

Fall 2017

# Ransomware in Healthcare Facilities: The Future is Now

Nikki Spence

David P. Paul III

Alberto Coustasse

*Marshall University*, [coustassehen@marshall.edu](mailto:coustassehen@marshall.edu)

Follow this and additional works at: [http://mds.marshall.edu/mgmt\\_faculty](http://mds.marshall.edu/mgmt_faculty)

 Part of the [Computer Engineering Commons](#), [Health and Medical Administration Commons](#), [Health Information Technology Commons](#), and the [Management Information Systems Commons](#)

---

## Recommended Citation

Spence, N., Paul III, D. P., & Coustasse, A. (2017, September). Ransomware in healthcare facilities: The future is now. Paper presented at the Academy of Business Research, Fall 2017 Conference. Atlantic City, NJ.

This Conference Proceeding is brought to you for free and open access by the Management, Marketing and MIS at Marshall Digital Scholar. It has been accepted for inclusion in Management Faculty Research by an authorized administrator of Marshall Digital Scholar. For more information, please contact [zhangj@marshall.edu](mailto:zhangj@marshall.edu), [martj@marshall.edu](mailto:martj@marshall.edu).

# Ransomware in Healthcare Facilities: The Future is Now

Nikki Spence  
Marshall University  
Healthcare Administration Program  
Marshall University  
College of Business  
South Charleston WV

David P. Paul, III  
Professor Emeritus of Marketing and Healthcare Management  
Monmouth University  
Leon Hess School of Business  
West Long Branch, NJ 07764  
(302) 227-1930  
[dpaul@monmouth.edu](mailto:dpaul@monmouth.edu)

and

Alberto Coustasse  
Professor of Healthcare Administration  
Marshall University  
College of Business  
100 Angus E. Peyton Drive  
South Charleston, WV 25303  
(304) 746-1968  
(304) 746-2063 FAX  
[coustassehen@marshall.edu](mailto:coustassehen@marshall.edu)

# HEALTHCARE FACILITIES: ANOTHER TARGET FOR RANSOMWARE ATTACKS

---

## ABSTRACT

*Ransomware is a type of malware used by cyber criminals who encrypt files and then extort money in return for unlocking those files. Without adequate disaster recovery and backup plans, many businesses are forced to pay the ransom. We examine recent ransomware infections in healthcare settings, the liabilities and cost associated with such infections, and discuss possible risk mitigation tactics. Risks associated with ransomware attacks on healthcare facilities include financial, future business loss and damage to reputation. Healthcare facilities should have a disaster plan with adequate data backups and educate employees who are the usual sources of ransomware attacks.*

---

## INTRODUCTION

Ransomware refers to a type of malware used by attackers that first encrypts files and then attempts to extort money in return for the key to unlock the files by demanding a “ransom” (Bridges, 2008). These ransoms are most often demanded in the form of bitcoins, a type of cryptocurrency. When using bitcoins, transactions are irreversible, there is also a low fee of approximately \$0.043 USD per transaction, and the owner of a particular bitcoin account can remain anonymous (Angel and McCabe, 2015). Due to bitcoin’s ability to make transactions easy while protecting the anonymity of those involved, it has become the preference currency for criminal activity including ransomware hackers (Schneider, 2014; Swartz, 2017). According to a November 2015 report by the Cyber Threat Alliance, a single ransomware variant - CryptoWall 3 - was responsible for 406,887 attempted infections and \$325 million in damages since it was discovered in January 2015 (Kumar, 2015). Based upon these financial estimates, it is believed that new variants of this version of ransomware and other ransomware approaches are certainly being developed and released (McCarthy, 2016). In fact, one estimate reports the number of new ransomware variants being developed as 100,000 a day (Pollock, 2016)!

In the past, ransomware of attacks had primarily been used to target individuals; however, criminals have the ability to not only encrypt the files on an individual victim’s local computer, but they can also encrypt networked files to which that user had access. This makes organizations a more lucrative target for cybercriminals (Bridges, 2008). In fact, according to the U.S. Department of Health and Human Service Office for Civil Rights' Breach Portal, which displays breaches of health data that affect 500 or more people, over 325,000 healthcare data breaches were reported (Arndt, 2017)

Ransomware is typically spread through fake emails that have been designed by the hacker to appear legitimate (Mustaca, 2014). These emails may contain a link to an infected website or include an attachment such as a Word document that contains macros. Once a link is clicked or a document is opened, it downloads and infects the machine quickly: estimates vary from seconds (Correa, 2017; NFF, 2017) to 20 minutes (Cybereason, 2016). During this time, the malware searches the hard drive, network files, external drives, and cloud drives for all files that can be encrypted. After encryption, a “key” is required to unlock the files; this key is saved by the hacker, and this key is not released until the victim pays a requested amount or “ransom” (Mustaca, 2014).

Prior to 2016, healthcare organizations were not thought to be a primary target for ransomware (McCarthy, 2016). However, hospitals have become an easy target for hackers, for two reasons: (1) the necessity for computer-stored information associated with patient care (e.g., electronic medical records) and (2) the security holes in information technology (IT) systems. In fact, a report from Ponemon Institute, in 2016 stated that 89% of healthcare organizations suffered at least one data breach involving the loss of patient data over a 2-year period, and 45% had more than 5 such breaches. In addition, the frequency of successful hacking of patient medical files increased from 55% in 2015 to 64% in 2016. When hit with ransomware, some hospitals have been desperate to pay the ransom due

to their need to provide critical care to patients with the most up-to-date information such as drug interaction, care directives, and medical history (Zetter, 2016a).

Ransomware has made it easy for hackers to attack hospitals due to their sudden adaptation of IT without a concomitant increase in the number and sophistication of IT support staff. This adaptation occurred after the government allocated funds for Meaningful Use, which was used to encourage the use of EHRs. With the Meaningful Use incentive, EHR utilization has increased from 9.4% in 2008 to 96.9% in 2014 (ONC, 2015).

With such a substantial increase in IT utilization in a short time frame, many healthcare facilities have been unable to adopt adequate network and other information technology resources to combat potential attacks (Verizon, 2016). Without adequate resources, many hospitals simply do not have the staff to provide simple barriers to hackers such as prompt installation of patches. According to a 2016 report by Verizon, 85% of successful exploits take advantage of vulnerabilities such as outdated patches.

The purpose of this study was to determine the extent of recent ransomware infections in the healthcare setting, the risk liabilities and cost associated with infections, and to determine possible risk mitigation tactics.

## METHODOLOGY

The primary hypothesis of this research was: in the event of a ransomware attack, hospitals may suffer significant profit loss if they are not properly prepared with adequate information technology resources and business continuity/disaster recovery policies.

The methodology for this study was a literature review. The method used, shown in Figure 1, is an adaptation of the conceptual framework by Yao, et al., which illustrates the factors of a ransomware attack and how they promote or discourage these attacks. The ransomware process starts with a cybercriminal targeting a hospital. When the ransomware is detected by the hospital, a decision must be made to pay the ransom if they had not previously planned for such an attack and were not able to use disaster recovery methods to restore data. If payment is made to the cybercriminal, this promotes hackers to use ransomware attacks and other criminals while proper disaster recovery and risk mitigation discourages the ransomware process.

The study was conducted in three stages: (1) identifying literature and collecting data (2) analyzing and evaluating the literature, and (3) categorizing the literature found.

### *Step 1: Literature Identification and Collection*

The key terms ‘ransomware’ and ‘healthcare’ or ‘information security’ or ‘disaster recover’ or ‘cost’ were searched through scholarly electronic databases. Databases included of PubMed, Academic Search Premier, ProQuest, and Google Scholar. Reputable websites of the Federal Bureau of Investigations and the International Association of Privacy Professionals were also reviewed.

### *Step 2: Literature Analysis*

The literature review generated 29 sources. Since ransomware has only recently become an issue in healthcare information technology (IT), searches were limited to articles published between 2005 and 2017 in the English language.

A semi-structured interview was conducted on August 26, 2016 with Paul Smith, a lawyer who is an expert in healthcare legal concerns. In addition, a personal communication was accompanied on August 31, 2016 with Dennis Lee, a Chief Information Officer who is an expert in healthcare information technology (Appendix A & B). The professionals are referred to as an “Expert in Healthcare Law” and an “Expert in Healthcare Information Technology” throughout the review. The literature search was conducted by NS and validated by AC, who acts as second reviewer and double checked that references met the research study inclusion criteria.

### *Step 2: Literature Categorization*

Original articles, reviews and research studies including primary and secondary data were included. Relevant articles were selected after a review of the abstracts was performed in order to determine if they were relevant to the research criteria. The findings are presented in the following results and categorized under the major subheadings of “Details of Previous Ransomware Events,” “Risk Liabilities and Cost of a Ransomware Attack,” and “Risk Mitigation and Information Security.”

## RESULTS

The rate of ransomware incidents has been growing, not just in the healthcare industry, but for all enterprise industries. The FBI estimated that by the end of 2016, monetary loss due to ransomware be over \$1 billion (Brewer, 2016). The number of ransomware variants has been also increasing: according to a 2016 Symantec report, there was a 250% increase in the number of ransomware variants from 2013 to 2014 (Savage, Coogan and Lau, 2015). More than 4 million ransomware variants were detected in the first quarter of 2015, including 1.2 million new ones, compared to fewer than 1.5 million total samples in the third quarter of 2013, when fewer than 400,000 were new (Brewer, 2016). Interestingly, McAfee Labs (2016) has predicted that ransomware attacks will peak in 2017 and decline thereafter, but others (Ashford, 2017; Butler, 2016b; Liska, 2017; Muncaster, 2016; Sustar, 2016) do not share in this optimism, believing instead that ransomware attacks will increase in both number and sophistication in 2018 and thereafter, at least until a solution to the problem is found and applied on a widespread basis. In an analysis of internet traffic in 2016 of the US, Bitdefender, an internet security software firm, found that over 61.8% of malicious internet files were found to contain some form of ransomware (Arsene and Gheorghe, 2016).

### Details of previous ransomware events

The first documented case of hospital ransomware was at Surgeons of Lake County in 2012. A similar attack occurred two years later in 2014 at Clay County Hospital. In both events, the extent of ransomware attack was not detailed; a ransom was believed to be paid in both cases, but the amounts were never disclosed (HIPAA Journal, 2016).

However, it was not until the highly publicized (Mogg, 2016; Waddell, 2016; Winton, 2016a) ransomware attack at Hollywood Presbyterian Medical Centre in February of 2016 that hackers actively began to target healthcare facilities. In this attack, staff was unable to access patient records, X-rays, and other equipment, or to restore equipment from backup data and was forced to pay the ransom (Goldsborough, 2016). Initial reports claimed that the criminal initially demanded a ransom of \$3.6 million but the ransom was negotiated down to approximately \$17,000 or 40 bitcoins (Network Security Journal, 2016).

Paying a ransom, however, did not ensure that cybercriminals will provide the encryption key for the locked files. In the case of Kansas Heart Hospital, the ransom was paid, but the key was not provided. Instead, the cybercriminals demanded a second, larger ransom, which was not paid (Jayanthi, 2016).

After the success of the ransomware attack on Hollywood Presbyterian Medical Centre, the healthcare industry was targeted more frequently, with two hospitals attacked later that month and five hospitals targeted the next month. These affected hospitals did not pay the ransom, but instead were able to restore information from their backups (Network Security Journal, 2016). Ransomware attacks on other hospitals and health systems quickly followed within a month (see Table 1).

### *Risk Liabilities and Cost of a Ransomware Attack*

According to an interviewed legal expert (Expert in Healthcare Law, personal communication, 2016, see Appendix A), there have been four risk categories associated with ransomware attacks: medical malpractice, data privacy, property, reputation, and cost and expenses issues. Although medical malpractice has been a regular concern for hospitals, there could be an additional risk of medical malpractice during a ransomware attack if patient care would be impacted or a patient was harmed as a result of ransomware: for example, if there was a medication error on a patient when the Computerized Prescription Order Entry (CPOE) system was down.

In a 2013 study the effects of CPOE on medication errors, data was pooled from the 2006 American Society of Health-System Pharmacists Annual Survey, the 2007 American Hospital Association Annual Survey, and the 2008

Electronic Health Record Adoption Database in order to approximate the reduction in medication errors that occur when using CPOE. This study found that CPOE reduced the rate of errors by 48%. If a hospital relying on a CPOE system was to lose that system due to whatever cause(s), the rate of prescription errors associated with returning to a manual prescription would increase substantially, perhaps doubling, especially during the forced transition when individuals who were familiar with the CPOE system had to be re-trained or trained to use the manual system (Radley et al., 2013).

The second threat has been the risk of patient data privacy loss, which could then lead to a HIPAA violation. During the first response to a breach, it is important for staff to identify, if possible, the type of malware that has infected their network. After the malware has been identified, professionals should assess what risks that particular malware has and if a solution to decrypt the files can be found (Lee, 2016; Sternstein, Maser and Nelson, 2016). Unfortunately, decryption without the necessary key is extremely unlikely and there are no free tools currently available to decrypt files (Cyber Point and Europol, 2016; Kennedy, 2017).

The risk of reputation loss and loss of future business were calculated in an annual study by the Ponemon Institute (2012), which examined cost related to 49 companies in the US and interviewed 400 individuals. This study found that, in 2011, the companies interviewed averaged over \$3 million in losses related to reputation loss, abnormal turnover of customers, increased customer acquisition activities and diminished goodwill. In a follow up study (Ponemon, 2016), 24% of companies surveyed expressed concern that their reputation would be diminished if they were to suffer a ransomware attack.

The final risk is cost and expense losses. In 2015, the average total cost of a data breach was \$4 million (IBM Global Technology Services, 2016). The average cost per record spent in the healthcare industry in 2014 was \$355, which would be a substantial amount for a large or small hospital to pay per record (IBM Global Technology Services, 2014). This may or may not include additional costs associated with a data breach which could vary when size of the organization and number of patients affected is considered. Such variable costs include credit monitoring per patient which may cost anywhere from \$8 to \$30 per person, depending on the level of monitoring needed (Identity Theft Protection Association, 2012).

If the institution chooses to pay the ransom, the average ransom demanded has been approximately \$10,000 for enterprises and \$700 for individuals. In a report published by cyber data and security vendor Imperva, attackers have often tailored the ransom to which country the affected institution is located. For example, the average demanded ransomware cost in the United States has been \$700; however, in countries such as Israel, Russia, and Mexico, the average price has been \$500. For this reason, companies in more developed nations such as the US are more popular targets as they are believed to be able to afford to pay a greater ransom (Everett, 2016).

### **Risk mitigation and information security**

The IBM Security Services Cyber Security Intelligence Index, an annual report compiled with the results of forensic investigations into the security incidents of the year, detailed events of over 1,000 of IBM Security Services clients in over 133 countries in 2014. The findings of the report showed that in 2014, over 95% of all investigated security incidents were attributed to “human error” with the most common reason being a user clicked a malicious attachment or unsafe web link (IBM Global Technology Services, 2014).

At the 2016 Cryptography and Information Security-Related conference, a cybersecurity event, 200 information security professionals who attended were interviewed. The results of the interview showed that 58% of those interviewed reported their company had seen an increase in spear phishing in the last year. Spear phishing – sending an e-mail which appears to originate from a high-ranking member of the organization (Butler, 2016a) – has a much higher chance (70%) of being successful than simply sending an e-mail with an attachment on which the receiver can click to open (1-3%) (Mangelsdorf, 2017). Of those interviewed, 52% did not feel confident that their executives could successfully identify a phishing scam and 58% expected that their company had seen more spear phishing attempts in the previous year (Boose, 2016).

Employees are often the “entry point” for ransomware (Andt, 2017b). Based upon a survey of 618 individuals in small to medium-sized organizations who have responsibility for containing ransomware infections in their organization, 58% reported that negligent employees put their company at risk of a ransomware attack, while only

29% were very confident (9%) or confident (20%) that their employees would be able to detect risky links or sites that could result in a ransomware attack (Carbonite, 2017). In an empirical study conducted by PhishMe, 8 million simulated phishing emails were sent to 3.5 million enterprise employees. In this study, 87% of employees who opened the malicious attachment did so within the day. Of the users that clicked the malicious files in the initial email, 67% opened a malicious file again when sent a second simulated phishing email (Anonymous, 2016). This risk could obviously be mitigated by better employee education. One company, KnowBe4, was able to decrease the number of employees who clicked on a potential phishing scam from 15.9% to 1.2% (Zetter, 2016b).

Data backup has proven a critical step for any prevention plan: without a way to restore the encrypted files, businesses may have no choice but to pay the ransom in order to continue business (Siwicki, 2016). However, when it comes to ransomware attacks, it has not enough to simply backup data. Data must also be backed up in such a manner that the backup process itself is not connected to computers or networks, lest the backup also become encrypted and held for ransom. One example of this would be to physically store the information offline or in a cloud storage solution not attached to the network. Some instances of ransomware have even been known to seek out and destroy network backups (Zetter, 2016a), making the offsite physical storage of backup data even more important to prevent the backups from contamination. For years, many studies (e.g., Backblaze, 2015; Heat Software, 2016; Titan, 2016) have suggested a 3-2-1 approach to backup: have at least 3 copies of the data, utilize two different media formats, and have one of the copies be offsite (Backblaze, 2015; Heat Software, 2016; Titan, 2016). Veeam (2016) suggested adding an additional level of security (3-2-1-1), store one of the media offline, and allowing the implementation of an offline or semi-offline copy of the data. However, backups suffer from several inherent problems. While it would be a viable option to restore data that has not been frequently accessed, but they are always be a “snapshot in time,” they will always be behind current data; i.e., some most current data will virtually always be lost (Tuttle, 2016). Also, if a digital backup was not quickly available, at least some, if not many, staff could be unfamiliar with “paper” forms, potentially further impeding patient treatment (Cox, 2016). Finally, because cybercriminals recognize that many organizations are moving their backups to the cloud, eventually a way may be found to attack this also (Phillips, 2017; Spector, 2016).

## DISCUSSION

Results showed that if a ransomware attack is successful, healthcare providers can face substantial financial and even clinical consequences. Proper risk mitigation and disaster recovery are crucial to reduce costs and the likelihood of data loss.

During a ransomware attack, information systems are shut down and staff members suffer from a denial of access to key information systems that they have relied on for decision making. Following a successful attack, providers would likely notice a substantial increase in medication errors associated with the CPOE. This, and other built-in EHR functionality (e.g., current medications or medication allergies, are likely to result in increased errors by staff and impaired decision-making capabilities by physicians, resulting in increased liability for both the institution and the healthcare clinicians.

Some potential costs that may be incurred by an organization during and after an attack are the cost of an initial response team, the loss of potential business while the response team restores backup data and installs new equipment, and cost associated if a call center must be temporary set up to answer patient questions about the attack. Hospitals could also suffer actual damage to hospital property. In terms of ransomware, property damage may be any software, hardware, or EHR records that are lost or damaged during the attack. Equipment items such as servers could be so damaged with malware that there is no way to recover them which will then result in further costs to the hospital (Expert in Healthcare Information Technology, personal communication, 2016, see Appendix B). Fortunately, to date no patient deaths have been reported due to a ransomware attack on a hospital, although concerns about the possibility of such an occurrence abound (Condliffe, 2017; Scott and Perlroth, 2017. Wong and Salon, 2017). However, the consequences of any patient death due to a ransomware attack are sufficiently severe that the Food and Drug Administration has begun to co-ordinate with other federal agencies regarding how to best respond should one occur (Sheber, 2017).

If only for business continuity reasons, it is very important for healthcare facilities large and small to have a disaster recovery plan with steps in place to recover from any malware attack. Not only must a business have this plan, but also have an adequate storage for data that does not include networked backups. Businesses must also make

sure to test backups regularly to ensure information is being saved correctly and can be restored. Without this, businesses have limited options during a ransomware incident to either pay the ransom or to completely lose all data (Expert in Healthcare Information Technology personal communication, 2016, see Appendix B).

Although data backup and a recovery plans are essential, efforts should obviously be made to prevent an attack before it starts. Users have been identified as the weakest link for hackers, and user education as well as adequate detection of policy violations have the potential to make a significant difference in deterring risky end user behavior that makes a network vulnerable to attack. One specific suggestion regarding how to prevent users from inadvertently exposing hospitals to a ransomware attack is to prohibit individuals from opening personal e-mails using one of the facility's computers, because "an organization's internal e-mail client is likely to have more sophisticated spam filters than web-based providers such as Gmail and Hotmail (Butler, 2016a)." Unfortunately, convincing busy physicians and healthcare staff to avoid this practice would be difficult, at best.

If the ransomware only encrypted files and did not steal information, it may not have been considered a HIPAA breach. However, if the ransomware also stole patient data before it encrypted it, there would be many factors to determine if this had been a HIPAA violation. One factor to determine if a HIPAA breach occurred is what data media and equipment had been infected and if those devices had been encrypted at rest. This means that if a server with patient information just encrypted information being transmitted and not the information on the server, this information could be subject to theft and a HIPAA violation. If the server was encrypted at all times, even at rest, this would not be considered a breach if criminals copied the information since they would not be able to access the files (Expert in Healthcare Law personal communication, 2016, see Appendix A).

Notwithstanding financial losses, one of the biggest concerns for hospitals should be reputation loss. Much of the costs associated with an attack can be recovered by cyber security insurance. Hospital reputation, however, and the loss of public trust in the facility can result in irreparable harm and profit loss if patients decide to go to another hospital. With the loss of business, smaller hospitals simply would not be able to afford to stay in business long after an attack (Expert in Healthcare Law personal communication, 2016, see Appendix A).

## **Limitations**

The literature review was limited by search strategy. This publication bias, along with the restricted number of databases utilized, may have constrained the contents of the review. Researcher bias may have also been present which could have limited the review.

Another limitation of this study was the lack of current research that exists for ransomware in the healthcare settings. Little in-depth research has been conducted to determine the average cost per attack. Without this research information, the study relied on data from other business fields and expert interview information which may or may not be applicable to the average healthcare facility during and after a ransomware attack.

Due to how new the topic of ransomware is in healthcare, research information was also limited on what long-term consequences, effects, and damages a healthcare facility may face after a ransomware attack. There was also no available information on the impact to a business if a ransom was paid versus if the business was able to complete a full data recovery from backups. This information would have been useful to illustrate the benefits and challenges associated with both outcomes.

## **Practical implications**

Due to the recent payment of ransoms in 2016 by Hollywood Presbyterian Medical Centre and Kansas Heart Hospital, it is possible that in the future, the healthcare industry will not only be a major target for additional ransomware attacks, but will also become a target for other cybercriminal hacks such as other types of malware or denial of service. If the majority of healthcare facilities refuse to pay the ransom, this trend may decrease in time, but this seems unlikely. The downside risk to cybercriminal appears slight, as no convictions have been noted in the literature, and the upside gain is substantial.

In addition, if ransomware is able to take advantage of the patient data, the anticipated trend in cyberattacks on healthcare facilities could potentially become a larger issue. Although currently ransomware does not appear to

have been developed specifically to view patient information and therefore would not be a HIPAA concern, this may not continue to be the case in the future. If a server or computer is not encrypted at rest and only encrypted during incoming and outgoing transactions, a ransomware virus could be adapted to exploit this vulnerability and copy the information on the server. If this were to happen, the provider would be open to all the previously mentioned costs in addition to the cost associated with HIPAA data breach violations as well.

Hackers would also be able to leverage the public release of patient information to the hospital for a higher ransom to facilities. In this case, these facilities might be even more willing to pay the ransom. If successful, this would, of course, also certainly lead to an increase in ransomware attacks on healthcare facilities.

## CONCLUSION

The number of ransomware attacks and variants has increased in recent years. Healthcare has become a major target for these attacks and in response to this increase it is crucial that they develop a proper disaster recovery plan and properly educate their users on information security. With proper planning in place, a healthcare facility is not only more likely to survive an attack but to also decrease costs associated with them and to mitigate the risk of reputation loss.

## REFERENCES

Angel, James J. and Douglas McCabe (2015), "The Ethics of Payments: Paper, Plastic, or Bitcoin?" Journal of Business Ethics, 132 (3), 603-611.

Anonymous (2016), "Employees Prone to Phishing," Computer Fraud & Security, (1), 3.

Arndt, Rachel (2017), "Emory Healthcare Cyberattack Affects 80,000 Patient Records," Modern Healthcare, March 2, 2017, downloaded 3/3/17 from [http://www.modernhealthcare.com/article/20170302/NEWS/170309983?utm\\_source=modernhealthcare&utm\\_medium=email&utm\\_content=20170302-NEWS-170309983&utm\\_campaign=am](http://www.modernhealthcare.com/article/20170302/NEWS/170309983?utm_source=modernhealthcare&utm_medium=email&utm_content=20170302-NEWS-170309983&utm_campaign=am)

Arsene, Liviu and Alexandra Gheorghe (2016), "Ransomware: A Victim's Perspective - A Study on US and European Internet Users," Bitdefender, downloaded 5/11/17 from [https://www.bitdefender.com/media/materials/white-papers/en/Bitdefender\\_Ransomware\\_A\\_Victim\\_Perspective.pdf](https://www.bitdefender.com/media/materials/white-papers/en/Bitdefender_Ransomware_A_Victim_Perspective.pdf)

Ashford, Warwick (2017), "Ransomware Expected to Dominate in 2017," ComputerWeekly, January 6, 2016, downloaded 5/6/17 from <http://www.computerweekly.com/news/450410530/Ransomware-expected-to-dominate-in-2017>

Backblaze (2015), "The 3-2-1 Backup Strategy," downloaded 6/7/17 from <https://www.backblaze.com/blog/the-3-2-1-backup-strategy/>

Boose, Shelley (2016), "Tripwire RSA Survey: Only 38 Percent of Security Professionals Confident in Ransomware Recovery," Tripwire, downloaded 2/21/17, from <http://www.businesswire.com/news/home/20160324005065/en/Tripwire-RSA-Survey-38-Percent-Security-Professionals>

Bridges, Lloyd (2008), "The Changing Face of Malware," Network Security, (1), 17-20.

Brewer, Ross (2016), "Ransomware Attacks: Detection, Prevention and Cure," Network Security, volume 2016 (9), 5-9.

Butler, Mary (2016a), "Tips for Preventing and Responding to a Ransomware Attack," Journal of AHRIMA, Apr 1, 2016, downloaded 2/21/17 from <http://journal.ahima.org/2016/04/01/tips-for-preventing-and-responding-to-a-ransomware-attack/>

Butler, Mary (2016b), "Ransomware and Hacking Attempts against Healthcare Expected to Increase in Severity, Scope," Journal of AHIMA, Nov 21, 2016, downloaded 2/21/17 from <http://journal.ahima.org/2016/11/21/ransomware-and-hacking-attempts-against-healthcare-expected-to-increase-in-severity-scope/>

Condliffe, Jamie (2017), "Widespread Ransomware Attack Hits U.K. Hospitals," MIT Technology Review, May 12, 2017, downloaded 6/7/17 from <https://www.technologyreview.com/s/607863/widespread-ransomware-attack-hits-uk-hospitals/>

Carbonite (2017), "The Rise of Ransomware," Ponemon Institute, downloaded 5/7/17 from <http://www.ponemon.org/local/upload/file/Ransomware%20Report%20Final%201.pdf>

Correa, Rick (2017), "How Fast Does Ransomware Encrypt Files? Faster than You Think," Barkly, downloaded 5/5/17 from <https://blog.barkly.com/how-fast-does-ransomware-encrypt-files>

Cox, John Woodrow (2016), "MedStar Health Turns Away Patients After Likely Ransomware Cyberattack," Washington Post [online], March 29, 2016, downloaded 5/11/17 from [https://www.washingtonpost.com/local/medstar-health-turns-away-patients-one-day-after-cyberattack-on-its-computers/2016/03/29/252626ae-f5bc-11e5-a3ce-f06b5ba21f33\\_story.html?utm\\_term=.db23ab524b05](https://www.washingtonpost.com/local/medstar-health-turns-away-patients-one-day-after-cyberattack-on-its-computers/2016/03/29/252626ae-f5bc-11e5-a3ce-f06b5ba21f33_story.html?utm_term=.db23ab524b05)

Cybereason (2016), "Ransomware Decoded: Free Behavioral-Based Ransomware Blocking by Cybereason," December 16, 2016, downloaded 5/5/17 from <https://www.cybereason.com/labs-blog/cybereason-introduces-free-behavioral-based-ransomware-blocking/>

Cyber Point and Europol (2016), "Ransomware: What You Need to Know," Europol Public Information, downloaded 5/12/17 from [file:///C:/Users/owner/AppData/Local/Temp/ransomware-what\\_you\\_need\\_to\\_know.pdf](file:///C:/Users/owner/AppData/Local/Temp/ransomware-what_you_need_to_know.pdf)

Everett, Cath (2016), "Ransomware: To Pay or Not to Pay?" Computer Fraud & Security, (4), 8-12.

Goldsborough, Reid (2016), "Protecting Yourself from Ransomware," Teacher Librarian, 43 (4), 70-71.

Heat Software (2016), "Ransomware: The Fight Back Starts Now," downloaded 6/7/17 from [https://heatsoftware.com/wp-content/uploads/2016/12/Ransomware\\_The\\_Fight\\_Back\\_Starts\\_Now-.pdf](https://heatsoftware.com/wp-content/uploads/2016/12/Ransomware_The_Fight_Back_Starts_Now-.pdf)

HIPAA Journal (2016), "Mobile Device Ransomware Warnings Becoming More Urgent," downloaded 8/2/16, from <http://www.hipaajournal.com/mobile-device-ransomware-warnings/>

BM Global Technology Service (2014), IBM Security Services 2014 Cyber Security Intelligence Index, downloaded 10/22/16, from [http://media.scmagazine.com/documents/82/ibm\\_cyber\\_security\\_intelligenc\\_20450.pdf](http://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf)

IBM Global Technology Service (2016), IBM Security Services 2016 Cyber Security Intelligence Index. downloaded 10/22/16, from <http://www-03.ibm.com/security/data-breach/>

Identity Theft Protection Association (2012), Credit Monitoring Services, downloaded 11/26/16, from <http://www.businessidtheft.org/Resources/PersonalCreditProtection/CreditMonitoringServices/tabid/114/Default.aspx>

Jayanthi, Akanksha (2016), "Kansas Heart Hospital Pays Ransom, Then Hackers Came Back for More," Becker's Health IT and CIO Review [online], May 23, 2016, downloaded 5/6/17 from <http://www.beckershospitalreview.com/healthcare-information-technology/kansas-heart-hospital-pays-ransom-then-hackers-came-back-for-more.html>

Kumar, Mohit (2015), "CryptoWall Ransomware raised \$325 Million in Revenue for Its Developer," The Hacker News, October 30, 2015, downloaded 5/5/17 from <http://thehackernews.com/2015/10/cryptowall-ransomware.html>

Landi, Heather (2016), "Kentucky-Based Methodist Hospital's System Restored Following Ransomware Attack Last Week," Healthcare Informatics, March 21, 2016, downloaded 5/11/17 from <https://www.healthcare->

informatics.com/news-item/kentucky-based-methodist-hospital-s-system-restored-following-ransomware-attack-last-week

Lee, Brian (2016), "Ransomware: Unlocking the Lucrative Criminal Business Model," Palo Alto Networks, downloaded 5/12/17 from [https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en\\_US/resources/research/ransomware-report](https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/research/ransomware-report)

Liska, Allan (2017), "7 Ransomware Trends to Watch for in 2017," Recorded Future, downloaded 5/6/17 from <https://www.recordedfuture.com/ransomware-trends-2017/>

Kennedy, Carrie (2017), "Ransomware and Healthcare: What You need to Know," OnLine Tech, downloaded 5/12/17 from <http://resource.onlinetech.com/ransomware-facts-and-figures/>

Mangelsdorf, Martha E. (2017), "What Executives Get Wrong about Cybersecurity," MIT Sloan Management Review, 58 (2), 22-24.

McAfee Labs (2016), "McAfee Labs Explores Top Threats Expected in the Coming Year," Intel Security, November 2016, downloaded 5/6/17 from <https://www.mcafee.com/us/resources/reports/rp-threats-predictions-2017.pdf>

McCarthy, Jack (2016), "Ransomware to Wreak Havoc in 2016, ICIT Study Says," Healthcare IT News, March 21, 2016, downloaded 5/5/17 from <http://www.healthcareitnews.com/news/ransomware-wreak-havoc-2016-icit-study-says>

Mogg, Trevor (2016), "Hollywood Hospital Pays \$17,000 to Ransomware Hackers," Digital Trends, February 18, downloaded 4/23/17 from <http://www.digitaltrends.com/computing/hollywood-hospital-ransomware-attack/>

Muncaster, Phil (2016), "New Ransomware Families to Rise 25% in 2017," InfoSecurity Magazine [online], December 6, 2016, downloaded 5/6/17 from <https://www.infosecurity-magazine.com/news/new-ransomware-families-to-rise-25/>

Mustaca, Sorin (2014), "Are your IT Professionals Prepared for the Challenges to Come?" Computer Fraud & Security, (3), 18.

Network Security Journal (2016), "Ransomware Expands, Attacks Hospitals and Local Authorities, and Moves to New Platforms," Network Security, volume 2016, (3), 1-2.

NFF (2017), "Ransomware: Understand the Threat. Know the Risks. Protect the Enterprise," NFF: Delivering Net Results, downloaded 5/5/17 from <http://www.nffinc.com/ransomware/done>

Office of the National Coordinator for Health Information Technology [ONC] (2015), "Adoption of Electronic Health Record Systems among U.S. Non-Federal Acute Care Hospitals: 2008-2014," ONC Data Brief No. 23, April 2015, downloaded 4/23/17 from <https://www.healthit.gov/sites/default/files/data-brief/2014HospitalAdoptionDataBrief.pdf>

Phillips, Gavin (2017), "Yes, Ransomware Can Encrypt Your Cloud Storage," MUQ: Security, May 29, 2017, downloaded 6/7/17 from <http://www.makeuseof.com/tag/cloud-drive-ransomware/>

Pilieci, Vito (2016), "Ottawa Hospital Hit with Ransomware, Information on Four Computers Locked Down," National Post [online], March 13, 2016, downloaded 5/11/17 from <http://news.nationalpost.com/news/canada/ottawa-hospital-hit-with-ransomware-information-on-four-computers-locked-down>

Pollock, Doug (2016). "Data Racketeering: When Ransomware Holds our Business Hostage," The Privacy Advisor, April 25, downloaded 8/27/16, from <https://iapp.org/news/a/data-racketeering-when-ransomware-holds-your-business-hostage/>

Ponemon Institute (2012), "2011 Cost of Data Breach Study: United States," downloaded 11/26/16, from [www.ponemon.org/local/upload/file/2011\\_US\\_CODB\\_FINAL\\_5.pdf](http://www.ponemon.org/local/upload/file/2011_US_CODB_FINAL_5.pdf)

Ponemon Institute (2016), "Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data," downloaded 5/8/17 from <file:///E:/Spring%202017/Research%20Projects/Alberto%202017/Ransomware%20and%20hospitals/Poneman%20Ransomware%20Report%20Final%202017.pdf>

Radley, David C., Melanie R. Wasserman, Lauren E. W. Olsho, Sarah J. Shoemaker, Mark D. Spranca and Bethany Bradshaw (2013), "Reduction in Medication Errors in Hospitals Due to Adoption of Computerized Provider Order Entry Systems," Journal of the American Medical Informatics Association, 20 (3), 470-476.

Reed, Tina (2016), "MedStar Took 'Extreme' Measures to Block Cyber Threat," Washington Business Journal [online], March 29, 2016, downloaded 5/11/17 from <http://www.bizjournals.com/washington/news/2016/03/29/medstar-took-extreme-approach-to-block-security.html>

Savage, Kevin, Peter Coogan and Hon Lau (2015), "Security Response: The Evolution of Ransomware," Symantec, downloaded 10/28/16, from [http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/the-evolution-of-ransomware.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf)

Schneider, Zachary (2014), "Bitcoin: Why is it Prone to Criminal Activity?" Law Street Media, February 17, 2014, downloaded 5/4/17 from <https://lawstreetmedia.com/news/bitcoin-why-is-it-prone-to-criminal-activity/>

Scott, Mark and Nicole Perlroth (2017), "With Ransomware, It's Pay and Embolden Perpetrators, or Lose Precious Data," The New York Times [online], May 17, 2017, downloaded 6/7/17 from [https://www.nytimes.com/2017/05/17/technology/bitcoin-ransomware-pay-lose-data.html?\\_r=0](https://www.nytimes.com/2017/05/17/technology/bitcoin-ransomware-pay-lose-data.html?_r=0)

Sheber, Sarah (2017), "Industry Keeping a Weather Eye for Medical Device, Ransomware Hacks," Journal of AHRIMA, Health IT, downloaded 4/22/17 from <http://journal.ahima.org/2017/04/20/industry-keeping-a-weather-eye-for-medical-device-ransomware-hacks/>

Siwicki, Bill (2016), "Tips for Protecting Hospitals from Ransomware as Cyberattacks Surge," downloaded 8/27/16, from <http://www.healthcareitnews.com/news/tips-protecting-hospitals-ransomware-cyber-attacks-surge>

Spector, Lincoln (2016), "How to Stop Ransomware: Backup Can Protect You, But Only If You Do It Right," PC World [online], May 6, 2016, downloaded 6/7/17 from <http://www.pcworld.com/article/3056907/security/how-to-stop-ransomware-backup-can-protect-you-but-only-if-you-do-it-right.html>

Sternstein, Jon, John Maser and Peter Nelson (2016), "The Rise of Ransomware," The North Carolina Healthcare Information & Communications Alliance, Inc., downloaded 5/12/17 from <https://nchica.org/wp-content/uploads/2016/06/Sternstein-Maser-Nelson-1.pdf>

Sustar, Lee (2016), "Ransomware 2017: Dead or Alive?" SC Magazine [online], December 7, 2016, downloaded 5/6/17 from <https://www.scmagazine.com/ransomware-2017-dead-or-alive/article/577732/>

Swartz, Jon (2017), "Bitcoin Ransomware Demand Shows Criminal Links Are Hard to Shake," USA Today [online], May 15, 2017, downloaded 6/8/17 from <https://www.usatoday.com/story/tech/news/2017/05/15/bitcoin-ransomware-hacking-prices/101711854/>

Symantec (2016), "Special Report: Ransomware and Businesses 2016," Symantec, downloaded 2/21/17 from <https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/ransomware-and-businesses-16-en.pdf>

Titan (2016), "Ransomware Protection: Why the 3-2-1 Backup Strategy Works," TitanHQ Blog, downloaded 6/7/17 from <https://www.titanhq.com/blog/ransomware-protection-why-the-3-2-1-backup-strategy-works>

Tuttle, Hilary (2016), "Ransomware Attacks Pose Growing Threat," Risk Management, 63 (4), 4.

Veeam (2016), “7 Practical Tips to Prevent Ransomware Attacks on Backup Storage,” downloaded 6/7/17 from <https://www.veeam.com/blog/tips-to-prevent-ransomware-protect-backup-storage.html>

Verizon (2016), Verizon Data Breach Investigation Report, downloaded 9/3/16, from <http://www.verizon.com/about/news/2016-data-breach-report-info/>

Waddell, Kaveh (2016), “A Hospital Paralyzed by Hackers,” The Atlantic [online], February 17, downloaded 4/23/17 from <https://www.theatlantic.com/technology/archive/2016/02/hackers-are-holding-a-hospitals-patient-data-ransom/463008/>

Winton, Richard (2016a), “Hollywood Hospital Pays \$17,000 in Bitcoin to Hackers; FBI Investigating,” Los Angeles Times [online], February 12, downloaded 4/23/17 from <http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html>

Winton, Richard (2016b), “2 More Southland Hospitals Attacked by Hackers Using Ransomware,” Los Angeles Times [online], March 22, 2016, downloaded 5/11/17 from <http://www.latimes.com/local/lanow/la-me-ln-two-more-so-cal-hospitals-ransomware-20160322-story.html>

Wong, Julia Carrie and Olivia Solon (2017), “Massive Ransomware Cyber-Attack Hits Nearly 100 Countries Around the World,” The Guardian [online], May 12, 2017, downloaded 6/7/17 from <https://www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs>

Zetter, Kim (2016a), “Why Hospitals Are the Perfect Targets for Ransomware,” Wired, downloaded 8/27/16, from <https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/>

Zetter, Kim (2016b), “4 Ways to Protect Against the Very Real Threat of Ransomware,” Wired, downloaded 8/27/16, from <https://www.wired.com/2016/4-ways-protect-ransomware-youre-target/>

Table: Details of Ransomware Events in Healthcare Immediately Following the Hollywood Presbyterian Medical Centre Incident

Hospital	Data Affected	Action Taken	Source
February 10, 2016 Lukas Hospital Neuss, Germany	Shutdown of all systems due to email attachment	No ransom paid, systems restored via backups and a few hours of data lost	Network Security Journal (2016)
February 12, 2016 Klinikun Arnsbury North Rhine-Westphalia, Germany	Detected on of 200 servers, network shut down to prevent infection	No ransom paid, systems restored via backups and a few hours of data lost	Network Security Journal (2016)
March 14, 2016 Ottawa Hospital,Canada	Four computers encrypted	No ransom paid, restored from backups	Pilieci, (2016)
March 18, 2016 Prime Health Care: Chino Valley Medical Center & Desert Valley Hospital Victorville, CA	Number of computers had locked data and some hospital servers	No ransom paid, backups restored	Winton (2016b)
March 21, 2016 Methodist Hospital Henderson, KY	Critical files encrypted	No ransom paid, systems restored via backups	Landi, (2016)
March 28, 2016 Medstar Health Baltimore, MD (a 10 hospital system)	No breach in patient data, but email and clinical support systems were unavailable	45 bitcoin ransom demanded (\$19,000) but no ransom paid	Reed (2016)

#### APPENDIX A

Questions asked in a Semi-Structured Interview of Paul Smith, VP/General Counsel, Cabell Huntington Hospital, Huntington, WV, an Expert in Healthcare Law, August 26, 2016

- What are some of the legal implications involved with a ransomware incident?
- If the hospital is unable to provide key services what legal actions can be taken?
- How would a ransomware incident at a hospital's business associate affect the hospital?
- Would a ransomware attack be considered a HIPAA breach?
- How are criminals prosecuted in the case of a ransomware attack?

#### APPENDIX B

Questions asked in a Personal Communication of Dennis Lee, VP/CIO, Cabell Huntington Hospital, Huntington, WV, an Expert in Healthcare Information Technology, on August 31, 2016

- What do you think is the most likely avenue for a ransomware attack at a healthcare facility (ex: email phishing)?
- In the event of a ransomware attack, what are the procedures for response?
- What costs would be associated with response and recovery?
- What are some important aspects of a malware prevention plan?
- In your opinion, when a hospital suffers a ransomware attack would this be concerned a HIPAA breach?