Fighting Cyber Crime
How healthcare organizations can stay safe
A Growing Threat

You hear it in the news and at industry gatherings: Healthcare organizations have become more serious and frequent targets of fraudsters and cybercriminals.

At Bank of America, we are committed to helping our clients understand the importance of fraud prevention. We want executives to understand the risks and to take precautions to protect their patients, employees and communities.

We understand what’s at stake. Like your organization, our company can only operate successfully if we maintain the trust of the public. Like you, we have a responsibility to the communities and clients we serve, to protect them and their information. It’s a precious public trust that can be broken quickly; as many organizations have found, cyber crime puts everyone’s reputation at risk. In addition, of course, a dollar lost to fraud at a hospital is a dollar lost to helping your community.

The first step in fraud prevention is education. Administrators must stay on top of the latest scams and fraud threats, and establish a framework to regularly communicate that information to staff members.

Our team has an ear to the ground; we share what we learn, both from others in your area and from clients around the world, in materials like this report. And offer solutions that can help protect your organization and help you combat fraud when it occurs.
Health Check

Why your organization may be vulnerable to cyber crime

Cyber crime is on the rise across industries and around the globe. The numbers are staggering. The FBI estimates that businesses have lost more than $5.3 billion to email fraud over the past five years. In 2017 alone, $5 billion was lost to criminals holding corporate systems hostage with ransomware—a tactic that’s grown exponentially, according to Cybersecurity Ventures estimates. And hackers were busy in 2017, perpetrating data breaches that exposed more than 3 billion personal information records, 6 billion email accounts and more than 2 billion Facebook accounts.

Cyber crime damage in 2017*

- 6 billion email accounts hacked
- $5 billion in ransomware losses
- 3 billion personal records exposed
- 2 billion Facebook accounts compromised

*cybersecurityventures.com
It used to be that healthcare wasn’t really part of the discussion. “Until recently, cybersecurity was just not a topic that was extensively discussed in healthcare,” says Lynn Wiatrowski, National Treasury Executive at Bank of America. “Healthcare organizations were able to keep their clinical focus, emphasizing medical innovation, patient safety and avoiding errors.”

But in the face of rapid industry consolidation and technical evolution, healthcare organizations have become uniquely vulnerable to cyberthreats. There is also increased awareness of the high value of healthcare data. “With increasing scale and complexity, the industry has become a target for fraud, and now finds itself having to deal with cybersecurity issues,” Wiatrowski says.

The risks are multifaceted. “If you don’t have the proper protections in place, that lack of security can really damage people’s trust, and your reputation as a provider,” says Charles Alston, Market Executive at Bank of America.

With the use of electronic records, online portals and connected devices all on the rise, healthcare finds itself going digital later than other industries — and unfortunately at a time when cyber crime is at an all-time high, says Mary Rosendahl, Director of Global Digital Channels, Fraud Education & Risk Management for Global Transaction Services at Bank of America.

---

### Three fraud types

Healthcare organizations face the sorts of universal cyber crime seen by all businesses.

1. **Unauthorized access of treasury info**

   Criminals will try to gain access to an organization’s treasury or employees’ financial information. They hope to trick the system into sending a check or ACH payment for a non-existent transaction, or persuade an employee into wiring a payment to a fraudulent bank account.

2. **Malware/ransomware installed**

   Criminals will try to install malware — software designed to damage or disable a computer system — onto an organization’s computer network, demanding a ransom in order to restore the system and its data to normal operations.

3. **Theft of personal info**

   Hackers will attempt to break into an organization’s database of information to steal the personal, medical or financial information of patients and employees.

---

Per BofAML’s Mary Rosendahl, 90% of these fraud attempts come through phishing* e-mails directed at an organization’s weakest link: its users, who often are unaware and unprepared. One click on a PDF or an internet link, or a reply to a fraudster’s email address, can open the door to these criminals.

---

*Cofense
Unique vulnerabilities

Although the types of attempted fraud are universal, unique aspects of the industry leave healthcare organizations more exposed.

Hospitals have become a key target because the types of data housed in healthcare ecosystems—from patient and employee records, to the information used to access corporate bank accounts and insurance monies—have become valuable commodities on the black market.

“Think about what is contained in a healthcare record; for instance. Compared to what a credit card is worth, what it sells for on the black market, your healthcare history is much more valuable to a fraudster,” Rosendahl says. “A stolen credit card will be noticed right away and be turned off immediately. The information in a medical record can be used for a long time, for a whole slew of different types of fraud”—obtaining medical services, prescription drugs and medical devices as well as the usual identity theft used to open credit accounts.

The complicated way medical bills are paid—often involving a back-and-forth between provider, insurer and patient—creates a time lag that can provide cover for criminal activities. It’s not unusual for a patient to receive a medical bill months after the services were rendered. At that point, fraudsters have ample opportunity to make off with stolen goods and services. In addition, healthcare’s central mission—protecting patients’ lives—makes medical facilities vulnerable to any criminal threat, such as ransomware, that might shut down potentially life-saving equipment or access to medical records.

Structural issues often make healthcare organizations particularly susceptible to cyber crime. For instance, data is often vulnerable, because healthcare organizations traditionally have data distributed in many places, often in department silos where it’s neither effectively shared nor jointly protected. Organizations don’t always have a cybersecurity chief in place, and often haven’t established solid policies to protect computer systems and data.

Consolidation risk factors

Consolidation has been both a plus and a problem. Mergers, acquisitions and partnerships mean ever-larger networks of medical facilities and offices working with many third parties, such as doctors’ offices, labs and insurance companies. On the plus side, larger healthcare systems often have established vendor policies, more extensive information system procedures and even cybersecurity officers, and can conduct due diligence of partners and vendors as part of a management agreement.

But there can also be drawbacks. “The scale is tremendous,” says Alston. “If you are bringing together 20-25 hospitals, there are so many disparate points of entry to the system: for patient care data, for collection and billing, for all the different medical providers and alliances. Each hospital may be working on its own legacy system. Organizations are working hard to integrate their operations, and make sure that the quality of care is integrated. But in the meantime, there are so many potential electronic openings for fraud to occur. It’s something that makes healthcare CEOs and directors lose sleep at night.”

90% of fraud attempts come through phishing emails directed at the weakest link: employees*

*Cofense
Healthcare industry trends have opened other potential windows for criminal attacks. Wiatrowski points out that the industry has worked hard to move from its historically fragmented nature to a more patient-centric model, which often means sharing patient information between a host of providers. However, an entire network of healthcare entities sharing information is only as protected as its weakest link.

**Holistic data and connected devices**

“Holistic data management is an aspiration,” Wiatrowski says. “The more that can be done to bring together data management under a single umbrella, the better. It can help in efficiencies, cost savings, and can provide structure to protect against data attacks.”

In addition, the industry has embraced innovation and new technology. “The pace of innovation is seen with a plethora of new devices being brought into the hospital for better care and better clinical outcomes,” Wiatrowski says. “But often it also makes it more difficult for the tech and IT departments to manage data security.”

The average number of devices connected to a hospital bed is 15, according to research presented at a recent conference by Mayo Clinic executives — who estimate that more than 7,000 different companies are producing items for the “internet of medical devices.” Connected devices such as imaging systems and infusion pumps can provide criminals with inadvertent entry points into a hospital’s computer systems, according to a recent analysis by ZingBox, because security often is not a priority for device manufacturers.

**The bottom line**

The bottom line is that 77% of U.S. healthcare organizations now report having experienced a data breach — and 48% of organizations say they have been breached in the past year, according to a 2018 analysis by Thales Security.

“Healthcare has become a huge target for what’s become a sophisticated black market. These breaches not only pose brand and reputational risk, but in a worst-case scenario, can directly impact patient care,” Wiatrowski says. “The bar is going to continue to be raised for what’s demanded from healthcare providers and those who partner with them.”

**Measuring the threat to healthcare organizations**

- 77% have been breached to date
- 48% were breached in the past year
The Scene of the Crime

Where and how healthcare fraud happens

What does cyber crime look like for a hospital or a healthcare group? Where does it happen, and how can organizations protect themselves? As you assess the security of your organization, here are top trends, emerging threats and things to consider.

1

Don’t forget the basics

As complicated as cyber crime may seem, don’t forget the basics. The scariest headlines for healthcare executives are about fraudsters using ransomware to shut down a system, as happened to the UK’s National Health Service in 2017. But a breach doesn’t require sophistication. “A lot of cyber crime continues to be perpetrated via good old-fashioned phishing techniques,” says Alston. “Fraudsters send an email that gets them into an organization. Then employees, oftentimes even though thoroughly trained, can make an error in judgment by clicking on a link or responding to a fraudulent email. That one action ends up pulling a thread that creates a system wide problem.”

Different types of phishing emails have different goals: installing malware, accessing data or locating an uninformed employee who can serve as an unwitting accomplice. But the primary task is to get access inside an organization. In one example, a company might receive an email message from a purported “vendor.” The message indicates the vendor is updating or changing its bank account and asks the healthcare organization to change the information in its payment system. Looking closely, there usually are clear signs of fraud, such as an inaccurate email address or phone number. But if an employee doesn’t catch those mistakes, and changes the vendor information in the system, payments can be sent to fraudsters’ bank accounts. The organization suffers a double loss; not only is the money lost to the fraud, but the actual vendor still needs to be paid.

In 2017, ransomware shut down the UK’s National Health Service
Watch for wire fraud

In addition to straightforward check and ACH fraud, “Healthcare is just as susceptible as any other business to wirefraud,” Alston says. In a wirefraud, the fraudster sends an email to a treasury employee that appears to be from a top-level executive in the organization; often it will be sophisticated enough to mimic the executive’s writing style, or arrive when the exec is at a conference or on vacation, and hard to reach. The message asks the recipient to wire funds to an account — again, presenting it as an emergency or time-sensitive situation. The recipient is reluctant to turn down the request, since it’s coming from management. “People ask, ‘Why would a controller or treasury employee respond to an email like that?’” Alston says. “Well, it appears legitimate, and it’s a rare event; no one has likely seen something like that before. And once that transfer is executed, the money is gone, because employees hadn’t been trained, or regularly reminded about such types of fraud, and there wasn’t a process in place to handle such situations. These are the situations that training can help avoid.”

Monitor for ransomware

Criminals’ use of ransomware is a threat that organizations should consider carefully, and will handle best if well prepared. One of the most effective preparation tools is a tabletop exercise that can walk the organization through a simulated ransomware event. Doing a simulation can help answer the key questions: Would we be able to identify a situation and stop it? Would we be able to trace where it came from? Do we have all the right disciplines at the table? What kind of communications do we need to let people know what’s happening? Can we get the system back up? Many executives may be tempted to invest in cryptocurrency like Bitcoin, so they’re able to quickly pay in the event of a ransom demand, but should carefully consider whether paying a ransom is the best solution.

Wiatrowski suggests that healthcare providers, who often train for emergency medical events and natural disasters, can apply those learnings to handle a cyber crime event. “Hospitals are second to none in preparing to care for patients in emergencies. Healthcare organizations can take those approaches developed in crisis training, and learn from that. They can apply those disciplines and rigors if a cyber breach occurs,” she says.

Tighten provider-insurer connections

The connections between healthcare providers and insurance companies can create cracks where cyber crime can flourish. “The structure of health insurance involves a lot of transactions and a slow process, a complicated architecture. And there is a lot of money fueling the system,” says Roger Boucher, Market Executive at Bank of America. “The process of reimbursement creates a back and forth interaction that the patient never sees; it can be weeks or months of submission, denial, resubmission, correction, denial (again), before the bills are processed. That lag creates a vulnerability. With so much data traveling back and forth, and such delays in payment, crooks find a way to insert themselves in the gap.” He says healthcare providers need to assess, and continually re-assess, the reimbursement process to double check that insurance companies are sending payments to the correct entity.
5  Protect patient data

Patient data needs to be protected in as many ways as possible. Not only do healthcare providers need to be cognizant of patient privacy and HIPAA rules, they need to continually remind themselves that patient data is currency for criminals. As patient records are migrated from paper to digital forms, organizations need to be vigilant in keeping track of older records and how they are handled, stored or disposed of. Policies need to be in place to ensure safety, for instance, when employees handle patient data while working at home.

Similarly, to keep records safe and up to date, providers need to regularly back up the data contained in their computer systems. Organizations will complain that backing up the database for the entire system is too time-consuming, or creates too much downtime. A solution is to break the data into smaller pieces, backing up a department or a piece at a time.

6  Keep tabs on third-parties

Whether it’s insurance companies, labs, doctors’ offices or other partners, an organization is only as protected as the third parties it works with and shares its computer connections and its data with. “A healthcare organization should be asking, ‘Where is all my data going, and who is keeping an eye on it?’” Boucher says.

A strong vendor management program should include regularly checking the data protection policies and cybersecurity procedures of vendors, third-party services and strategic partners to make sure everyone is on the same page. “When contracts are reviewed, there should be an opportunity to build on a security element as well as outline liability of loss, if those items do not already exist,” Alston says.

Healthcare organizations can be unpleasantly surprised by the manner in which partners handle things like data breaches. For instance, some third parties’ software can include a mechanism that responds to an internal data breach by shutting down not just the vendor’s system, but the entire hospital system’s computer network. “The items that make a company a good healthcare partner might not mean it’s a good security partner,” says Rosendahl.

7  Secure new equipment

The industry has been buzzing about how new products in the internet of things and medical devices are offering new entry points into a healthcare system. “When a hospital is introducing the newest, most sophisticated piece of medical equipment, thoughts are on the difference this new technology will make in patients’ lives, rather than considering that the new technology may also be introducing a cyberthreat,” Wiatrowski says. “It is not second nature to think about who is on the other end of those pieces of equipment, and what entry points may be introduced.”

When you think about securing your organization, think about all the assets that are accessing your company, Rosendahl says. “That used to be computers and mobile phones. Now it’s expanding to the internet of things, whether that’s a printer connected to the internet, a thermostat, digital imaging systems or the huge variety of medical devices available for patient care,” she says. “Each of those devices has software that needs to be kept updated to remain secure.” Check into the design of these new devices and the built-in governing security protocols.

8  Stay alert for new threats

Finally, remember that the threat environment will continue to evolve. “Bad actors will continue to find new ways to attack,” Rosendahl says. Stay updated on the newest forms of cyberattacks by reading trade publications, attending conferences and webinars to share information with your peers, and comparing notes with your own strategic partners about what they are seeing.

Says Alston, “There is a lot more ground to protect if you are in a healthcare organization, and a lot more opportunity for fraud to occur. And it’s hard to stop something if you have never seen it before. That’s why ongoing education and training are so important.”
Protect your data
- Develop a data storage plan and policies for data retention, privacy and disposal that extend across your entire organization
- Be wary of any requests for information on patients or employees
- Regularly back up digital information and data, and check to see that departments with their own databases and information collections are similarly performing backups

Keep your systems safe and up to date
- Install firewalls and limit employee internet access while on the system
- Create a software management plan including checking for software updates, updating antivirus software, and installing software patches on a regular or as-needed basis

Arm your employees to recognize and handle potential fraud
- Conduct employee training on cyber crime, including how to recognize a phishing email and understanding the potential consequences of opening and clicking on one
- Teach employees how to protect the organization with smart password management
- Test your staff on a regular basis by sending out fake phishing emails
- Share news of new types of threats and also good news when fraud attempts are successfully quashed

Create policies to support cybersecurity
- Establish data protection policies for employees working off site or at home — policies for using data and also for disposing of any information
- Institute a clear policy for professionals bringing their own devices — tablets, phones, laptops — into a facility, and especially when they use those devices to access patient or hospital data
- Make two approvals a requirement for any significant financial transaction, including initiating payments, changing vendor information and creating user accounts

Be prepared for a fraud event
- Construct a plan to deal with fraud events, ransomware and other situations that affect data and potentially freeze the system
- Conduct tabletop exercises that simulate a cybercrisis, and evaluate the results. Apply appropriate lessons from emergency medical preparedness

Stay informed
- Keep updated on the newest types of cyberthreats and criminal activity by reading trade publications and business news
- Keep in touch with partners, like Bank of America, who have a global view of fraud across markets and industries
- Attend webinars and roundtables
- Share information with your peers