals try to breach systems.

Encrypt information on laptops and mobile devices to help protect vulnerable data in case first-line defenses like staff education fail. Fridsma says encryption is common in other industries, such as financial services.

Focus on small physician practices. "Large organizations, whether they are health plans or health systems, have much more data, which makes them a more attractive target, but they also have more resources and a more sophisticated

architecture that will allow them to protect that data," Fridsma says. Many small physician practices are especially vulnerable because cybersecurity is simply not part of their culture.

Educate leadership on cybersecurity threats. "Everyone in the C-suite and on the board should understand what is required to meet the modern threat," McCoy says. They also should understand the cost to the organization if they do not invest in the proper defensive strategies.

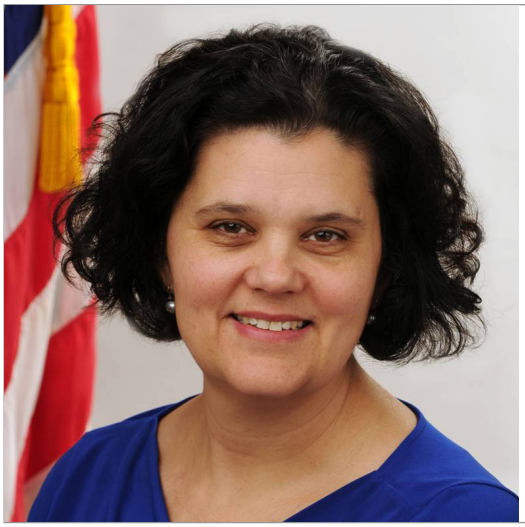
Use test phishing emails to track which employees might be likely to download ransomware or another type of malware virus. McCoy says this strategy can help leaders direct cybersecurity training where it is most needed.

Invest in network monitoring. Such monitoring can help detect the transfer of data to suspicious internet protocol (IP) addresses in places such as Russia, Ukraine, or China, where cyberattacks often originate.

Use two-factor authentication, which grants access only after users provide a password and another piece of information that only the user knows. This practice, common in banking, makes it harder for potential data thieves to sneak behind firewalls, McCoy says.

Regularly update business associate agreements to spell out the privacy and security requirements with third parties. "Third parties are required to be accountable and report any breaches across the chain of trust relative to protected health information," Gillespie says.

Invest in mobile device management software to help mitigate the risk when employees use their own devices at work. Gillespie says 80 percent of hospitals allow employees to bring their own device into the hospital setting to access data.



Lucia Savage, chief privacy officer for the Office of the National Coordinator for Health Information Technology (ONC) (quoted in the sidebar on pages 36-37).

Photo: ONC

Be ready to respond. Every healthcare organization should have a team that can jump into action and assess the damage when a potential breach occurs, Gillespie says. The team can provide the required notification to OCR and distill lessons from breaches to prevent future occurrences.

The Persistence of Risk

Finance leaders should recognize that there are no absolutes when it comes to securing data. In the words of Fridsma: "You're never going to be able to totally lock down these systems." Nonetheless, a risk management strategy can effectively reduce the greatest vulnerabilities, and such a strategy remains the best approach to making a healthcare organization more secure. ■

About the authors

Laura Ramos Hegwer is a freelance writer and editor based in Lake Bluff, Ill., and a member of HFMA's First Illinois Chapter (laura@vitalcomgroup.com).