September 2017

Using an Enterprise Risk Management Approach to Limit Ransomware Threats in Healthcare
By Barbara Youngberg
Introduction

Healthcare organizations are becoming increasingly mindful of the risks associated with cyber-attacks caused by ransomware. Organizations victim to recent, widely publicized attacks include MedStar in Washington DC, Hollywood Presbyterian Medical Center in California, Kentucky Methodist Hospital in Kentucky, and the NHS or British Healthcare system. Many reporters and security firms predict continued attacks on healthcare organizations for a variety of reasons. Some suggest that after the government’s mandate requiring healthcare organizations to convert to electronic health records quickly to receive government subsidies, healthcare organizations focused on implementation rather than security. Others cite the lack of healthcare staff focused on security. Finally, many suggest that healthcare organizations’ reliance on operational IT systems to deliver safe care to patients increases the likelihood that they will pay the ransom demanded to access their systems.

These attacks, which can render computers unusable or critical files unreadable, can have significant impact on organizations. Perpetrators seem uninterested in the dissemination of confidential information; they are instead interested in disrupting business operations until the ransom is collected. Implementing an enterprise risk management strategy can help decrease the likelihood of ransomware attacks and the negative impact attacks they may have on your organization.

The term “ransomware” refers to malicious software introduced into an IT system and potentially medical devices that immediately encrypts the data in the system making it unusable. The program displays a screen demanding payment (generally in Bitcoin) to obtain access to data. The price typically increases until the end of a countdown, at which point the files are destroyed. If the ransom is paid, the attacker provides a decryption key, which enables the organization to unscramble and regain access to data.

Bitcoin

Bitcoin is a form of digital currency transmitted over the internet. Buyers and sellers transfer funds directly with no intermediary such as a payment service or bank. The identity of the buyer or the seller is unknown, and this information is untraceable. Bitcoin is a truly global currency and has no limits in amount transferred or frequency of transfers.

The FBI strongly advises against paying ransom when these attacks occur; however, when a healthcare organization feels it has no other choice, guidance from the Board may be required. Circumstances where it may be advised to pay the ransom could include instances where the loss of critical data will compromise patient quality and safety. Ransom must only be paid as a final resort.

Time is of the essence with these attacks, so your organization should determine how to obtain Bitcoin in the event of an emergency. In a recent publication by CommVault three steps are identified for obtaining Bitcoin:

» Determine the current US dollar value of the Bitcoin request. This currency’s value fluctuates significantly. Know exactly what the ransom is that will be paid in order to make an informed
decision and to set up the fund transfer. Using a bitcoin currency calculator™ can facilitate this conversion.

> Set up a Bitcoin wallet, a software program where Bitcoins are stored. There are a number of companies that offer this service.

> Buy Bitcoin from an exchange. Multiple exchanges are set up for the purchase of Bitcoin.

### How Hackers Enter Your System

According to a publication from Everbridge,™ malware can enter your organization’s communication systems in multiple ways:

> Emails, the most common point of entry, are often disguised as internal memos from other departments and contain a link or download. Once an employee clicks on the link, the ransomware attack begins.

> Flash drives provided by an organization or owned by employees can pose a large threat by creating multiple new entry points throughout the IT system. The risk may be hard to contain since risk managers, security professionals, and IT staff may not know how many of these devices are being plugged into your organization’s computers.

> Hackers can enter a system when employees, patients, or even guests surf the web utilizing an organization’s Wi-Fi. An email may point the reader to a URL that begins downloading the malware as soon as the link is clicked. More sophisticated hackers are even injecting on to legitimate websites that the site visitor innocently lands on through a normal web search.

> Malvertising occurs when hackers visit a legitimate URL and download the virus on a legitimate ad through a backdoor channel. When the computer user clicks on the ad, the malware enters the computer system.

> Botnets can also be used by hackers. “Bots are one of the most sophisticated and popular types of cybercrime today. They allow hackers to take control of many computers at a time, and turn them into ‘zombie’ computers, which operate as part of a powerful ‘botnet’ to spread viruses, generate spam, and commit other types of online crime and fraud.”™

### HIPAA Obligations when Ransomware Incidents Occur

On July 11, 2017, the Department of Health and Human Services’ Office of Civil Rights advised hospitals and other healthcare systems of their obligations should a ransomware attack occur.™ This warning extended to other covered entities and business associates of healthcare entities. In this notice, the Office of Civil Rights warned that in the event of a ransomware attack, healthcare organizations must presume that a breach (in violation of HIPAA) has occurred unless they can establish that the probability that personal health information has been compromised is low. This triggers the need to report the potential breach to any individuals or organizations whose data may be impacted.

### Cyber Insurance

The complexity of cyber risks cannot be understated. Cyber liability insurance is an essential product in an organization’s risk transfer portfolio to protect the organization from many types of the risks presented. The products vary in scope of coverage, and policies may change to respond to emerging risks. It is important to work carefully with your broker to identify carriers that provide the broadest
coverage and that have expertise in responding to these types of risks. For organizations with limited expertise in this area, it may be beneficial to identify carriers that can provide experts to both identify and mitigate this unique risk.

An Enterprise Wide Approach

Developing an enterprise risk management strategy will help your organization manage complicated cyber risks. The ASHRM publication, “Enterprise Risk Management: A Framework for Success,” can serve as a guide to develop a multi-disciplinary approach focused on both proactive planning and effective response. Individuals from the following risk domains will need to collaborate to manage the risks associated with ransomware:

» **Operational** – Remain up-to-date on the emerging and evolving risks and the infrastructure in place to address them. If vulnerabilities are identified, budget priorities may need to be reassessed.

» **Clinical / Patient Safety** – Plan for the possibility that all information necessary to care for patients safely will become unavailable in the event of a ransomware attack.

» **Strategic** – Proactively establish a plan for working with clients to assure them that every possible action to secure their data is being taken. Reputational risks associated with ransomware attacks must be considered, as patients expect their personal health information to receive the highest level of protection.

» **Financial** – Develop a strategy for quantifying the potential financial risk should a ransomware attack occur. Although payment to those initiating the attack is not recommended, it will be important to calculate the cost of business interruption and the risk of continuing operations without access to vital information. If the ransom will be paid, work with others (attorneys, cyber carrier, or broker) to acquire the necessary Bitcoin or currency required to obtain a decryption key.

» **Human Capital** – Identify the educational needs of employees who introduce malware into the hospital system by having risk management, IT, and human resources staff work together. Computer based educational modules and reminders placed on computers should be utilized to provide guidance as to how to avoid this potential risk.

» **Technology** – Develop a reliable back-up system for all files. The IT staff budget must be evaluated to allow proper measures to be taken. Some attacks have occurred in organizations or systems that failed to download the patches for Microsoft software that were recommended in months prior.

» **Legal / Regulatory** – Develop processes for not only reporting the potential privacy violations associated with ransomware attacks but also for reporting events to appropriate carriers to assure that cyber liability carriers are put on notice.

Key Elements of an ERM Strategy

Hacking tactics are constantly changing, so your enterprise risk management strategy must evolve accordingly. Measures that can be identified and carried out prior to an attack are as follows:

» Assess your entire organization including remote facilities to understand where all critical data is stored.
» Identify systems that present the highest risk. Construct your organization’s risk inventory, and determine focus areas.

» Quantify all potential sources of risk including electronic health records, medical devices, and physical and digital media. Work with your organization’s cyber liability carrier to verify that all devices are covered.

» Apply all available security controls, and verify that recommended patches have been installed.

» Develop an educational plan for all employees. Creating online learning modules that staff can access on their own time may be advised. Post flyers at work stations reminding staff not to click on suspicious links or download suspicious material.

» Appoint an individual to monitor this evolving risk and to ensure that system changes and staff education are responsive.

If an attack on your organization is reported, the response plan should include the following steps:

» Immediately identify and implement the back-up strategy. Prioritize efforts so that the most critical data is made available to those who need it to support operations.

» Advise the compliance department of the nature of the attack to determine the need to report to the Office of Civil Rights.

» Work with your broker or cyber liability provider to determine coverage.

» Perform a root cause analysis to determine failure modes contributing to the attack.

» Implement the necessary fixes to address failure modes.

» Consider engaging an external IT expert to try and hack into your system from the outside to identify any additional problems.

Many believe paying ransom to attackers only increases the likelihood of future, more sophisticated attacks. It is best to develop and implement a comprehensive and proactive plan. Beecher Carlson’s Cyber Practice can help you manage the intricate risks that cyber liabilities pose. Contact Beecher Carlson today to increase your program’s efficiency, educate your staff, reduce your risk, and customize your response strategy.
LIMITING RANSOMWARE THREATS

https://www.washingtonpost.com/local/likely-ransomware-cyberattack-still-crippling-medstar-health-computers-at-somehospitals/2016/03/30/a82c9fa8-6f87-11e5-8b23-538270a1l (accessed 8/15/2017)


http://www.ashrm.org/pubs/files/white_papers/ERM-White-Paper-8-29-14-FINAL.pdf

Ibid at 10


http://www.ashrm.org/pubs/files/white_papers/ERM-White-Paper-8-29-14-FINAL.pdf at page 13

Disclaimer

This article is intended for informational purposes only. It is not a guarantee of coverage and should not be used as a substitute for an individualized assessment of one’s need for insurance or alternative risk services, nor should it be relied upon as legal advice, which should only be rendered by a competent attorney familiar with the facts and circumstances of a particular matter. Copyright Beecher Carlson Insurance Services, LLC. All Rights Reserved.