HELD FOR RANSOM: PROTECTING YOURSELF AGAINST GROWING CYBER EXTORTION THREATS

Authored by:
Colin Konschak, FACHE, Divurgent
Shane Danaher, MBA, Divurgent

INTRODUCTION

Targeting healthcare in cyber extortion attacks is becoming a lucrative business for criminals, but it is also serious business, because when healthcare is hit with cyber extortion, people's lives are literally being held for ransom. Hospitals, health systems, private practices, and even vendors who support the healthcare system, are constantly under imminent danger of being locked out of access to their data, their computer systems, and their lifesaving medical devices.

In this latest whitepaper in our continuing cybersecurity series, we look at cyber extortion—how it happens, where the vulnerabilities lie, and how lessons learned from inside and outside of healthcare can help you avoid being attacked or recover more quickly from the hit.

When most people think of cyber extortion, they think of ransomware—malicious software that encrypts data in a manner that can lock people out of access to their data, and even backups of the data. Although ransomware has become a synonym for cyber extortion, it is only one element, and sometimes not involved, as in the case of denial of service cyber extortion attacks. Instead, cyber extortion is a process, and understanding how that process works is the most important step in guarding against it.

> *"Healthcare enterprises face all the same challenges that the rest of us do, but a recent plague is one for them to focus on, and that is the ransomware plague. Hackers suddenly see the healthcare sector as a piggy bank."*
>
> -- FBI Director James Comey speaking at a March 2017 conference in Boston (Chalfant, 2017).

HOW CYBER EXTORTION WORKS

In its January 2018 monthly cybersecurity newsletter, the Department of Health and Human Services Office for Civil Rights (OCR) provided this succinct definition of cyber extortion: "Cyber extortion can take many forms, but it typically involves cybercriminals demanding money to stop (or in some cases, to merely delay) their malicious activities, which often include stealing sensitive data or disrupting computer services" (OCR, 2018). The newsletter also pointed out the most common types of attacks used in cyber extortion: ransomware, denial of service/distributed denial of service, and outright stealing of sensitive data. These are highlighted briefly below:

Ransomware—malicious code (known as malware) that locks users out of access to a system or sensitive data—is usually delivered through a social engineering attack, such as "phishing" or "pretexting." In phishing, the attacker poses as a trusted party, and sends an email designed to persuade the recipient to download open an attachment containing the malware or visit an infected website. While phishing is a generalized attack, criminals

also may also target a particular individual—called "spear phishing"—or they may target executive staff or other organizational leaders, which is known as "whaling." Pretexting is also a form of spoofing in which the attacker impersonates a trusted or known individual, such as an employee, client, or someone from tech support, and requests information in an attempt to gain access to the organization's network.

Denial of service (DoS) and **distributed denial of service** (DDoS) are different from ransomware attacks because they don't use malware. Instead, computers and networks are targeted directly with a volume of network traffic so high that it overwhelms them, rendering them unable to respond to users. The distinction between DoS and DDoS attacks is that DoS attacks come from a single source while DDoS attacks come from many sources and are more difficult to defend against and recover from. In DoS and DDoS, the extortionist demands payment to either stop an attack in progress or to not initiate an attack. People in healthcare organizations need to be vigilant for unusual activity on their computers and networks.

Another type of cyber extortion attack happens when the attacker breaches an organization's network, steals sensitive data, and then threatens to publicly expose the data or sell it to others.

The big question these types of cyber extortion attacks raise with potential and actual targets is: "Will it do us any good to pay the ransom?" We will delve into that subject a little later in this whitepaper after exploring who is being attacked and how these attacks are being carried out.

WHO IS GETTING HIT?

In its report titled, "Threat Predictions for 2018," global cybersecurity firm Kaspersky predicted the 2018 cybersecurity threats to connected healthcare. Of the company's nine major predictions for 2018, the following four are related to cyber extortion:

- "Attacks targeting medical equipment with the aim of extortion, malicious disruption or worse, will rise.
- There will also be a rise in the number of targeted attacks focused on stealing data.
- There will be more incidents related to ransomware attacks against healthcare facilities.
- Disruptive attacks—whether in the form of denial of service attacks or through 'ransomware' that simply destroys data (such as WannaCry)—are a growing threat to increasingly digital health care facilities" (Kaspersky Lab, 2017).

As we mentioned above, healthcare has become a particular focus of cyber extortion. The global cybersecurity insurance company Beazley reports that healthcare suffered more ransomware attacks than any other industry in 2017. In more than 2,600 data incidents studied in 2017 across several industries, 45 percent of all ransomware attacks occurred in the healthcare sector. The next highest volume of ransomware attacks happened in the financial (12 percent) and

professional services (12 percent) sectors. (Beazley, 2018). In addition, Verizon's 2018 Data Breach Investigations Report found that in 2017, ransomware made up 85 percent of malware attacks, which is up from 72 percent in 2016 (Verizon, 2018).

Cyber extortion was a factor in several of the biggest healthcare breaches in just the first four months of 2018:

- On the night of January 11, staff at Greenfield, Indiana-based Hancock Health noticed their network was running slowly. Not too long after, a ransomware notice was found on a hospital computer screen, with the attacker stating parts of the system would be held hostage until a bitcoin ransom was paid. Officials immediately shut down the system and employees were instructed to turn off all computers and revert to using pen and paper for recording patient visits. Hancock Health officials said the attacks were very sophisticated and did not involve an employee opening an infected email, and that the goal was to shut down hospital operations (Davis, 2018, January 15).

- On January 26, the electronic health record (EHR) giant Allscripts was sued by one of its healthcare clients, alleging that it had not properly secured and audited its system after suffering a week-long ransomware attack starting on Jan. 18 that locked some users out of patient information. The clients claimed they suffered "significant business interruption" during the outage, which was caused by SamSam ransomware and affected about 1,500 clients. Users complained on Twitter that the company's cloud EHR was down and they were not able to access patient information (Davis, 2018, January 26).

- In late February, the IT vendor for three Southern California locations of the Center for Orthopaedic Specialists (COS) was hit by attackers locking out users and encrypting patient data. The breach of approximately 85,000 patient records was involved. The IT provider was not disclosed by COS (Davis, 2018, April 26).

HOW DOES AN ORGANIZATION DEFEND ITSELF?

First rule: Don't be stupid. That may sound a little harsh, but it is good advice, because many cyber extortion attacks start with targeting the human attack surface, where deception and trust are used as the main levers for getting in the door. Cultivating an organizational awareness of how these attacks occur is the best defense against dumb mistakes. Let's look at ransomware attacks first, because they most often start with an attacker exploiting human vulnerabilities through social engineering.

Ransomware attacks occur when cybercriminals insert malware, such as Locky, into a company's system, usually through a phishing attack. When activated, the software locks the system, denying

access to all or some of an organization's files. The cybercriminals then demand payment, often in untraceable bitcoin. A sample message might say: "You have only 96 hours to submit the payment. If you do not send money within the provided time, all your files will be permanently encrypted and no one will be able to recover them."

In one year, the Institute for Critical Infrastructure Technology (ICITech) reported that the Samas ransomware group earned $450,000 from organizations that paid, though not all of these were in the healthcare sector (ICITech, 2017).

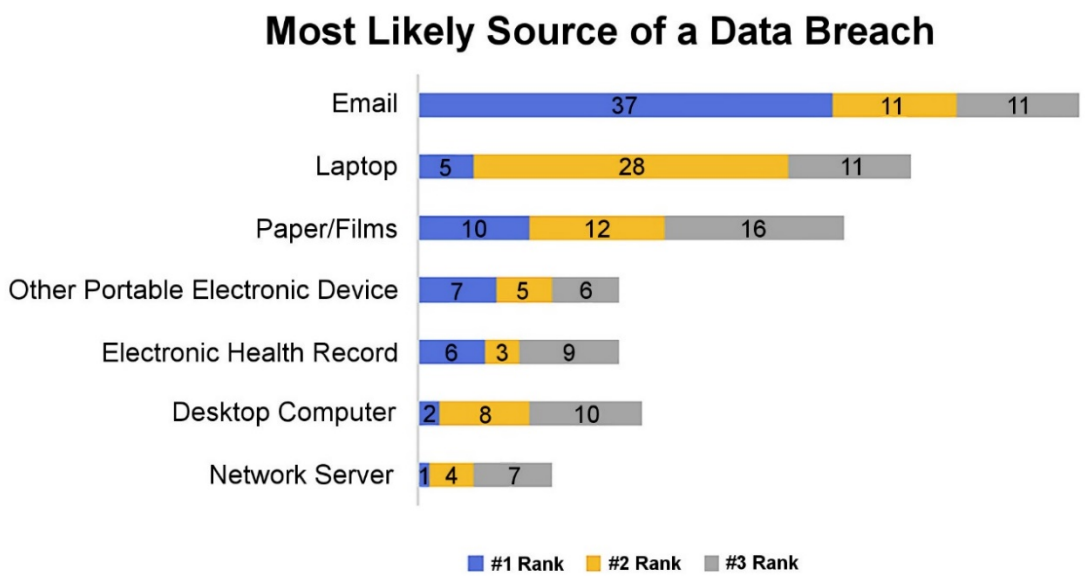
The 2017 Data Breach Industry Forecast from Experian estimates healthcare entities were paying about $300,000 a day in ransoms to reclaim their data, although the average payment is relatively small–about 2 bitcoins, or $670 at the time (Experian, 2017).

Getting to the real numbers when it comes to ransomware attacks in healthcare is challenging, in part because companies try to keep the attacks under wraps. A *Healthcare IT News* and HIMSS Analytics survey found that more than half of all hospitals were hit with ransomware between April 2015 and April 2016, but that 25 percent of institutions surveyed didn't even know whether they had experienced such an attack. (Davis, 2017, March 20)

This problem appears to be getting worse, and infected e-mail sent to unsuspecting users is the culprit in a great majority of the cases. In December 2017, the results of a study conducted for a leading email and data security company, Mimecast, by HIMSS Analytics found that U.S. healthcare providers rank email by far as the number-one source of potential data breaches. The study revealed that 78 percent of respondents had already experienced an email-related cyberattack in the form of ransomware or malware, or both, in the previous 12 months, and in many cases, more than a dozen instances were reported by each entity. Of the respondents, 87 percent expect email-related security threats to either increase or significantly increase in the future. (Mimecast, 2017).

In the Mimecast/HIMSS survey, respondents left no doubt as to the greatest source of data breaches in their organizations. As Figure 1 below shows, email gained more first-place votes than all other categories combined.

Figure 1: Major Sources of Data Breaches

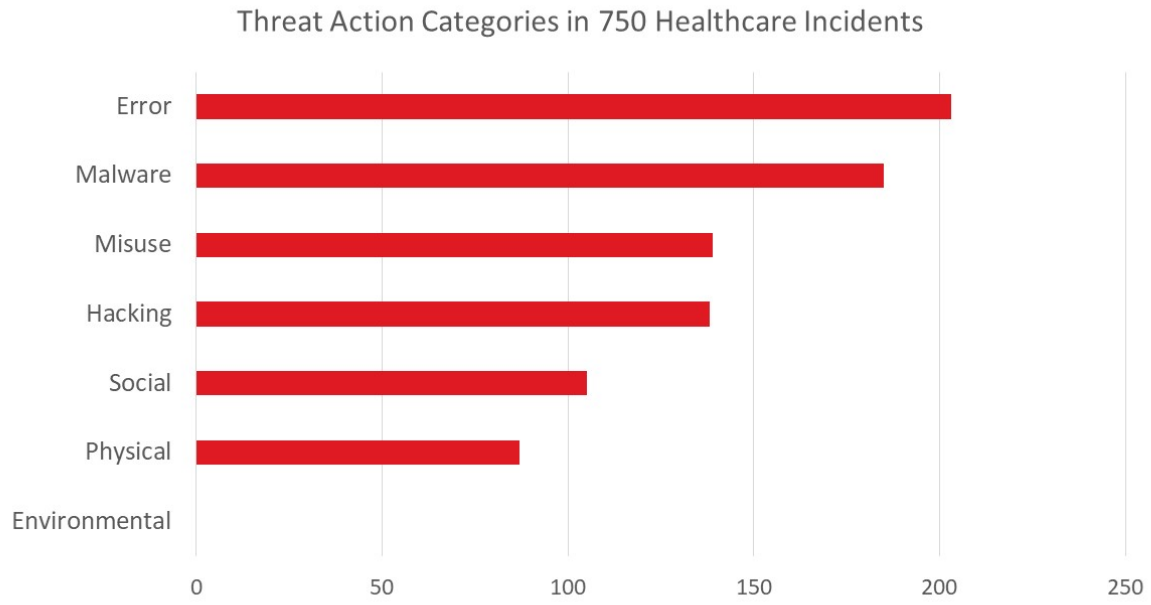


Source: Mimecast (2017, December 11). *Healthcare provider survey finds email most likely source of data breach.* [Web Blog]

So who are the threat actors? In an earlier whitepaper in this series titled, "A Culture of Security: Turning Your Greatest Threat into an Asset," we pointed out that the biggest breach threats a healthcare organization faces is not from malicious, external bad actors, but from inside the organization. In the Introduction of the Healthcare section of the 2018 Verizon Data Breach Investigations Report (from 2017 data) the report states the following: "The Healthcare vertical is rife with Error and Misuse. In fact, it is the only industry vertical that has more internal actors behind breaches than external. In addition to these problem areas, ransomware is endemic in the industry" (Verizon, 2018).

The Verizon report found that among the 750 breaches (536 with confirmed data disclosures) the threat actors were 43 percent external, 56 percent internal, 4 percent partners and 2 percent multiple parties. The top three patterns that were found in these breaches were miscellaneous errors, malware (ransomware accounts for 85 percent of that malware in healthcare) and privilege misuse, which together were implicated in 63 percent of the breaches. (See Figure 2 below.)

Figure 2: Threats in Healthcare



Source: Verizon. (2018). Data Breach Investigations Report.

The report notes that social engineering attacks, employing primarily phishing and pretexting "are a definite matter for concern," accounting for 14 percent of the incidents.

"Healthcare has a wide attack surface for social tactics due to the very nature of what they do," the Verizon report states. "Relatives and friends calling in to check on patients, third-party providers of equipment and services and so on can provide a social engineering criminal with a great deal of both opportunities and cover." (Verizon, 2018, p. 34)

Phishing emails are just one way in which bad actors take advantage of human failings to do evil. These failings also surface when people take actions such as choosing passwords, or determining whether they think a website is legitimate, both of which require decision making that rarely meets the security parameters most IT professionals would expect. You have to assume that your employees are under constant threat of being used by malicious actors on the outside to gain access to your systems, but you can't lose sight of the fact that they make mistakes internally that can also open the door. That's why the internal policies and protections you put in place are so important, and why they need to be continually reinforced.

The following is from Mimecast's "Top Five Tips for Better Email Security," based on the research from the HIMSS-conducted study:

1. "Train Employees on the Risks Inherent in Email: Real-time reminders are better than annual training.

2. Analyze Inbound Attachments: With multiple AV engines, safe file conversion and behavioral sandboxing.
3. Apply URL Checking: At the time a user clicks, not when it enters the organization.
4. Inspect Outbound Emails: For protected health information, other sensitive content and threats.
5. Increase Cyber Resilience: Against ransomware and other sources of data destruction with backup capabilities and continuity solutions" (Mimecast, 2017).

That last bit of advice gets to the question of, "What do we do once we have been compromised by a ransomware attack?" The following are a few examples from major healthcare breaches in 2017 that demonstrate the importance of continually backing up sensitive patient and operational data and keeping those backups out of the reach of cyber attackers.

- In mid-2017, Atlanta-based Peachtree Neurological Clinic reported it had been the victim of a ransomware attack that had potentially involved 176,295 individuals. Because it was able to restore the encrypted files through backup records, Peachtree refused to pay the ransom demanded by the attackers. During the investigation of the incident, Peachtree officials learned that their systems had been breached for 15 months, from February of 2016 to May of 2017. (Snell, 2017)

- Texas-based Urology Austin was hit by a ransomware attack on January 22, 2017 that involved information of 279,663 individuals, including patient names, addresses, birthdates, social security numbers and medical information. Urology Austin had maintained current backups of patient information and was able to use them to recover, empowering them to refuse the ransom demand. (Snell, 2017)

In another major ransomware attack in 2017 of Michigan-based Airway Oxygen that may have affected the information of a half-million individuals, company President Stephen Nyhuis released a statement, part of which provides further valuable security tips:

> "Since learning of the incident, we immediately took steps to secure our internal systems against further intrusion, including by scanning the entire internal system, changing passwords for users, vendor accounts and applications, conducting a firewall review, updating and deploying security tools, and installing software to monitor and issue alerts as to suspicious firewall log activity" (Snell, 2017).

When Your Electronic Health Record is Being Held Hostage

EHR unavailability, which will occur in every EHR-enabled healthcare environment, represents a significant potential patient safety hazard that directly affects patient care. Losing access to your electronic health record is more than just inconvenient; it can shut down your hospital or practice and put patients at risk. It can increase the risk of medication errors, make images unavailable, and lead to canceled procedures. Thus, the Office of the National Coordinator for Health Information Technology recommends that all healthcare institutions have a contingency plan in place that is developed and implemented by a contingency planning team. The team should include practicing clinicians who can help develop substitute workflows during downtimes. Complete instructions for such plans, including templates and worksheets are available online at https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html/. (ONC, 2017)

RANSOMWARE IS BECOMING INCREASINGLY SOPHISTICATED

Ransomware is not static – it is ever evolving. Whenever cyber criminals achieve success through their ransomware attacks, they use those means to create more sophisticated software designed to evade security measures.

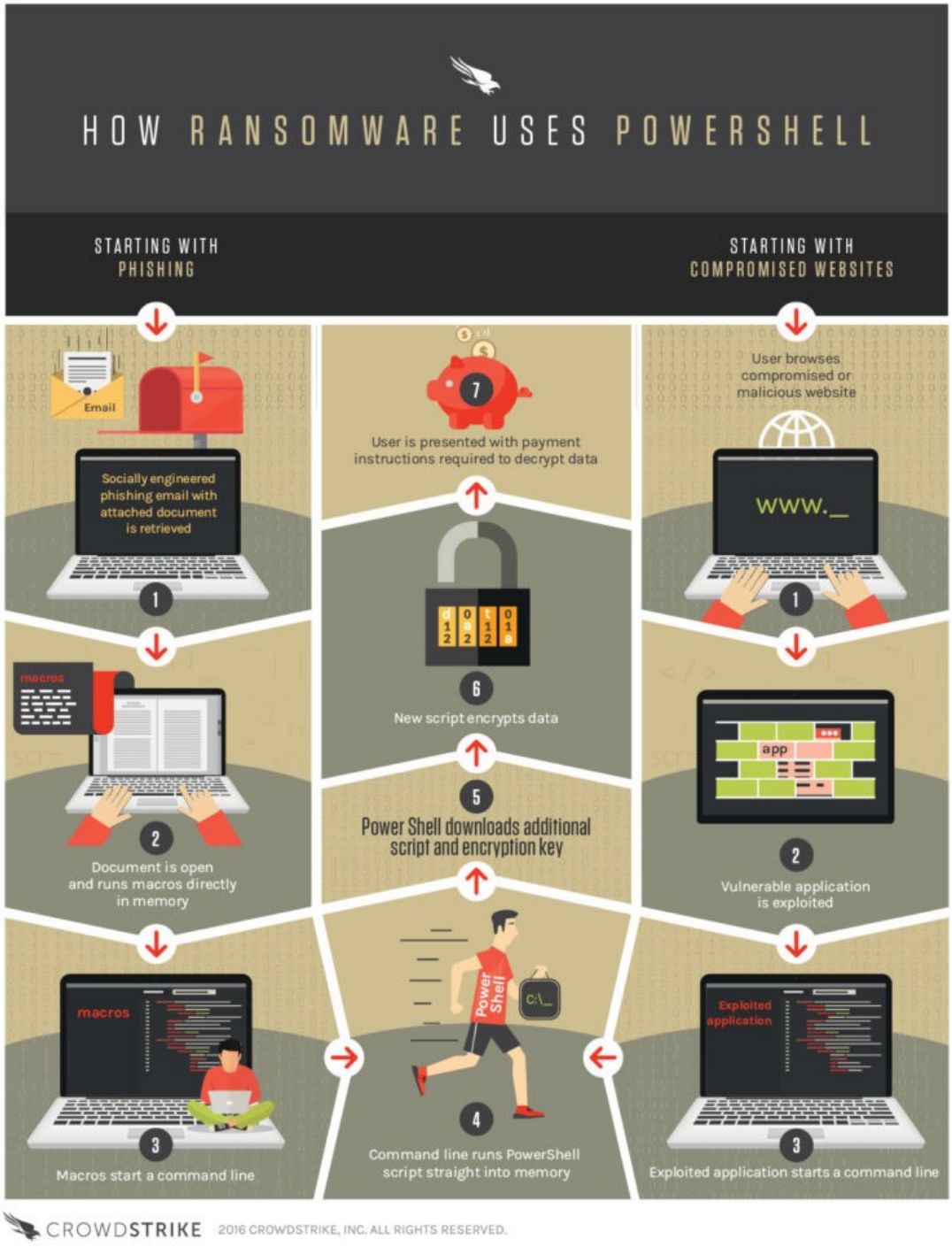
As we mentioned before, backing up your sensitive information is key to recovering from an attack, and thus, being ready for one. But don't assume your backups are safe. Cybercriminals can lock the backup, as well. Locky, for instance, erases Volume Shadow Copy files, a Windows feature that backs up files as people work on them (Zetter 2016).

A ransomware program called Cerber can even evade detection from machine learning tools, making the file appear safe. It can also jump into stealth mode and turn itself off if it senses detection and analysis of its code (Davis, 2017, March 29).

ICITech warns that because today's ransomware can propagate through a network and freeze all equipment, it could be used to target specialized equipment like CT and MRI scanners as well as patient devices like infusion pumps (ICITech, 2017).

Other experts warn of new ransomware variants, such as fileless ransomware. This enables cybercriminals to embed the malware in a native scripting language or straight into memory through PowerShell, bypassing the need to download code onto a user's computer (Figure 3).

Figure 3: How Ransomware Uses PowerShell



YOU HAVE BEEN ATTACKED: TIME TO PAY UP?

So you have been attacked. Time to start doling out the bitcoins, right? According to the FBI, this is not a good strategy and it strongly recommends against paying the ransom. However, many healthcare entities ignore the FBI's advice. Several studies find that most companies pay when they are victims of an attack, and some companies are now even stockpiling bitcoins, just in case. While it's not clear how much hospitals have paid to cyber-extortionists, the FBI estimates that businesses, as a whole, shelled out $209 million in the first quarter of 2016 alone because of ransomware attacks (Fitzpatrick, 2016; Simonite, 2016).

After all, it's tempting to pay up when your hospital has no working email, and fax and paper have replaced computers for everything from test results to treatment orders, and the media is demanding answers. In healthcare, time isn't just money, it's lives (Wharton, 2016).

Healthcare entities aren't alone in their rush to get their systems back online. A recent IBM study found that 70 percent of all businesses attacked by ransomware pay out—a propensity that might have had the potential to net Internet blackmailers $1 billion or more in 2017 (IBM Security Intelligence, 2016).

But, as the FBI warns, paying up can backfire. Plus, it encourages criminals to try their scheme again, possibly on you. Don't hold out hopes of finding the criminals; their demand for ransom in digital currency makes them nearly impossible to track. And, because the average payment is relatively small, it's unlikely that the FBI or Justice Department will get involved despite their pleas to businesses to report a breach. The former requires a loss costing at least $5,000 but probably won't get involved until losses hit at least $100,000; the latter requires about $50,000 (IBM Security Intelligence, 2016).

Remember, just because you pay the ransom doesn't mean you'll get your data back. According to HHS, some victims who paid were then required to pay again to get the promised decryption key (Manning, 2016).

If you've been attacked, the FBI recommends the following steps:

1. Immediately secure backup data or systems by taking them offline. Ensure backups are free of malware.
2. Contact law enforcement immediately, ideally a local field office of the FBI or Secret Service to report a ransomware event and request assistance.
3. If available, collect and secure partial portions of the ransomed data that might exist.
4. If possible, change all online account passwords and network passwords after removing the system from the network. Furthermore, change all system passwords once the malware is removed from the system.
5. Delete registry values and files to stop the program from loading. (US Justice Department, 2016)

Clearly, cyber extortion has become the threat du jour for healthcare entities. As with any hostage situation, the decision on whether or not to pay is an individual one. The best defense, of course, is a good offense. Follow this cybersecurity whitepaper series to learn more about creating that offense.

REFERENCES

Kaspersky Lab. (2017). Kaspersky Lab Threat Predictions for 2018. Retrieved at: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07164714/KSB_Predictions_2018_eng.pdf/.

Chalfant M. (2017, March 19). Health industry plays catch-up on cybersecurity. *The Hill*. Available at: http://thehill.com/business-a-lobbying/323081-health-industry-plays-catch-up-on-cybersecurity/.

Davis, J. (2017, March 20). Ransomware rising, but where are all the breach reports? *Healthcare IT News*. Available at: http://www.healthcareitnews.com/news/ransomware-rising-where-are-all-breach-reports/.

Davis, J. (2017, March 29) Updated Cerber ransomware can hide from machine learning tools. *Healthcare IT News.* March 29, 2017. Available at: http://www.healthcareitnews.com/news/updated-cerber-ransomware-can-hide-machine-learning-tools.

Davis, J. (2018, January 15). Ransomware attack on Hancock Health drives providers to pen and paper. *Healthcare IT News*. Available at: http://www.healthcareitnews.com/news/ransomware-attack-hancock-health-drives-providers-pen-and-paper/.

Davis, J. (2018, January 26). Allscripts sued over ransomware attack, accused of 'wanton' disregard. *Healthcare IT News*. Available at: http://www.healthcareitnews.com/news/allscripts-sued-over-ransomware-attack-accused-wanton-disregard/.

Davis, J. (2018, April 26). Ransomware attack against California provider breaches data of 85,000 patients. *Healthcare IT News*. Available at: http://www.healthcareitnews.com/news/ransomware-attack-against-california-provider-breaches-data-85000-patients/.

Department of Health and Human Services, Office for Civil Rights. (2016) *Fact Sheet: Ransomware and HIPAA.* Available at: https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html/.

Experian. (2017). *Data Breach Industry Forecast*. Available at https://www.experian.com/assets/data-breach/white-papers/2018-experian-data-breach-industry-forecast.pdf/.

Fitzpatrick, D. (2016, April 15) Cyber-extortion losses skyrocket, says FBI. *CNN Money.* Available at: http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/.

IBM Security Intelligence. (2016) *Ransomware: How Consumers and Businesses Value Their Data.* Available at: https://securityintelligence.com/media/ransomware-report/.

Institute for Critical Infrastructure Technology (ICITech). (2017). *How to Crush the Health Sector's Ransomware Pandemic*. Retrieved from: http://icitech.org/icit-analysis-how-to-crush-the-health-sectors-ransomware-pandemic/.

Manning, M. (2016, September 7). Tampa FBI: Your business is going to get hacked. *Tampa Bay Journal.* https://www.bizjournals.com/tampabay/news/2016/09/07/tampa-fbi-your-business-is-going-to-get-hacked.html/.

Mimecast (2017, December 11). Healthcare provider survey finds email most likely source of data breach. [Web blog]. https://www.mimecast.com/blog/2017/12/email-the-biggest-source-of-data-breach/.

Office for Civil Rights, Department of Health and Human Services. (2018, January) *Cyber Awareness Newsletter*: Cyber Extortion. Retrieved from: https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html/.

Simonite, T. (2016, June 7) Companies are stockpiling bitcoin to pay off cybercriminals. *MIT Technology Review*. Available at: https://www.technologyreview.com/s/601643/companies-are-stockpiling-bitcoin-to-pay-off-cybercriminals/.

Snell, E. (2017, December 11). Healthcare ransomware attacks contribute to 2017 top data breaches. *Health IT Security*. Available at: https://healthitsecurity.com/news/healthcare-ransomware-attacks-contribute-to-2017-top-data-breaches/.

Verizon. (2017). *Data Breach Investigations Report*. Retrieved from: https://www.verizonenterprise.com/verizon-insights-lab/dbir/.

Verizon. (2018). *Data Breach Investigations Report*. Retrieved from: https://www.verizonenterprise.com/verizon-insights-lab/dbir/.

Wharton, University of Pennsylvania. (2016, February 24). Hollywood Presbyterian: Is this only the beginning? Knowlege@Wharton. Available at: http://knowledge.wharton.upenn.edu/article/whitehside-yeo-hollywood-presby-ransomware/.

U.S. Justice Department. (2016). *How to Protect Your Networks from Ransomware*. Available at: https://www.justice.gov/criminal-ccips/file/872771/download/.

Zetter, K. (2016, March 30) Why hospitals are the perfect targets for ransomware. *WIRED*. Available at: https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/.