Ransomware: Coming to a Health Care Organization Near You

Executive Summary, April 2016

Enterprise Risk Management Task Force

AUTHORS

Patricia Hughes*

OneBeacon Healthcare Group

Farmington, CT

Michaela D. Poizner

Baker Donelson Bearman Caldwell & Berkowitz PC

Nashville, TN

Karina C. Smuclovisky

Memorial Healthcare System

Hollywood, FL

Ransomware

Cyber risk is constantly evolving and unpredictable, making preparation difficult and mitigation costly. The health care industry is no stranger to cyber risk and ransomware is the "new kid on the block," making headlines monthly and paralyzing hospitals across the country. According to the Risk Insurance Management Society, ransomware is one of the top ten cyber threats of 2016[1] and is the modern day form of highway robbery. U.S. state and federal regulators and the courts already have taken an active role in "policing" cyber risks and their impact on businesses and individuals. In a 2015 court ruling,[2] the Federal Trade Commission confirmed its authority to regulate corporate cybersecurity. Companies should take note that they can be held responsible for failing to properly safeguard consumers' information. Representative Ted Lieu (D-CA), a member of the House Oversight and Government Reform Subcommittee on Information Technology, recently noted that under federal law there is no requirement for hospitals to report a ransomware attack or notify patients whose information may have been compromised, because ransomware doesn't necessarily take data itself, but just blocks access to the data. Lieu indicated he is considering legislation that would amend the Health Information Technology for Economic and Clinical Health Act to require health care organizations to notify patients, and perhaps the federal government, of a ransomware attack.[3]

In a recent Independent Security Evaluators Report that looked at the critical elements within hospital and health care-related infrastructures and systems related to securing patient health, the authors came to an ominous and provocative conclusion:

> The findings show an industry in turmoil: lack of executive support, insufficient talent, improper implementations of technology, outdated understanding of adversaries, lack of leadership, and a misguided reliance upon compliance. These findings illustrate our greatest fear: patient health remains extremely

---

[1] Hilary Tuttle, *10 Cyberthreat Predictions of 2016*, RISK MGMT. MAG., Mar. 2016, *available at* www.rmmagazine.com/2016/03/01/10-cyberthreat-predictions-for-2016/.
[2] *Federal Trade Comm'n v Wyndham Worldwide Corp*, 799 F.3d 236 (3d Cir. 2015).
[3] Alex Ruoff, "*Lawmaker Mulls Requiring Hospitals to Report Ransomware Attacks*, BLOOMBERG BNA, Mar. 24, 2016, *available at* www.bna.com/lawmaker-mulls-requiring-n57982068994/.

> vulnerable. One overarching finding of our research is that the industry focuses almost exclusively on the protection of patient health records, and rarely addresses threats to or the protection of patient health from a cyber threat perspective.[4]

Health care organizations traditionally have not been a target of ransomware attacks, but this is no longer the case. The ransomware mostly targeting the health care industry is known as "crypto ransomware," which encrypts personal data and files, disabling access to those resources. Once those files are targeted by the malware, a time-limited ransom fee is required to regain access. If the clock to pay the ransom expires, the decryption key may be permanently deleted and the user may permanently lose access to the targeted files, leaving victims little time to consider options. The malware's crippling effect forces most victims to pay the ransom. Once the ransom is paid many questions remain unanswered, such as whether the hackers will utilize any of the information accessed and whether other malware was embedded into the systems infected.

Since the beginning of 2016, hospitals have appeared monthly in the headlines as victims of ransomware attacks. On January 15, 2016, Titus Regional Medical Center in Texas was the first of those hospitals when a ransomware virus infected the health system's servers, prohibiting access to electronic medical records and restricting the ability to input or access interdepartmental orders. The health system chose not to pay the ransom and was forced to resort to paper while simultaneously working to restore its servers.

The February 5, 2016 ransomware that infected Hollywood Presbyterian Medical Center (HPMC) in California affected computers essential to the function of the laboratory, pharmacy, radiology area, and emergency room. Two weeks after the attack, the hospital paid 40 Bitcoins in ransom, equaling $17,000, to restore its systems. Computers at the Los Angeles County Health Department (Health Department) also were infected with ransomware in February 2016. Unlike HPMC, the Health Department

[4] Independent Security Evaluators Report, *Securing Hospitals: A research study and blueprint*, Feb. 23, 2016.

refused to pay the ransom and is restoring its systems from backups. Most recently, ransomware is the suspected culprit behind the attack at MedStar Health Inc., and the Federal Bureau of Investigation (FBI) investigation is ongoing.

The dramatic events at HPMC are a sobering reminder of the threat that ransomware presents to health care organizations, and the attack on HPMC is not an isolated incident. According to a report by Intel Security, ransomware samples grew 58% in the second quarter of 2015 alone and 172% year-over-year.[5] Similarly, data from the FBI's Internet Crime Complaint Center demonstrates that the most current and significant ransomware targeting the United States, CryptoWall, was the source of 992 complaints and victim losses totaling more than $18 million between April 2014 and June 2015.[6] Electronic systems are critical for hospital operations and patient care and when those systems are breached, lives are at stake. It is imperative that health care providers take proactive steps for mitigation, including implementing a comprehensive cybersecurity strategy and having the appropriate cyber insurance coverage.

Enhancing Cybersecurity

Ransomware presents a very real enterprise risk, and it is imperative that health care providers take proactive steps with respect to their cybersecurity to mitigate the risk of an attack and to be prepared to respond quickly and effectively in the event of a ransomware incident.

[5] Intel Security, *McAfee Labs Threat Report*,, Aug. 2015, *available at* www.mcafee.com/us/resources/reports/rp-quarterly-threats-aug-2015.pdf.
[6] Federal Bureau of Investigation, Public Service Announcement, *Criminals Continue to Defraud and Extort Funds from Victims Using CryptoWall Ransomware Schemes*, June 23, 2015, *available at* www.ic3.gov/media/2015/150623.aspx.

Prevention

Organizations should take a comprehensive cybersecurity approach to stay out of the grips of a ransomware attacker. While a hack is never completely preventable, following these tips will help to reduce your organization's risk:

- Take your Health Insurance Portability and Accountability Act (HIPAA) security policies and procedures seriously well before an attacker strikes. Too many organizations get focused on cybersecurity *after* they've experienced a breach. The proliferation of hacker incidents against providers of all types and sizes demonstrates that no one is immune. Specifically, the U.S. Department of Health and Human Services Office for Civil Rights (OCR) and the FBI recommend:
    - Segmenting data among networks and regularly backing it up to ensure that critical data can be restored in the event of a ransomware attack.
    - Always using antivirus software and a firewall, and maintaining these defenses with regular updates.
    - Enabling pop-up blockers and internet filters on the organization's computers to avoid accidental clicks that could be harmful.

    Work with trained experts who can develop and implement cybersecurity policies and procedures that are thorough and that are tailored to your organization. This step will both help you ensure HIPAA compliance (which is crucial in the event of a breach or an audit) and protect your organization from damage at the hands of a hacker.

- Make sure employees are well-trained to be suspicious of emails with attachments or links from unknown senders. Even emails that appear to be from a trusted party should be carefully examined before clicking. Many, many breaches occur because a well-intentioned, but unwitting, employee clicked a link or opened a file that allowed a virus to infiltrate the organization's network.

- To help organizations stay ahead of email scams, the Better Business Bureau has launched a "Scam Tracker"[7] that allows users to report scams and issues scam alerts. Encourage information technology personnel to monitor the Scam Tracker to stay on top of scam alerts and warn employees of threats.

Response

If your organization is the victim of a cybersecurity attack, a fast and effective response is critical, both operationally and legally. It is important to have a detailed, up-to-date incident response plan in place well before any sign of trouble. If the organization goes into a crisis, key personnel should be in a position to respond immediately rather than trying to create a response plan "on the fly."

Additionally, personnel must be trained to never ignore signs of a breach. Even if the incident appears to be insignificant, the organization must take the threat seriously and respond right away. Allowing a situation to develop, or "waiting to see what happens," may put the organization's ability to function in jeopardy (and create a public relations nightmare if the breach turns out to be serious).

A comprehensive cybersecurity program is key to preventing and responding to ransomware attacks like the one at HPMC. Because when an attack will occur is unpredictable, getting your cybersecurity house in order as soon as possible—and keeping it in order—should be a top priority for your organization.

Mitigating Economic Risk Through Cyber Insurance

Cybercrime has been a significant risk exposure for all types of businesses for some time and is not a new type of loss for insurers. But as recent events have shown, a relatively newer, but rapidly growing, type of cyber risk perpetrated against health care organizations is ransomware and other malware attacks with extortion demands. The

[7] *Available at* www.bbb.org/scamtracker/us.

economic impact to health care organizations is significant as attackers demand increasingly higher “ransoms” to regain access to data, or to decrypt data, with no guarantees that the organization could not be attacked again. Additionally, there may be ongoing economic impact as entities may find themselves providing patient identity theft protection monitoring for a large volume of individuals over long periods of time, becoming the subject of litigation, coming under scrutiny by OCR and being subject to other federal and state regulatory enforcement actions, and suffering reputational harm.

Cyber Insurance: Ransomware Attacks and Cyber Extortion

One well-established technique for treating losses is risk financing. Cyber insurance is an important method for mitigating the financial risk exposures of information privacy and data security breaches, business interruption, or other types of cyber-related events in health care.

Cyber extortion coverage is the type of insurance that would respond to a ransomware attack. According to David Molitano, Senior Vice President at OneBeacon Technology Insurance, “cyber extortion” types of coverage can provide compensation for the cost of the ransom demand that is paid when an entity must get their business operations back in service quickly. However, organizations may still incur significant costs. Often the amounts demanded are below the insurance policy’s deductible. In the event of an attack, a carrier may guide an insured on how to respond to the event, but the money will be paid by the breached organization. This need is often not contemplated by many companies. If the attack exceeds the coverage limits purchased, or the losses or aspects of the losses come under policy exclusion, the attacked organization may experience a significant financial impact.

Terminology is important in these policies. The general terms of coverage in the policy usually revolve around the word “extortion.” The key to what may or may not be covered is in the language itself. Trigger language in a policy may deal with the event only after the network has been seized, not when the threat is received. Unbeknownst to the company, their network may be seized prior to the request for money. It can become

somewhat tricky to determine when coverage is applied unless there is language in a policy that also indicates that the policy will respond to a threat.

“Covered territory” language in a policy also may pose an issue. As the “cloud” is everywhere, will an insurance policy cover events for U.S. data that reside in another country? Will it respond to non-U.S. data that are housed in the United States? The covered territory condition in a policy is a key one to establish since the location where the data rest will weigh significantly in the coverage decision.

Considerations for Cyber Policies

As with any type of insurance policy purchase, the decision-making process is a two-way street, and both the organization and the carrier must consider key issues.

For the organization seeking cyber coverage, some questions to ask of itself include:

- Do you have a comprehensive enterprise risk management, cybersecurity strategy in place?
- What is your governing body’s expectation regarding how enterprise risk financing decisions are made? Can you present quantitative data to support your proposal, including risk/threat assessment results, breach/attack response, coverage needs, coverage options, possible coverage gaps, and an analysis of possible losses?
- Does the organization need more than one insurance product to provide a comprehensive cyber security coverage program? Traditional cyber policies may not be able to provide protection against some of the newer emerging “hybrid” risks, such as loss of intellectual property, bodily injury, or property damage. What about reimbursement coverage for other costs such as downtime, scanning, and uploading of handwritten files; destruction of business or patient files by the cyber extortionists; identity theft (PII or PHI); or the economic impact of reputational loss?

- If the entity is part of an insurance captive, a risk retention group, or has a self-insurance trust, what, if any, cyber-related issues are being addressed by these vehicles? And to what extent?
- Can your insurance broker bring expertise and knowledge about cybercrime and cyber coverage products to assist you in your decision-making process?
- Can the broker/agent bring experienced cyber insurance carriers in the marketplace to the table?
- Do the considered carriers provide resources such as risk assessment tools, educational/training tools, breach/attack response plans, and access to a pre- and post-breach response vendor? Is there a cost for accessing these resources?

For the insurance carrier considering new or renewing business:

Remember, the insurance submission for coverage is an organization's first opportunity to reassure a carrier that you are knowledgeable about your business and will be a "good risk" and partner over the long term, and therefore deserving a "good policy at a good price." The following are questions the insurance carrier will consider when evaluating a submission:

- Does the organization have a comprehensive enterprise risk management, cybersecurity strategy in place?
- Are threat assessments and analyses performed at periodic intervals? Do these analytic measures include outsourced penetration testing by a reputable resource?
- What tools or programs are in place to detect intrusion?
- What hardware and software measures are in place? Are they updated as needed?
- What policies and procedures are in place to address electronic and physical information privacy and data security?

- What backup systems are in place?
- Is there a tested incident response plan for data breach/attack in place?
- Who responds to breaches? How and when an organization first responds to an attack is critically important.
- Is there a comprehensive business continuity and recovery plan in place?
- What is the organizational policy regarding payment of a demand in a ransomware attack?
- What types of training and education are required for employees, medical staff, students, and/or volunteers?
- What do your vendor and contractor agreements address?
- Is there an incident reporting program in place that will ensure timely notification internally and of your carrier?
- Have there been any cyber-related incidents, claims, or lawsuits?
- What does the current insurance coverage program look like? What are the goals and objectives for the organization regarding cyber insurance coverage?

Conclusion

The health care industry is in need of a more comprehensive approach to controlling and mitigating cyber-related risks. Ransomware attacks and extortion demands may be a clarion call to those organizations that have not yet fully recognized or acknowledged the need. The financial impact cannot be ignored. Although there are a number of ways to try to control and mitigate cyber-related risks, complete elimination of the risk is not likely. In today's world, all types of cyber risks must be considered a top enterprise risk exposure to be proactively planned for and managed, rather than to be reacted to when detected.

We would like to thank Patricia Hughes (Senior Vice President, Healthcare Risk Management, OneBeacon Healthcare Group, Farmington, CT), Michaela D. Poizner (Attorney, Baker Donelson Bearman Caldwell & Berkowitz PC, Nashville, TN), and Karina C. Smuclovisky (Assistant General Counsel, Memorial Healthcare System, Hollywood, FL) for authoring this Executive Summary.