Putting Out A Cyber Fire: 7 Rules For Hospitals

Law360, New York (July 15, 2016, 11:07 AM ET) --

Daniel B. Garrie Richard M. Borden

Richard M. Borden

Health care today is facing a deluge of cyberthreats from internal and external actors without any meaningful assistance from the government. This is much different than most dangers confronting a health care institution. While health care institutions face a multitude of cyberthreats, ransomware is certainly one of the most troubling.

It is not clear why preparing for and responding to cyberthreats is different from other risks faced by institutions. For example, a hospital today has multiple protocols, processes and systems in place to address fire safety — mandated by government and legal system. Moreover, health care entities can count on, in most situations, the local fire department to respond with meaningful resources in the event of a fire, and that law enforcement will conduct a fire investigation. Ransomware is effectively the same as someone burning down all the key paper documents hospitals keep, including patient and billing records. Yet, none of the usual support exists should a hospital experience a cyberattack.

A cyberattack can happen quickly. A midlevel programmer on the database team receives an email from a major delivery service. The email says that the package was sent by the company's health care insurer. Although she is not expecting a package, the programmer clicks on the link to track the package. The link takes her to a page that looks like the delivery service. While she is typing in the tracking number, malware is delivered to her computer. The malware quickly captures her login credentials, and because she has broad administrative rights to company systems, ransomware quickly spreads across the systems and encrypts the data, network and backups. The ransomware also puts itself on every USB drive that is plugged into any computer in the system. Patient records are not available, so treatment is delayed or patients are turned away. The FBI is called, but does not have a solution. The incident makes the national news. The hospital system eventually decides to pay the ransom. Now, they are a known target.

Ransomware is only one of the many cyberthreats confronting health care institutions, big and small, in the cyber realm. While no magical bullet exists to slay the cyber beast, we offer the following seven basic rules that can help put out the ransomware fire.

1. Implement cybersecurity education and training that is frequent and reaches across the entire organization.

Most hospital systems have cybersecurity annual training programs. However, annual training is not enough. Most ransomware enters a company through human error.

Create a phishing training program that becomes increasingly sophisticated over time. Provide employees immediate feedback, good and bad, from the phishing results. Make clear the potential ramifications of not following procedures, both to the company and to the employee personally. Develop a specialized training program for senior and midlevel information technology and operations leaders in order to stress that security is not just the responsibility of the information security group.

The goal is to change the culture within the organization so that every person, from the lowest to the highest, believes that security of information is their personal responsibility. With proper training, the story above would have been: A midlevel programmer receives an email from a major delivery service. The email says that the package was sent by the company's healthcare insurer. She is not expecting a package. She forwards the email to the institution's information security team's "abuse" mailbox. The team checks the email, realizes that is a dangerous phishing email, and sets the system to intercept all similar emails. A warning is sent throughout the company warning them about the particular threat. Ransomware does not infect the system.

2. Fire someone and put warnings in employee permanent files.

This sounds harsh. However, the best way to change the culture within an organization is to strictly enforce policies. Someone who is unwilling to follow proper security procedures risks the enterprise and the patients. If they email personal health information to their personal email address, if they click on a phishing link, if they share their passwords, fire them. More than any training, terminating someone's employment sends a message to the entire organization that cybersecurity is critical — to the company and to their jobs. Remember: Habitual clickers are putting your company at risk, with millions of dollars and patient lives in play

3. Back up data in a secure manner.

Back up your data. This sounds like a simple IT function. However, modern ransomware encrypts backups along with the primary data stores. Even certain backups clouds are subject to ransomware encryption. It is possible to backup data in ways that are more secure, and allows recovery without paying the ransom. The legal, risk and compliance teams need to work with IT and information security to understand the architecture of the system and what data will be available under differing attack scenarios. Testing of both the system and the backup is critical.

4. Bring in qualified consultants and counsel to do a cybersecurity preparedness review.

Hire a consultant and have them come in and provide an independent review of the overall preparedness of the organization. If you have counsel, hire them for the review and tie it to a legal compliance assessment, so that the initial report is privileged. Pick a consultant and counsel that are highly qualified, have good references and are able to provide information not only to the IT team but to the legal, risk and compliance teams as well. A good consultant will provide information that will identify areas of risk and suggestions of mitigation strategies. Some advice may help prevent a ransomware attack.

Often, companies have a response plan for cyber events sitting on the shelf. That plan needs to be pulled out, reviewed, most likely revised, and made a part of operations for at least IT, information security, legal, risk and compliance. Have names associated with activities and responsibilities. Include backup people. Plan for communication failures, both within and outside the company. Designate who is responsible for contacting the authorities, the forensic team, outside legal counsel, your cyber response organization and applicable regulators. Assume that systems, including email and phone, may not be available. Update the plan on a regular basis, at least quarterly. Develop scenarios with counsel and the consultants, and then test the response under varying scenarios. Often legal, risk and compliance groups work in silos, or don’t communicate effectively with the IT and information security groups. That is no longer acceptable if an organization wants to have an appropriate cybersecurity protection and response plan.

5. Cyberinsurance.

Sufficient cyberinsurance is difficult to obtain and is expensive. Each insurance company has different coverages, with significantly differing definitions and exceptions. A lawyer experienced in cyberinsurance is invaluable in assessing the coverage of a particular policy, and matching it to the requirements of the company, so that appropriate coverage exists when an event occurs. Certain brokers specialize in cyberinsurance. Between a qualified broker and an experienced lawyer, the hospital system will know what protections they have, and what risks they continue to bear. Additionally, many insurance companies provide services along with the insurance when an incident occurs. Notifying the insurance company promptly upon discovery of an event is critical. The insurance company may be able to help in ways you may not know.

6. Hire an experienced ransom negotiator.

Don't hire the wrong person to negotiate a ransom. First, there may not be time to negotiate. Second, if the person trying to negotiate does not have the right experience with the types of cybercriminals who are the primary actors today, the situation may spiral out of control and data may become permanently unavailable. Some of the newer ransomware variants copy the data from the system. You may not just be negotiating whether the hospital institution is able to run its systems and use the data, you may be negotiating whether critical information, including Personal Health Information, is released publicly. These are dangerous issues, and having the most experienced team is critical.

7. Hire a cybersecurity lawyer.

The above six steps assume that the institution has hired competent cybersecurity counsel. This is not privacy counsel that has added cybersecurity to their resume, or breach counsel who has assisted in responding to a data breach. Cybersecurity lawyers operate at the intersection of technology, forensics, risk and legal issues. A true cybersecurity lawyer will be able to speak with the technology and information security teams, understand the precise technical situation, including the cryptographic techniques that are being used, and translate this to the business, compliance and risk teams. The cybersecurity lawyer will guide the investigation, including ensuring that the team does not break laws during the investigation, and that all of the appropriate legal avenues are being pursued.

All too often people mistakenly hire repurposed privacy lawyers or rely on their usual counsel. The result is often akin to what happens when you allow an academic military adviser with no real-world experience to devise the strategy for battle: You get slaughtered.

The seven basic rules shared above are akin to installing fire sprinklers, and establishing fire safety protocols. Hospitals have fire response plans with coordinators on every floor, written protocols to ensure the safety of employees and patients, and directions as to the proper authorities to contact if there is a fire. With a cyberattack, the hospital system should have all of that, plus it must play the role of the fire department and emergency medical services for the entire system, both technological and physical. This is far more complicated than dealing with a fire, yet most hospital systems have devoted far fewer resources to cyberattack prevention and response. This must change. With the right advisers, foresight and effort, a hospital system may be able to put out its cyber fire before it begins.

—By Daniel B. Garrie, JAMS, and Richard M. Borden, Robinson & Cole LLP

Daniel Garrie is an arbitrator, forensic neutral and technical special master at JAMS, available in Los Angeles, New York and Seattle. He is executive managing partner of Law & Forensics LLC and head of the computer forensics and cybersecurity practice groups, with locations in the United States, India and Brazil. He is an adjunct professor at Cardozo School of Law.

Richard Borden is counsel in Robinson & Cole's Hartford, Connecticut, office and an adjunct professor at Cardozo School of Law. He was previously chief privacy officer and chief information security and privacy counsel of DTCC, and senior vice president and assistant general counsel at Bank of America.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.