# Hacked! What to Do Following a Cyberattack



By Mary Butler

Steve Giles, chief information officer (CIO) at Hollywood Presbyterian Medical Center, says the experience of his organization's 2016 high-profile ransomware attack was among the top three most terrible events he has lived through in his professional and personal life. Hospital officials started to notice that access was blocked to certain servers at 6:30 p.m. on a Friday, so they immediately implemented their downtime procedures as well as internal triage processes. The following morning a ransom message appeared on Hollywood Presbyterian's computer terminals, prompting Giles and his colleagues to contact the cyber unit of the Los Angeles Police Department. However, since it was a weekend, the cyber unit put off their own response until Monday, as did the local Federal Bureau of Investigation (FBI) office. Giles and the hospital staff were on their own for the weekend.

Because ransomware attacks were thought to be rare events in early 2016, there were few industry best practices for Giles to follow—such as not paying the ransom, enacting a specific ransomware incident response plan, or, if worse comes to worst, knowing exactly how to obtain Bitcoin. With no law enforcement help coming in the near future and the fear growing that waiting could lead to increased patient risk, Hollywood Presbyterian ended up paying the $17,000 ransom in Bitcoin. At the time many experts and some in law enforcement typically recommended paying the ransom just to ensure retrieval of vital data like health records—but it is a practice that security experts now advise against.

According to Clyde Hewitt, MS, CISSP, CHS, executive advisor at CynergisTek, organizations that pay a ransom are 75 percent more likely to experience another attack. If word gets out in the press that a ransom was paid, or if the hackers brag to their friends about their exploits, hospitals find themselves targeted again. Giles says that in the wake of Hollywood Presbyterian's attack, the volume of phishing emails and other attempted hacks tripled.

Fortunately, the medical center had monthly downtime periods when security updates are pushed out, which gave the staff practice with quickly transitioning to paper-based processes such as charting and registering new patients. However, the attack shut down the payroll system, which added a layer of stress because of California's strict regulations about paying hospital employees on time. So, in addition to addressing systems related to patient care, getting payroll back online was a priority. Lab systems, pharmacy systems, and electronic health records (EHRs) stayed operational during the attack.

"Our saving grace was that our backups were still on tape," Giles says. "They were then and they are still. And as a result the malware could not reach them. I've taken calls from other hospitals that had their backups on a disc drive technology that were also networked with the rest of the system and they got attacked too."

Giles now gives talks at conferences around the country about what it's like to survive a ransomware attack so that others can learn from the experience and know what to expect. The fact is, many organizations—and, specifically, health information management (HIM) professionals—don't know how to prepare for or react to a cyberattack.

Privacy and security officers, health IT workers, and HIM professionals must be on the frontlines of healthcare organizations trying to thwart and mitigate cyberattacks that are increasingly coming from every direction. They can come from nation state actors—North Korea is believed to be behind the WannaCry ransomware attack; Russia is the suspected source of the mock ransomware virus NotPetya (in fact, insurance companies that sell cyber insurance policies have at times refused to pay out because cyberattacks are considered "an act of war").

And in other less-publicized incidents, which can be equally as damaging, cyberattacks can come from within an organization through current or former employees, or hospital visitors looking to disrupt Wi-Fi networks. In most industries targeted by cyberattackers, the biggest risk is financial. In healthcare, cyberattacks can take down EHRs, cardiac cath labs, CT scanners, lab systems, heart monitors, ventilators, and even hospital beds. Experts predict that cyberattacks against healthcare organizations are only going to increase as hackers exploit this vulnerability and increase their profits by selling stolen data.

According to a survey from the Department of Health and Human Services (HHS) and the Healthcare and Public Health Sector Coordinating Councils, which got its numbers from IBM and the Ponemon Institute, the cost of a data breach for healthcare organizations rose from $380 per breached record in 2017 to $408 per record in 2018. Across all industries, healthcare has the highest cost for data breaches;[1] while cost per record is $408 in healthcare, it is only $166 per education industry record.

While incident response plans at many healthcare organizations are led by IT and information systems staff, HIM can play a huge role in protecting patient information during and after an attack. Contingency plans for unexpected EHR system downtime can help mitigate the impact of a cybersecurity attack from an HIM standpoint—but as many healthcare facilities have found, even the best-made preparation plans can't account for every scenario. There are, however, best practices for preparing for, responding to, and recovering from attacks that can help set you up for success in the event of a cyberattack.

### Cybersecurity Definitions

- **Breach:** A breach is, generally, an impermissible use or disclosure under the HIPAA Privacy Rule that compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual.
- **Cybersecurity:** Broad term referring to the practice of keeping computers and electronic information safe and secure.
- **Malware:** Malicious software that is designed to damage or do other unwanted actions to another unsuspecting computer.
- **Phishing:** A type of cyberattack used to trick individuals into divulging sensitive information via electronic communication by impersonating a trustworthy source. For example, an individual may receive an email or text message informing the individual that their password may have been hacked. The phishing email or text then instructs the individual to click on a link to reset their password.
- **Ransomware:** A type of malware distinct from other malware; its defining characteristic is that it attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid. After the user's data is encrypted, the ransomware directs the user to pay the ransom to the hacker (usually in a cryptocurrency, such as Bitcoin) in order to receive a decryption key.

Sources: Department of Health and Human Services Office for Civil Rights: www.hhs.gov/sites/default/files/cybersecurity-newsletter-february-2018.pdf; Office of the National Coordinator for Health IT: www.healthit.gov/sites/default/files/cybersecure/downloads/Cybersecurity_Glossary.pdf

## Prepare for the Worst, Expect the Best

Now that ransomware and other cyberattacks—including malware and viruses—are in the news constantly, provider organizations and their vendors would be foolish to continue ignoring the problem. Ty Greenhalgh, HCISPP, managing principal and founder of Cyber Tygr, says it's much harder to adequately respond to a cyberattack without having prepared for one. A good place to start, he says, is the HHS and Healthcare and Public Health Sector Coordinating Councils' document "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients,"[2] which HIM professionals can use to help formulate an incident response plan. He thinks most providers are wholly unprepared for what they could be facing.

"They think they're prepared and they have some paper prescription pads, different things they might need in a paper environment. But they underestimate the length of time they will be down and so really it falls back to an incident response plan. A good incident response plan is going to prepare you and detail what you and what each department in the organization should do," Greenhalgh says.

"What do [incident response] teams look like? Whose got what, who's talking to the media, what are we saying? Someone has to decide if prescriptions should be written out. Someone needs to know how to get Bitcoin—going out and getting Bitcoin after the breach is not a good strategy. So more detail you can get in that plan the better."

Ed Brown, director of IT systems at CaroMont Health in Gastonia, North Carolina, had one of the best probable outcomes when his hospital was struck with a WannaCry attack in July 2018, which he describes as a "minimal breach." The WannaCry virus infiltrated CaroMont's system through a laptop that didn't belong to the hospital, and it was minimal in scale because it only affected the organization's mobile thin devices. A mobile thin device looks like a laptop but doesn't have a full hard drive, so in essence it's an "over-glorified monitor," Brown says.

"Once we cornered it [the WannaCry malware] we were able to restore the network back to almost normal operating. So for example, some of our nursing units were able to continue to chart, some of our other units had no issues. We had a phone system that operates across the internet, across our data network that was not impacted. From the time we got a call from our security monitoring service to the time we verified that the last mobile thin device was back to normal and WannaCry was eradicated from our system, we were back up in 56 hours," Brown says.

Brown's department benefited from a lot of work in advance of the attack. He had been working with cybersecurity experts on contingency plans for two to three years and contracted with a security monitoring vendor that kept an eye out for unusual activity on hospital servers and networks. Additionally, every server and work station were up to date with security patches.

Nuance Communications, a vendor that provides speech recognition, transcription, and other digital services—along with global shipping giant FedEx, Maersk, GE, Verizon, and many other major companies—were not as lucky when they were sidelined by the NotPetya malware on June 27, 2017. The goal of NotPetya was not to steal data but to cause disruption. Joe Petro, executive vice president and chief technology officer at Nuance, said that on the first day NotPetya hit he started to receive alarming text messages from colleagues at 7:15 a.m.

Michael Clark, senior vice president, general manager, provider solutions at Nuance, says, "At the beginning, law enforcement didn't know if the attack was malware, ransomware, or another type of virus. They also didn't know if there would be 'another wave' or another phase of the attack." Because of the uncertainty, a major decision was made to cut transcription connections to outside entities.

As a result of the protective measures, HIM departments had to enable dictation and get all the data plugged into their own EHRs. This struck at the heart of HIM in many healthcare facilities that used Nuance for services. Fortunately, no personal health information was compromised—but that hardly stopped it from being disruptive.

"One way to think about it is HIM professionals are responsible for documentation and systems. We in essence provide a transcription dial tone, and when that dial tone went down, it put the HIM departments under pressure," Petro says. "Clinicians in clinical areas and executives in institutions turned to HIM and asked, 'How are you going to fix this?'"

Petro says that in our personal and professional lives, we assume that when systems go down, they'll come right back up, since 99 percent of the time they do. However, the reality of cybercrime is that it can deliver weeks of disruption.

"One thing we all need to contemplate in HIM, as well as software vendors, is preparing for something that's worse than we could have imagined ahead of time. Even if something has a low probability of happening, really think through the details and prepare for that," Petro says.

### TV vs. Reality: 'Anatomy' of a Ransomware Attack

Every bed in the trauma center's emergency department is filled with patients that are sick but stable. Suddenly, the heart monitors at the side of each bed start beeping, seeming to suggest that each patient is crashing. On a medical-surgical floor elsewhere in the hospital, an attending physician can't get into her patient's electronic health record (EHR), and another physician's iPad chart is malfunctioning outside a critical patient's room. Then a frozen computer issues a message asking for $20 million in Bitcoin in exchange for an encryption key.

This isn't a summary of the latest high-profile healthcare ransomware attack, but a recent plot on the long-running medical drama *Grey's Anatomy*. CynergisTek's Executive Advisor Clyde Hewitt, MS, CISSP, CHS, actually uses parts of this cliffhanger episode when he does cybersecurity training because he says the show provides useful information for real-life healthcare providers within the somewhat fantastical plot.

"The possibility of everything happening was 100 percent, but the probability of all of it happening at the same hospital at the same time is almost impossible," Hewitt says. "But everything that happened in that episode is a serious real probability of causing harm to that hospital."

Hewitt credits the relative accuracy of the episode with the fact that a chief information officer from a hospital that had recently been attacked had a relative that worked at ABC (the network that broadcasts *Grey's Anatomy*) and was able to provide real details to the writing staff.

The show did pack a lot of cyberattack symptoms into its two-part episode. For example:

- Hackers crept into the thermostat and ratcheted the hospital's temperature up to 90 degrees
- The keypad allowing doctors into the hospital's blood bank was locked
- All of the equipment in the laboratory went down
- A surgeon was forced to do an open procedure instead of a laparoscopic one because the camera on the device stopped working

The episode did a believable job conveying the terror healthcare practitioners experience when a cyberthreat strikes a healthcare organization's infrastructure. For example, the doctors in the episode considered paying the $20 million ransom—a tactic that the FBI and cybersecurity experts always advise against. In the real world, ransoms are usually more affordable since it makes victims more likely to be able to pay. When Hollywood Presbyterian Medical Center was hit with ransomware, hackers demanded $17,000. Hackers are taking advantage of the very real fear of harm—and the sense that anything can happen.

Joe Petro, executive vice president and chief technology officer at Nuance Communications, said that in the wake of his company's ransomware attack, his thinking about these ongoing threats has evolved.

"In these situations, you have to take the fractional probability [of an event like this], multiply it by gigantic risk, and that's what should drive your behavior on a day to day basis," Petro says. "If someone had described [our attack] to us the day before it happened, we would've said, 'That's insane, it'll never happen as long as we're alive,' and it did. And that's the crazy part."

But the *Grey's Anatomy* story line wasn't completely accurate. One of Hewitt's qualms with the episode was the speed with which the FBI stormed the hospital with laptops and gear. While he has FBI agents on speed dial, Hewitt says they never arrive as quickly as on the show. Hewitt also took issue with how easily the characters in the show ended the attack. As skeptical viewers might expect, it's unlikely that a surgical resident would be able to decrypt the encryption key before the FBI could.

## Formulating an Action Plan

It's important that healthcare providers and HIM professionals be prepared, but also understand that absolutely no one is immune from cybercrime, and even the most prepared vendors and business associates can get hit. In many ways, it's not all that different from having a downtime plan in response to natural disasters like hurricanes and tornadoes. Clark says Nuance's clients were very helpful and understanding. But every client they talked to wanted to know how to better put up their defenses. The vendor-provider relationship became much more collaborative after the breach, he says.

And once HIM gets a true sense of the realities and the risk involved with modern-day cybercrimes, they may need to work with IT and information systems teams to convince organizational leadership that protecting against cyberthreats should get priority status. In addition to having downtime plans, there should also be comprehensive cyber hygiene training for the entire workforce. One strategy that experts recommend is simulating phishing attempts to test how many employees still don't know the warning signs of suspicious emails.

"You stress test the system and then you can bring that back as evidence that you have to train, etc. Making it real is a bit of an art form. Back it up with science and evidence. We reoriented but in this day-and-age of sophisticated cybercrime it's not so easy out there if you haven't been through it," Petro warns.

In a perfect world, providers and vendors should already be working with security firms before a breach event, like Brown was doing at CaroMont.

"Ideally, people should call us way before a breach," Greenhalgh says. "Most of the clients we work with… everybody has different needs, different resources, but [typically we] go in and help with infrastructure, awareness training programs, and doing monitoring for them."

Another thing HIM and privacy officers should keep in mind is that breach events need to be reported to HHS's Office for Civil Rights within 60 days of an attack, and Greenhalgh notes that's not a lot of time in the grand scheme of things.

"A lot of our clients put in place a retainer for a forensics team and a breach team [prior to an attack]. Then reconnaissance work can be done, and they understand the environment—there's boots on the ground immediately. Basically the faster you can respond, the less impact a breach is going to have," Greenhalgh says.

HIM will also play a big role in converting any downtime documentation from a paper state to a digital state when EHRs are reactivated after a breach. CynergisTek's Hewitt recalls one breach where a system's EHR was down for two weeks. When it went back up, HIM staff were greeted with enormous stacks of paper records that needed to be entered into the EHR. During that two-week downtime period at a 600-bed hospital, no claims were sent to payers, and within two weeks they lost $60 million in cash flow. In approximately three months they recovered about half of that.

"So one of the things HIM needs to look at is they have to make payroll and they have to pay bills, and all of a sudden they don't have cash to do it. Second, any projects they thought were priority—for the next six months or year, they can just put those on the shelf. All resources should be going into fixing the problems that allow the ransomware to take place the first time. They have to fix security holes, and every spare dime should be spent on fixing security and privacy, or patient notification, or outside attorneys or OCR fees," Hewitt says.

One unexpected aspect of Hollywood Presbyterian's attack was that once they paid the ransom, the hackers sent them well over 900 different decryption codes that had to be meticulously matched to each and every impacted computer terminal in the medical center.

"So we had to apply decryption codes very, very carefully and very specifically to the right server, because if we didn't the warning said using the wrong encryption key could strip the server of all data. So we were very, very careful in terms of all of our servers," Giles says.

Giles says he learned that there's no absolute, secure capability an organization can have that will keep you safe. "I think you really have to understand that your whole goal in keeping safe is minimizing the potential of it happening again. But you can't eliminate every possibility."

## Notes

1. US Department of Health and Human Services and Healthcare and Public Health Sector Coordinating Councils. "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients." www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf.
2. Ibid.

Mary Butler (mary.butler@ahima.org) is associate editor at the *Journal of AHIMA.*

**Article citation**:
Butler, Mary. "Hacked! What to Do Following a Cyberattack." *Journal of AHIMA* 90, no. 4 (April 2019): 12-17

Driving the Power of Knowledge