Ransomware in Healthcare Facilities: A Harbinger of the Future?

by Nikki Spence, MS; Niharika Bhardwaj, MBBS, MS; David P. Paul III, DDS, PhD; and Alberto Coustasse, DrPH, MD, MBA, MPH

Abstract

Cybercriminals have begun to target the healthcare industry with ransomware, malware that encrypts an infected device and any attached devices or network drives. After encryption, cybercriminals demand a ransom before releasing the devices from encoding. Without adequate disaster recovery and backup plans, many businesses are forced to pay the ransom. We examined the extent of recent ransomware infections in healthcare settings, the risk liabilities and costs associated with such infections, and possible risk mitigation tactics. The methodology of this study was a literature review. The review was limited to sources published in English from 2005 to 2017. Of the 118 sources found, 74 were used in the results section. We also performed two semistructured interviews, one with an expert in health care law and the other with a chief information officer from a local teaching hospital who was an expert in healthcare information technology. Financial costs associated with business recovery after ransomware attacks on healthcare facilities are significant and are growing in both magnitude and scope. Other risks are a loss of future business and reputation damage. Research has suggested that the best plan of action is to have a proper business continuity and disaster plan with adequate data backups and to be vigilant in educating employees about the sources of ransomware to prevent potential attacks.

Keywords: cost; cyberattacks; hospitals; health information security; ransomware

Introduction

The term *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 unlocking the data by demanding a ransom.[1, 2] These ransoms are most often requested in the form of bitcoins, a type of cryptocurrency. When using bitcoins, transactions are irreversible and have a low fee of approximately USD 0.043 per operation, and the owner of a particular bitcoin account can remain anonymous.[3] Because of the ability of bitcoin to make transactions accessible while protecting the anonymity of those involved, it has become the preferred currency for criminal activity, including that of ransomware hackers.[4] According to a November 2015 report by the Cyber Threat Alliance, a single ransomware variant—Crypto Wall 3—was responsible for 406,887 attempted infections and $325 million in damages since it was discovered in January 2015.[5, 6] In light of these financial estimates, researchers believe that new variants of this version of ransomware and other ransomware approaches are probably being developed and released.[7] In fact, one assessment reports that new ransomware variants are developed at a rate of 100,000 a day.[8]

In the past, ransomware attacks were primarily used to target individuals; however, criminals can encrypt not only the files on an individual victim's local computer but also the networked data to which that user had access. This makes organizations a more lucrative target for cybercriminals.[9] In fact, according to the US Department of Health and Human Services Office for Civil Rights' Breach Portal,

which displays breaches of health data that affect 500 or more people, more than 325,000 healthcare data breaches have been reported until February of 2017.[10]

Ransomware is typically spread through fake emails that have been designed by the hacker to appear legitimate.[11] 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, the malware is downloaded and infects the machine quickly: estimates vary from seconds[12, 13] to 20 minutes.[14] During this time, the malware searches the hard drive, network files, external drives, and cloud drives for all data that can be encrypted. After encryption, an electronic "key" is required to unlock the files; this key is saved by the hacker and is not released until the victim pays a requested amount or ransom.[15]

Before 2016, healthcare organizations were not thought to be a primary target for ransomware.[16] However, 14 hospitals had become the target of ransomware and a total of 173 hacking/information technology (IT) incident data breaches had been officially reported by October 16, 2016, [17, 18] Hospitals have become an easy target for hackers for two reasons: (1) the necessity of computer storage of information associated with patient care (e.g., electronic medical records) and (2) the security holes in IT systems.[19] In fact, a report from Ponemon Institute in 2016 stated that 89 percent of healthcare organizations suffered at least one data breach involving the loss of patient data over a two-year period, and 45 percent had more than five such breaches.[20, 21] Also, the frequency of successful hacking of patient medical files increased from 55 percent in 2015 to 64 percent in 2016.[22] When hit with ransomware, some hospitals have been desperate to pay the ransom because of their need for the most up-to-date information, such as drug interactions, care directives, and medical history, in order to provide critical care to patients.[23] Accordingly, the healthcare industry is now considered to be at a substantial risk of a ransomware attack,[24] mainly because it trails other leading industries in securing vital data.[25, 26]

Hackers have found it easy to attack hospitals with ransomware because of hospitals' rapid adoption of IT without a concomitant increase in the number and sophistication of IT support staff. This IT adoption occurred after the government allocated funds for the Meaningful Use program, which encouraged the use of electronic health records (EHRs). With the Meaningful Use incentives, EHR utilization increased from 9.4 percent in 2008 to 96.9 percent in 2014.[27]

With such a substantial increase in IT utilization in a short time frame, many healthcare facilities have been unable to adopt adequate network security and other information technology resources to combat potential attacks.[28] Without sufficient funds, many hospitals do not have the staff to employ simple barriers to hackers, such as the quick installation of electronic patches. According to a 2016 report by Verizon, 85 percent of successful exploits take advantage of vulnerabilities such as old patches.[29]

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

Methodology

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

The methodology of this study was an extensive and detailed literature review. The research design was an adaptation of the research framework used by Yao et al. (2010)[30] and depicts the factors related to a ransomware attack and how they promote or discourage these attacks. The ransomware process starts with a cybercriminal targeting a hospital. When the hospital staff detects the ransomware, a decision must be made to pay the ransom if the staff 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, it encourages hackers and other criminals to use ransomware attacks, whereas proper disaster recovery and risk mitigation discourage the ransomware process (shown in Figure 1). Because the emphasis of this review was on the use of new technology in healthcare settings, this research framework was suitable for the

current study. The internal validity of this research framework, as well as the literature review framework, has been supported by its effective utilization in prior studies.[31–34]

The research 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" or "cyber attack" and "healthcare" or "information security" or "disaster recovery" or "cost" were searched in scholarly electronic databases. Databases included PubMed, Academic Search Premier, ProQuest, and Google Scholar. The websites of the Federal Bureau of Investigations and the International Association of Privacy Professionals, along with certain reputable news websites, were also reviewed.

Step 2: Inclusion Criteria and Literature Analysis

The literature review generated 118 sources, of which 74 were used in the results section. Because ransomware has only recently become an issue in healthcare IT, searches were limited to articles published between 2005 and 2017 in the English language. Original articles, reviews, and research studies including primary and secondary data related to ransomware were included. Relevant articles were selected after the abstracts were reviewed to determine if they were related to the research criteria.

Step 3: Literature Categorization

The themes that emerged from the literature are presented in the results section and were categorized under the main categories of the research framework: detection of ransomware (details of previous ransomware events and cyberattacks on personal health information of healthcare facilities); risk mitigation and disaster recovery (risk mitigation and information security); and payment of ransom (risk liabilities and cost of a ransomware attack).

Additionally, two semistructured interviews were conducted, the first on August 26, 2016, with Paul English Smith, a lawyer who is an expert in healthcare legal concerns, and the second on August 31, 2016, with Dennis Lee, a chief information officer of a local teaching hospital (see Appendix A and Appendix B). These professionals are referred to as an "expert in healthcare law" and an "expert in healthcare information technology" throughout the review. These interviews were tape-recorded and transcribed. Appropriate answers were used in the study to support the findings from the literature and to provide more in-depth perspectives on the findings.

Results

The rate of ransomware incidents has been growing, not just in the healthcare industry, but in all enterprise industries. The FBI estimated that by the end of 2016, monetary losses due to ransomware totaled more than $1 billion.[35] The number of ransomware variants has also been increasing: according to a 2016 Symantec report, the number of ransomware variants increased 250 percent from 2013 to 2014.[36] 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.[37] Interestingly, McAfee Labs (2016) predicted that ransomware attacks would peak in 2017 and decline thereafter, but others did 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.[38–43] In an analysis of internet traffic in 2016 in the United States, Bitdefender, an internet security software firm, found that more than 61.8 percent of malicious internet files were found to contain some form of ransomware.[44]

Details of Previous Ransomware Events

The first documented case of hospital ransomware occurred 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 the ransomware attack was not reported; a ransom was believed to be paid in both cases, but the amounts were never disclosed.[45] However, it was not until the highly publicized ransomware attack at Hollywood Presbyterian Medical Center in February 2016 that hackers actively began to target healthcare facilities.[46–48] In this attack, the 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.[49] 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.[50]

Paying a ransom, however, does 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, more substantial ransom, which was not paid.[51]

After the success of the ransomware attack on Hollywood Presbyterian Medical Center, 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.[52] Ransomware attacks on other hospitals and health systems quickly followed within a month.[53–58] (See Table 1.)

Risk Liabilities and Cost of a Ransomware Attack

According to the legal expert whom we interviewed (see Appendix A), four risk categories are associated with ransomware attacks:

1. medical malpractice,
2. data privacy,
3. property and reputation, and
4. cost and expense 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 is affected or if a patient is harmed as a result of ransomware, for example, if a medication error affected a patient when the computerized prescription order entry (CPOE) system was down.[59] In a 2013 study of the effects of CPOE on medication errors, data were 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 to estimate the reduction in medication errors that occurs when CPOE is used. This study found that CPOE reduced the rate of errors by 48 percent.[60] Multiple other studies have provided evidence that CPOE minimizes medication errors.[61–63] If a hospital relying on a CPOE system were to lose that system for any reason, the number of prescription errors associated with returning to a manual prescription system would increase substantially, perhaps doubling, especially during a forced transition when individuals who were familiar with the CPOE system would have to be retrained or trained to use the manual method.[64]

The second threat has been the risk of patient data privacy loss, which could lead to a HIPAA violation. During the first response to a breach, it is vital for staff to identify, if possible, the type of malware that has infected their network. After the malware has been detected, professionals should assess the risks of that particular malware and whether a solution to decrypt the files can be found.[65, 66] Unfortunately, decryption without the necessary key is extremely unlikely, and no free tools are currently available to decrypt files.[67, 68]

The risk of reputation loss and loss of future business were calculated in an annual study that included interviews with 400 individuals and examined the costs related to these factors in 49 companies in the United States.[69] This study found that, in 2011, the organizations examined averaged more than $3 million in losses related to reputation loss, abnormal turnover of customers, increased customer

acquisition activities, and diminished goodwill. In a follow-up study, 24 percent of companies surveyed expressed concern that their reputation would be diminished if they were to suffer a ransomware attack.[70]

The final risk is losses due to costs and expenses. In 2016, the average total cost of a data breach was $3.62 million.[71] The average cost per record in the healthcare industry in 2014 was $355, which would be a substantial amount for a large or small hospital to pay per record.[72] This total may or may not include additional costs associated with a data breach, which could vary depending on the size of the organization and number of patients affected. Such variable costs include credit monitoring provided to patients, which may cost anywhere from $8 to $30 per patient, depending on the level of oversight needed.[73]

If the institution chooses to pay the ransom, the amount must be considered. The average ransom demanded has been approximately $10,000 for enterprises and $710 for individuals. In a report published by cyberdata and security vendor Imperva, attackers have often tailored the ransom to the country in which the affected institution is located. For example, the average ransom demand in the United States has been $710. However, in countries such as Israel, Russia, and Mexico, the average demand has been $500. For this reason, companies in more developed nations such as the United States are more favorite targets, as they are thought to be able to afford to pay a greater ransom.[74]

Cyberattacks on Personal Health Information in Healthcare Facilities

When ransomware accesses patient data, cyberattacks on healthcare facilities become a much more significant problem.[75] If a server or computer is not encrypted at rest and information is encrypted only during incoming and outgoing transactions, a ransomware virus could exploit this vulnerability and copy the information on the server.[76] 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.[77] In recent years, the number of cyberattacks on personal health information stored on the computer systems of healthcare facilities has been increasing rapidly; see Table 2 for an exhaustive review of recent ransomware attacks involving the unauthorized theft of patient health information.[78–84]

Although the extent of illegally obtained patient health information collected varies by institution and by attacker, most facilities noted the loss of patient names, addresses, telephone numbers, email addresses, dates of birth, IP addresses, marital status, race, provider information, patient Social Security numbers, health insurance numbers, and mental or health condition or treatment information. In 2016, 34.5 percent of all identity thefts occurred as a result of breaches through the healthcare sector, second only to the business sector, which accounted for 45.2 percent of identified violations. However, the number of identity theft breaches associated with the healthcare sector has grown more quickly than in any other industry for every year between 2010 and 2016.[85] A study from Johns Hopkins University in 2017 found that between October 21, 2009, and December 31, 2016, there were 1,798 data breaches. Among them were 257 breaches reported by 216 hospitals.[86] Clearly, cybercriminals have discovered the high vulnerability of healthcare facilities to cyberattack and the low risk involved. The stolen personal health information sold in 2014 for $10 per piece, about 10 or 20 times the value of a US credit card number, as it could be used to create fake IDs to buy medical equipment or drugs that can be resold, or combined with a false provider number to file made-up claims with insurers.[87]

Risk Mitigation and Information Security

One study analyzed the different types of ransomware (CryptoWall 3.0, CryptoLocker, CTB-Locker, TeslaCrypt, NK_, VO_, Locky) along with potential ransomware prevention methods (PC update, PC and server data backup, web page file and site safety checks, shared folder management, system security settings, read-only folder settings). It was noted that only PC updates and read-only folder settings worked effectively for all types of ransomware.[88]

The IBM Security Services Cyber Security Intelligence Index, an annual report compiling the results of forensic investigations into the security incidents of the year, reported specific events affecting more than 1,000 IBM Security Services clients in more than 133 countries in 2014. The findings of the report showed that in 2014, more than 95 percent of all investigated security incidents were attributed to “human error,” with the most common reason being a user’s click of a malicious attachment or unsafe web link.[89]

At the 2016 Cryptography and Information Security Conference, a cybersecurity event, 200 information security professionals who attended were interviewed. The results of the interview showed that 58 percent of those questioned reported that their company had seen an increase in spear phishing in the last year.[90] Spear phishing—sending an email that appears to originate from a high-ranking member of the organization[91]—has a much higher chance (71 percent) of being successful than just sending an email with an attachment that the receiver can click to open (1 to 3 percent).[92] Of those interviewed, 52 percent did not feel confident that their executives could successfully identify a phishing scam.[93]

Employees are often the "entry point" for ransomware.[94] Based on a survey of 618 individuals in small to medium-sized organizations who have responsibility for containing ransomware infections in their company, 58 percent reported that negligent employees put their organization at risk of a ransomware attack, while only 29 percent were very confident (9 percent) or confident (20 percent) that their employees would be able to detect risky links or sites that could result in a ransomware attack.[95] In an empirical study conducted by PhishMe, 8 million simulated phishing emails were sent to 3.5 million enterprise employees. In this study, 87 percent of employees who opened the malicious attachment did so within the day. Of the users who clicked the malicious files in the initial email, 68 percent exposed a malicious file again when they received a second simulated phishing email.[96] 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 percent to 1.2 percent.[97]

Data backup has proven to be a critical step in any prevention plan: without a way to restore the encrypted files, businesses may have no choice but to pay the ransom to continue doing business.[98] However, when it comes to ransomware attacks, merely backing up data is not enough. 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, making the offsite physical storage of backup data even more critical to prevent the backups from contamination.[99] For years, many studies have suggested a 3-2-1 approach to backing up: have at least three copies of the data, utilize two different media formats, and have one of the copies be off-site.[100–102] The software company Veeam suggested adding a level of security (3-2-1-1) by storing one of the media offline, creating an offline or semi-offline copy of the data.[103] However, backups suffer from several inherent problems. Although backups provide a viable option to restore data that are not frequently accessed, they are always a "snapshot in time" and will always be behind current data; that is, some of the most current data will nearly always be lost.[104] Also, the use of paper forms may be necessary if a digital backup is not quickly available, but at least some, if not many, staff could be unfamiliar with these forms, potentially further impeding patient treatment.[105] Finally, because cybercriminals recognize that many organizations are moving their backups to the cloud, eventually a way may be found to attack these backups also.[106, 107]

Recognizing this vulnerability, Lee et al. proposed a cloud-based system for preventing ransomware and reported that this system could perform real-time network, file, and server monitoring and data backups—thus improving detection and reducing the damage resulting from ransomware.[108] However, further research is needed before such systems are operationalized.

Discussion

The results of this study 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' work is hindered by the denial of access to crucial information systems that they rely on for decision making.

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 the cost associated with a call center if one must be temporarily set up to

answer patient questions about the attack. Hospitals could also suffer actual damage to hospital property. Property damage from ransomware may involve any software, hardware, or EHR records that are lost or damaged during the attack. Equipment such as servers could be so extensively damaged by malware that there is no way to recover them, which would then result in further costs to the hospital (expert in healthcare information technology interview; see Appendix B). Fortunately, to date, no patient deaths have been attributed to a ransomware attack on a hospital, although concerns about the possibility of such an occurrence abound.[109–111] However, the consequences of any patient death due to a ransomware attack are sufficiently severe that the Food and Drug Administration has begun to coordinate with other federal agencies regarding how best to respond should one occur.[112]

If only for business continuity reasons, it is crucial for healthcare facilities large and small to have a disaster recovery plan with steps in place to recover from any malware attack. In addition to establishing such a policy, businesses must also have adequate storage of data apart from networked backups. Companies must further make sure to test their backups regularly to ensure that the information is being saved correctly and can be restored. Without appropriate backups, businesses' options during a ransomware incident are limited to either paying the ransom or completely losing all data (expert in healthcare information technology interview; see Appendix B).

Although data backup and recovery plans are essential, efforts should 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, has 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 emails on 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."[113] Unfortunately, convincing busy physicians and healthcare staff to avoid this practice would be difficult, at best.

If ransomware only encrypts files and does not steal information, the attack may not be considered a HIPAA breach. However, if the ransomware also takes patient data before encoding it, many factors have to be considered to determine whether the attack constitutes a HIPAA violation. One factor in deciding if a HIPAA breach occurred is what data media and equipment were infected and whether those devices had been encrypted at rest. This means that if a server with patient information encrypts only the information being transmitted and not the information on the server, this information could be subject to theft, which would constitute a HIPAA violation. If the server were encrypted at all times, even at rest, it 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 interview; see Appendix A).

Notwithstanding financial losses, one of the most significant concerns for hospitals should be reputation loss. Much of the cost associated with an attack can be recovered by cybersecurity insurance. The hospital's reputation, however, and the damage 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 may not be able to afford to stay in business long after an attack (expert in healthcare law interview; see Appendix A).

Limitations

The literature review was limited by the search strategy. Publication bias, along with the restricted number of databases utilized, may have constrained the contents of the study. Researcher bias may have also have been present and could have limited the review. Another limitation of this study was the lack of current research on ransomware in healthcare settings. Presently, little in-depth analysis has been conducted to determine the average cost per attack. Without this information, this study relied on data from other business fields and expert interview information, which may or may not apply to the average healthcare facility during and after a ransomware attack.

Because ransomware is a relatively new concern in healthcare, information on the long-term consequences, effects, and damages that a healthcare facility may face after a ransomware attack was also limited. Also, no information was available on the different effects on a business if a ransom is paid

versus if the company is able to complete a full data recovery from backups. This information would have been useful to illustrate the benefits and challenges associated with each of these outcomes. It seems reasonable that the leadership of many healthcare facilities could be hesitant to admit publicly not only that their computer systems are vulnerable to a ransomware attack but that such an attack (or attacks) had been successful. To the extent that healthcare systems failed to publicly acknowledge attempted or successful ransomware attacks, the scope of the problem would be understated.

Future research should examine the effects attributable to ransomware in healthcare. A systematic review and or a meta-analysis should be performed to gain a more precise measurement of the effects (i.e., costs and consequences) of cyberattacks and ransomware in healthcare facilities.

Practical Implications

Because of the payment of ransoms in 2016 by Hollywood Presbyterian Medical Center and Kansas Heart Hospital, it is possible that in the future, the healthcare industry not only will be a significant target for additional ransomware attacks but also will become a target for other cybercriminal attacks, such as different types of malware or denial-of-service attacks, or that cybercriminals could target individual medical devices such as pacemakers,[114] especially those that are connected to internal networks.[115] If the majority of healthcare facilities refuse to pay the ransom, this trend may decrease over time, but this outcome seems unlikely because the risk to cybercriminals appears slight, given that no convictions have been reported, and the chance of gain for cybercriminals appears to be substantial.

Also, if ransomware can take advantage of patient data, the anticipated trend in cyberattacks on healthcare facilities could potentially become a more significant issue. Although ransomware does not currently appear to have been explicitly developed to view patient information and therefore an attack 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 is encrypted only during incoming and outgoing transactions, a ransomware virus could 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 costs associated with HIPAA data breach violations. Hackers would also be able to leverage the threat of public release of patient information to obtain a higher ransom from facilities. In this case, institutions might be even more willing to pay the ransom. If successful, such tactics would undoubtedly lead to an increase in ransomware attacks on healthcare facilities.

Recommendations

As stated by Chinthapalli (2017),[116] hospitals should have clear digital hygiene, with policies in place to remind employees that not all emails should be opened. Additionally, backups should be made daily (or up to every hour) using tape drives, which cannot be hacked digitally. Furthermore, hospitals should establish a ransomware policy detailing step by step the actions to be taken in the event of this crisis. Hospitals should be ready to deal with ransomware because many hospitals will unquestionably be affected by it in the near future.[117, 118]

Conclusion

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

Nikki Spence, MS, is an alumni of the health informatics program at Marshall University in Huntington, WV.

Niharika Bhardwaj, MBBS, MS, is an alumni of the health informatics program at Marshall University in Huntington, WV.

David P. Paul III, DDS, PhD, is a professor emeritus of marketing and healthcare management at Monmouth University in West Long Branch, NJ.

Alberto Coustasse, DrPH, MD, MBA, MPH, is a professor of healthcare administration at the Lewis College of Business, Marshall University in South Charleston, WV.

Notes

1. Mansfield-Devine, S. "Ransomware: Taking Businesses Hostages." *Network Security* 2016, no. 10 (2016): 8–17.
2. Pope, Justin. "Ransomware: Minimizing the Risks." *Innovations in Clinical Neuroscience* 13, nos. 11–12 (2016): 37.
3. Angel, James J., and Douglas McCabe. "The Ethics of Payments: Paper, Plastic, or Bitcoin?" *Journal of Business Ethics* 132, no. 3 (2015): 603–11.
4. Brown, Steven David. "Cryptocurrency and Criminality: The Bitcoin Opportunity." *The Police Journal: Theory, Practice and Principles* 89, no. 4 (2016): 327–39.
5. Kumar, Mohit. "CryptoWall Ransomware Raised $325 Million in Revenue for Its Developer. *The Hacker News*, October 30, 2015. Available at http://thehackernews.com/2015/10/cryptowall-ransomware.html (accessed May 5, 2017).
6. Richardson, Ronny, and Max North. "Ransomware: Evolution, Mitigation and Prevention." *International Management Review* 13, no. 1 (2017): 10.
7. McCarthy, Jack. "Ransomware to Wreak Havoc in 2016, ICIT Study Says." *Healthcare IT News*, March 21, 2016. Available at http://www.healthcareitnews.com/news/ransomware-wreak-havoc-2016-icit-study-says (accessed May 5, 2017).
8. Pollock, Doug. "Data Racketeering: When Ransomware Holds Our Business Hostage." *The Privacy Advisor*, April 25, 2016. Available at https://iapp.org/news/a/data-racketeering-when-ransomware-holds-your-business-hostage/ (accessed August 27, 2016).
9. Mansfield-Devine, S. "Ransomware: Taking Businesses Hostages."
10. Arndt, Rachel. "Emory Healthcare Cyberattack Affects 80,000 Patient Records." *Modern Healthcare*, March 2, 2017. Available at http://www.modernhealthcare.com/article/20170302/NEWS/170309983?utm_source=modernhealthcare&utm_medium=email&utm_content=20170302-NEWS-170309983&utm_campaign=am (accessed March 3, 2017).
11. Mustaca, Sorin. "Are Your IT Professionals Prepared for the Challenges to Come?" *Computer Fraud & Security*, no. 3 (2014): 18.
12. Correa, Rick. "How Fast Does Ransomware Encrypt Files? Faster Than You Think." *Barkly*, 2017. Available at https://blog.barkly.com/how-fast-does-ransomware-encrypt-files (accessed May 5, 2017).
13. NFF. "Ransomware: Understand the Threat. Know the Risks. Protect the Enterprise." *NFF: Delivering Net Results*, 2017. Available at http://www.nffinc.com/ransomware/done (accessed May 5, 2017).
14. Cybereason. "Ransomware Decoded: Free Behavioral-based Ransomware Blocking by Cybereason." December 16, 2016. Available at https://www.cybereason.com/labs-blogcybereason-introduces-free-behavioral-based-ransomware-blocking/ (accessed May 5, 2017).
15. Mustaca, Sorin. "Are Your IT Professionals Prepared for the Challenges to Come?"
16. McCarthy, Jack. "Ransomware to Wreak Havoc in 2016, ICIT Study Says."
17. Mansfield-Devine, Steve. "Leaks and Ransoms—the Key Threats to Healthcare Organisations." *Network Security* 2017, no. 6 (2017): 14–19.
18. US Department of Health and Human Services, Office of Civil Rights. "Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information." 2017. Available at https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (accessed November 26, 2017).
19. NFF. "Ransomware: Understand the Threat. Know the Risks. Protect the Enterprise."
20. Cybereason. "Ransomware Decoded: Free Behavioral-based Ransomware Blocking by Cybereason."
21. Gue, D'Arcy." Ponemon Study: Healthcare Aware of Security Threats, But Not Really Ready for Them." *Medsphere*, 2016. Available at http://www.medsphere.com/blog/ponemon-study-

healthcare-aware-of-security-threats-but-not-really-ready-for-them (accessed November 25, 2017).
22. PwC. *Managing Cyber Risks in an Interconnected World: Key Findings from the Global State of Information Security® Survey 2015*. Available at https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf (accessed November 25, 2017).
23. Zetter, Kim. "Why Hospitals Are the Perfect Targets for Ransomware." *Wired*, 2016. Available at https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/ (accessed August 27, 2016).
24. Sittig, Dean F., and Hardeep Singh. "A Socio-technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks." *Applied Clinical Informatics* 7, no. 2 (2016): 624.
25. Kruse, Clemens Scott, Benjamin Frederick, Taylor Jacobson, and D. Kyle Monticone. "Cybersecurity in Healthcare: A Systematic Review of Modern Threats and Trends." *Technology and Health Care* 25, no. 1 (2017): 1–10.
26. Mukherjee, Sy. "Why Health Care Is Especially Vulnerable to Ransomware Attacks." *Fortune: Health*, May 15, 2017. Available at http://fortune.com/2017/05/15/ransomware-attack-healthcare/ (accessed September 8, 2017).
27. Office of the National Coordinator for Health Information Technology. *Adoption of Electronic Health Record Systems among U.S. Non-Federal Acute Care Hospitals: 2008-2014* (ONC Data Brief No. 23). April 2015. Available at www.healthit.gov/sites/default/files/data-brief/2014HospitalAdoptionDataBrief.pdf (accessed April 23, 2017).
28. Verizon. *Verizon Data Breach Investigation Report*. 2016. Available at http://www.verizon.com/about/news/2016-data-breach-report-info/ (accessed September 3, 2016).
29. Ibid.
30. Yao, Wen, Chao-Hsien Chu, and Zang Li. "The Use of RFID in Healthcare: Benefits and Barriers." *Proceedings of the 2010 IEEE International Conference on RFID Technology and Applications (RFID-TA)* (2010): 128–34.
31. Coustasse, A., S. Tomblin, and C. Slack. "Impact of Radio-Frequency Identification (RFID) Technologies on the Hospital Supply Chain: A Literature Review." *Perspectives in Health Information Management* (Fall 2013).
32. Deslich, S., and A. Coustasse. "Expanding Technology in the ICU." *Telemedicine and e-Health* 20, no. 5 (2014): 485–92.
33. Porterfield, A., K. Engelbert, and A. Coustasse. "Electronic Prescribing: Improving the Efficiency and Accuracy of Prescribing in the Ambulatory Care Setting." *Perspectives in Health Information Management* (Spring 2014).
34. Bhardwaj, Niharika N., Bezawit Wodajo, Keerthi Gochipathala, David P. Paul III, and Alberto Coustasse. "Can mHealth Revolutionize the Way We Manage Adult Obesity?" *Perspectives in Health Information Management* (Spring 2017).
35. Brewer, Ross. "Ransomware Attacks: Detection, Prevention and Cure." *Network Security* 2016, no. 9 (2016): 5–9.
36. Savage, Kevin, Peter Coogan, and Hon Lau. *Security Response: The Evolution of Ransomware*. Symantec, 2015. Available at http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf (accessed October 28, 2016).
37. Brewer, Ross. "Ransomware Attacks: Detection, Prevention and Cure."
38. McAfee Labs. *McAfee Labs 2017 Threats Predictions*. November 2016. Available at https://www.mcafee.com/us/resources/ reports/rp-threats-predictions-2017.pdf (accessed May 6, 2017).
39. Ashford, Warwick. "Ransomware Expected to Dominate in 2017." *Computer Weekly*, January 6, 2017. Available at http://www.computerweekly.com/news/450410530/Ransomware-expected-to-dominate-in-2017 (accessed May 6, 2017).
40. Butler, Mary. "Ransomware and Hacking Attempt against Healthcare Expected to Increase in Severity, Scope." *Journal of AHIMA*, November 21, 2016. Available at

http://journal.ahima.org/2016/11/21/ransomware-and-hacking-attempts-against-healthcare-expected-to-increase-in-severity-scope/ (accessed February 21, 2017).
41. Liska, Allan. "7 Ransomware Trends to Watch for in 2017." *Recorded Future*, January 4, 2017. Available at https://www.recordedfuture.com/ransomware-trends-2017/ (accessed May 6, 2017).
42. Muncaster, Phil. "New Ransomware Families to Rise 25% in 2017." *Infosecurity Magazine*, December 6, 2016. Available at https://www.infosecurity-magazine.com/news/new-ransomware-families-to-rise-25/ (accessed May 6, 2017).
43. Sustar, Lee. "Ransomware 2017: Dead or Alive?" *SC Magazine*, December 7, 2016. Available at https://www.scmagazine.com/ransomware-2017-dead-or-alive/article/577732/ (accessed May 6, 2017).
44. Arsene, Liviu, and Alexandra Gheorghe. *Ransomware: A Victim's Perspective: A study on US and European Internet Users*. Bitdefender, 2016. Available at https://download.bitdefender.com/resources/files/News/CaseStudies/study/59/Bitdefender-Ransomware-A-Victim-Perspective.pdf (accessed May 11, 2017).
45. HIPAA Journal. "Mobile Device Ransomware Warnings Becoming More Urgent." 2016. Available at http://www.hipaajournal.com/mobile-device-ransomware-warnings/ (accessed August 27, 2016).
46. Ibid.
47. Ross, Jacqueline. "Cybersecurity: A Real Threat to Patient Safety." *Journal of PeriAnesthesia Nursing* 32, no. 4 (2017): 370–72.
48. Waddell, Kaveh. "A Hospital Paralyzed by Hackers." *The Atlantic*, February 17, 2016. Available at https://www.theatlantic.com/technology/archive/2016/02/hackers-are-holding-a-hospitals-patient-data-ransom/463008/ (accessed April 23, 2017).
49. Ibid.
48. Winton, Richard. "2 More Southland Hospitals Attacked by Hackers Using Ransomware." *Los Angeles Times*, March 22, 2016. Available at http://www.latimes.com/local/lanow/la-me-ln-two-more-so-cal-hospitals-ransomware-20160322-story.html (accessed May 11, 2017).
49. Ross, Jacqueline. "Cybersecurity: A Real Threat to Patient Safety."
50. Goldsborough, Reid. "Protecting Yourself from Ransomware." *Teacher Librarian* 43, no. 4 (2016): 70–71.
51. Jayanthi, Akanksha. "Kansas Heart Hospital Pays Ransom, Then Hackers Came Back for More." *Becker's Health IT and CIO Review*, May 23, 2016. Available at http://www.beckershospitalreview.com/healthcare-information-technology/kansas-heart-hospital-pays-ransom-then-hackers-came-back-for-more.html (accessed May 6, 2017).
52. Network Security Journal. "Ransomware Expands, Attacks Hospitals and Local Authorities, and Moves to New Platforms." *Network Security*, no. 3 (2016): 1–2. 53. Ibid.
54. Jayanthi, Akanksha. "Kansas Heart Hospital Pays Ransom, Then Hackers Came Back for More."
55. Pilieci, Vito. "Ottawa Hospital Hit with Ransomware, Information on Four Computers Locked Down." *National Post*, March 13, 2016. Available at http://news.nationalpost.com/news/canada/ottawa-hospital-hit-with-ransomware-information-on-four-computers-locked-down (accessed May 11, 2017).
56. Winton, Richard. "2 More Southland Hospitals Attacked by Hackers Using Ransomware."
57. Landi, Heather. "Kentucky-based Methodist Hospital's System Restored Following Ransomware Attack Last Week." *Healthcare Informatics*, March 21, 2016. Available at https://www.healthcare-informatics.com/news-item/kentucky-based-methodist-hospital-s-system-restored-following-ransomware-attack-last-week (accessed May 11, 2017).
58. Reed, Tina. "MedStar Took 'Extreme' Measures to Block Cyber Threat." *Washington Business Journal*, March 29, 2016. Available at http://www.bizjournals.com/washington/news/2016/03/29/medstar-took-extreme-approach-to-block-security.html (accessed May 11, 2017).
59. Gordon, William J., Adam Fairhall, and Adam Landman. "Threats to Information Security—Public Health Implications." *New England Journal of Medicine* 377, no. 8 (2017): 707–9.

60. Radley, David C., Melanie R. Wasserman, Lauren E. W. Olsho, Sarah J. Shoemaker, Mark D. Spranca, and Bethany Bradshaw. "Reduction in Medication Errors in Hospitals Due to Adoption of Computerized Provider Order Entry Systems." *Journal of the American Medical Informatics Association* 20, no. 3 (2013): 470–76.
61. Shamliyan, Tatyana A., Sue Duval, Jing Du, and Robert L. Kane. "Just What the Doctor Ordered: Review of the Evidence of the Impact of Computerized Physician Order Entry System on Medication Errors." *Health Services Research* 43, no. 1, pt. 1 (2008): 32–53.
62. Slight, Sarah P., Diane L. Seger, Karen C. Nanji, Insook Cho, Nivethietha Maniam, Patricia C. Dykes, and David W. Bates. "Are We Heeding the Warning Signs? Examining Providers' Overrides of Computerized Drug-Drug Interaction Alerts in Primary Care." *PLoS One* 8, no. 12 (2013): e85071.
63. Bates, David W., and Sarah P. Slight. "Medication Errors: What Is Their Impact?" *Mayo Clinic Proceedings* 89, no. 8 (2014): 1027–29.
64. Agency for Healthcare Research and Quality. "Hospital Evacuation Decision Guide." 2011. Available at https://archive.ahrq.gov/prep/hospevacguide/ (accessed August 23, 2017).
65. US Department of Health and Human Services. *Fact Sheet: Ransomware and HIPAA*. Available at https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf (accessed November 25, 2017).
66. Sternstein, Jon, John Maser, and Peter Nelson. "The Rise of Ransomware." North Carolina Healthcare Information & Communications Alliance, Inc., 2016. Available at https://nchica.org/wp-content/uploads/2016/06/Sternstein-Maser-Nelson-1.pdf (accessed May 12, 2017).
67. Check Point and Europol. "Ransomware: What You Need to Know." Europol Public Information, 2016. Available at https://www.europol.europa.eu/publications-documents/ransomware-what-you-need-to-know (accessed May 12, 2017).
68. Kennedy, Carrie. "Ransomware and Healthcare: What You Need to Know." *Online Tech*, 2017. Available at http://resource.onlinetech.com/ransomware-facts-and-figures/ (accessed May 12, 2017).
69. Ponemon Institute. "2011 Cost of Data Breach Study: The United States." 2012. Available at www.ponemon.org/local/upload/file/2011_US_CODB_FINAL_5.pdf (accessed November 26, 2016).
70. Ponemon Institute. "Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data." 2016. Available at https://www.ponemon.org/local/upload/file/Sixth%20Annual%20Patient%20Privacy%20%26%20Data%20Security%20Report%20FINAL%206.pdf (accessed May 8, 2017).
71. IBM Global Technology Service. *Ponemon Institute's 2017 Cost of Data Breach Study: Global Overview*. 2017. Available at https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN& (accessed May 29, 2018.
72. IBM Global Technology Service. *IBM Security Services 2014 Cyber Security Intelligence Index.* http://media.scmagazine.com/documents/ 82/ibm_cyber_security_intelligenc_20450.pdf (accessed October 22, 2016).
73. Identity Theft Protection Association. "Credit Monitoring Services." 2012. Available at http://www.businessidtheft.org/Resources/PersonalCreditProtection/CreditMonitoringServices/tabid/114/Default.aspx (accessed November 2016).
74. Everett, Cath. "Ransomware: To Pay or Not to Pay?" *Computer Fraud & Security* 2016, no. 4 (2016): 8–12.
75. American Hospital Association. *FBI Cyber Division Bulletin: Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*. 2014. http://www.aha.org/content/14/140408--fbipin-healthsyscyberintrud.pdf (accessed November 25, 2017).
76. Zetter, Kim. "4 Ways to Protect Against the Very Real Threat of Ransomware." *Wired*, May 13, 2016. Available at https://www.wired.com/2016/05/4-ways-protect-ransomware-youre-target/ (accessed November 25, 2017).

77. Crowe, Jonathan. "Ransomware Attacks on Healthcare Providers Are Officially Being Reported as Data Breaches." Barkly, 2017. Available at https://blog.barkly.com/healthcare-ransomware-attacks-2017-data-breaches (accessed September 13, 2017).
78. Ibid.
79. Monica, Kate. "Ransomware Attack May Affect 10K Plastic Surgery Patients." Health IT Security, 2017. Available at https://healthitsecurity.com/news/ransomware-attack-may-affect-10k-plastic-surgery-patients (accessed September 13, 2017).
80. Monica, Kate. "PHI of 4.7K Ohio Patients Affected by Unauthorized EHR Access." Health IT Security, 2017. Available at https://healthitsecurity.com/news/phi-of-4.7k-ohio-patients-affected-by-unauthorized-ehr-access (accessed September 13, 2017).
81. Monica, Kate. "St. Mark's Ransomware Attack Could Affect 33K Patients." Health IT Security, 2017. Available at https://healthitsecurity.com/news/st.-marks-ransomware-attack-could-affect-33k-patients (accessed September 13, 2017).
82. Monica, Kate. "PHI of 13K Involved in Ransomware Attack at PA Health Clinic." Health IT Security, 2017. Available at https://healthitsecurity.com/news/phi-of-13k-involved-in-ransomware-attack-at-pa-health-clinic (accessed September 13, 2017).
83. Monica, Kate. "Ransomware Attack May Impact 19K Oncology Hematology Patients." Health IT Security, 2017. Available at https://healthitsecurity.com/news/ransomware-attack-may-impact-19k-oncology-hematology-patients (accessed September 13, 2017).
84. Monica, Kate. "MI Computer System Health Data Breach May Involve Data of 106K." Health IT Security, 2017. Available at https://healthitsecurity.com/news/mi-computer-system-health-data-breach-may-involve-data-of-106k (accessed September 13, 2017).
85. Identity Theft Protection Association. "ITRC Breach Statistics 2005–2016." 2017. Available at http://www.idtheftcenter.org/images/breach/Overview2005to2016Finalv2.pdf (accessed September 13, 2017).
86. Bai, Ge, John Xuefeng Jiang, and Renee Flasher. "Hospital Risk of Data Breaches." *JAMA Internal Medicine* 177, no. 6 (2017): 878–80.
87. Humer, Caroline and Jim Finkle. "Your Medical Record Is Worth More to Hackers Than Your Credit Card." Reuters, 2014. Available at https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924 (accessed September 13, 2017).
88. Lee, Jeong Kyu, Seo Yeon Moon, and Jong Hyuk Park. "CloudRPS: A Cloud Analysis Based Enhanced Ransomware Prevention System." *The Journal of Supercomputing* 73, no. 7 (2017): 3065–84.
89. IBM Global Technology Service. *IBM Security Services 2014 Cyber Security Intelligence Index.*
90. Boose, Shelley. "Tripwire RSA Survey: Only 38 Percent of Security Professionals Confident in Ransomware Recovery." Tripwire, 2016. Available at http://www.businesswire.com/news/home/20160324005065/en/Tripwire-RSA-Survey-38-Percent-Security-Professionals (accessed February 21, 2017).
91. Butler, Mary. "Tips for Preventing and Responding to a Ransomware Attack." *Journal of AHIMA*, April 1, 2016. Available at http://journal.ahima.org/2016/04/01/tips-for-preventing-and-responding-to-a-ransomware-attack/ (accessed February 21, 2017).
92. Mangelsdorf, Martha E. "What Executives Get Wrong about Cybersecurity." *MIT Sloan Management Review* 58, no. 2 (2017): 22–24.
93. Boose, Shelley. "Tripwire RSA Survey: Only 38 Percent of Security Professionals Confident in Ransomware Recovery."
94. Arndt, Rachel Z. "Frequent Employee Training Helps Stave Off Ransomware." June 3, 2017. Available at http://www.modernhealthcare.com/article/20170603/MAGAZINE/170539976?utm_source=modernhealthcare&utm_medium=email&utm_content=20170603-MAGAZINE-170539976&utm_campaign=am (accessed June 5, 2017).

95. Ponemon Institute. *The Rise of Ransomware*. 2017. Available at http://www.ponemon.org/local/upload/file/Ransomware%20Report%20Final%201.pdf (accessed May 22, 2018).
96. "Employees Prone to Phishing." *Computer Fraud & Security* 2016, no. 1 (2016): 3.
97. Zetter, Kim. "4 Ways to Protect Against the Very Real Threat of Ransomware."
98. Siwicki, Bill. "Tips for Protecting Hospitals from Ransomware as Cyberattacks Surge." 2016. Available at http://www.healthcareitnews.com/news/tips-protecting-hospitals-ransomware-cyber-attacks-surge (accessed August 27, 2016).
99. Zetter, Kim. "4 Ways to Protect Against the Very Real Threat of Ransomware."
100. Backblaze. "The 3-2-1 Backup Strategy." 2015. Available at https://www.backblaze.com/blog/the-3-2-1-backup-strategy/ (accessed June 7, 2017).
101. Heat Software. *Ransomware: The Fight Back Starts Now*. 2016. https://heatsoftware.com/wp-content/uploads/2016/12/ Ransomware_The_Fight_Back_Starts_Now-.pdf (accessed June 7, 2017).
102. Titan. "Ransomware Protection: Why the 3-2-1 Backup Strategy Works." *TitanHQ Blog*. 2016. Available at https://www.titanhq.com/blog/ransomware-protection-why-the-3-2-1-backup-strategy-works (accessed June 6, 2017).
103. Veeam. "7 Practical Tips to Prevent Ransomware Attacks on Backup Storage." 2016. Available at https://www.veeam.com/blog/tips-to-prevent-ransomware-protect-backup-storage.html (accessed June 7, 2017).
104. Tuttle, Hilary. "Ransomware Attacks Pose Growing Threat." *Risk Management* 63, no. 4 (2016): 4.
105. Cox, John Woodrow. "MedStar Health Turns Away Patients After Likely Ransomware Cyberattack." *Washington Post*, March 29, 2016. Available at 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 (accessed May 11, 2017).
106. Phillips, Gavin. "Yes, Ransomware Can Encrypt Your Cloud Storage." *MUQ: Security*, May 29, 2017. Available at http://www.makeuseof.com/tag/cloud-drive-ransomware/ (accessed June 7, 2017).
107. Spector, Lincoln. "How to Stop Ransomware: Backup Can Protect You, But Only If You Do It Right." *PC World*, May 6, 2016. Available at http://www.pcworld.com/article/3056907/security/how-to-stop-ransomware-backup-can-protect-you-but-only-if-you-do-it-right.html (accessed June 7, 2017).
108. Lee, Jeong Kyu, Seo Yeon Moon, and Jong Hyuk Park. "CloudRPS: A Cloud Analysis Based Enhanced Ransomware Prevention System."
109. Condliffe, Jamie. "Widespread Ransomware Attack Hits U.K. Hospitals." *MIT Technology Review*, May 12, 2017. Available at https://www.technologyreview.com/s/607863/widespread-ransomware-attack-hits-uk-hospitals/ (accessed June 7, 2017).
110. Scott, Mark, and Nicole Perlroth. "With Ransomware, It's Pay and Embolden Perpetrators, or Lose Precious Data." *New York Times*, May 17, 2017. Available at https://www.nytimes.com/2017/05/17/technology/bitcoin-ransomware-pay-lose-data.html?_r=0 (accessed June 7, 2017).
111. Wong, Julia Carrie, and Olivia Solon. "Massive Ransomware Cyber-Attack Hits Nearly 100 Countries around the World." *The Guardian*, May 12, 2017. Available at https://www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs (accessed June 7, 2017).
112. Sheber, Sarah. "Industry Keeping a Weather Eye for Medical Device, Ransomware Hacks." *Journal of AHIMA*, April 20, 2017. Available at http://journal.ahima.org/ 2017/04/20/industry-keeping-a-weather-eye-for-medical-device-ransomware-hacks/ (accessed April 22, 2017).
113. Butler, Mary. "Tips for Preventing and Responding to a Ransomware Attack."
114. Loughlin, Sean, Axel Wirth, Kevin Fu, Tim Gee, and Izabella Gieras. "A Roundtable Discussion: Safeguarding Information and Resources against Emerging Cybersecurity Threats." *Biomedical Instrumentation & Technology* 48, no. S1 (2014): 8–17.

115. Siwicki, Bill. "Ransomware 2.0: It's Coming, and Healthcare Needs to Get Prepared." *Healthcare IT News*, August 8, 2017. Available at http://www.healthcareitnews.com/news/ransomware-20-its-coming-and-healthcare-needs-get-prepared (accessed September 13, 2017).
116. Chinthapalli, Krishna. "The Hackers Holding Hospitals to Ransom." *BMJ* 357 (2017): j2214.
117. Ladika, S. "Health Care, an Easy Target, Needs to Get Its Guard Up." *Managed Care* 25, no. 12 (2016): 31.
118. US Department of Health and Human Services. *Health Care Industry Cybersecurity Task Force: Report on Improving Cybersecurity in the Health Care Industry*. June 2017. Available at https://www.phe.gov/preparedness/planning/cybertf/documents/report2017.pdf (accessed November 25, 2017).

Table 1

Details of Ransomware Events in Healthcare Following the Hollywood Presbyterian Medical Center Incident

Date and 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, Klinikum Arnsberg, North Rhine-Westphalia, Germany	Detected on one 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)
May 18, 2016, Kansas Heart Hospital, Wichita, KS	Files locked	Ransom paid (small undisclosed amount) but full access not restored; second ransom demanded but not paid	Jayanthi (2016)
March 14, 2016, Ottawa Hospital, Canada	Four computers encrypted	No ransom paid; data restored from backups	Pilieci, (2016)
March 18, 2016, Prime Health Care: Chino Valley Medical Center and Desert Valley Hospital, Victorville, CA	A number of computers and some hospital servers had locked data	No ransom paid; backups restored	Winton (2016)
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 of patient data, but email and clinical support systems were unavailable	45 bitcoin ransoms demanded ($19,000), but no ransom paid	Reed (2016)

Sources:

Jayanthi, Akanksha. "Kansas Heart Hospital Pays Ransom, Then Hackers Came Back for More." *Becker's Health IT and CIO Review*, May 23, 2016. Available at http://www.beckershospitalreview.com/healthcare-information-technology/kansas-heart-hospital-pays-ransom-then-hackers-came-back-for-more.html (accessed May 6, 2017).

Landi, Heather. "Kentucky-based Methodist Hospital's System Restored Following Ransomware Attack Last Week." *Healthcare Informatics*, March 21, 2016. Available at https://www.healthcare-informatics.com/news-item/kentucky-based-methodist-hospital-s-system-restored-following-ransomware-attack-last-week (accessed May 11, 2017).

Network Security Journal. "Ransomware Expands, Attacks Hospitals and Local Authorities, and Moves to New Platforms." *Network Security*, no. 3 (2016): 1–2.

Pilieci, Vito. "Ottawa Hospital Hit with Ransomware, Information on Four Computers Locked Down." *National Post*, March 13, 2016. Available at http://news.nationalpost.com/news/canada/ottawa-hospital-hit-with-ransomware-information-on-four-computers-locked-down (accessed May 11, 2017).

Reed, Tina. "MedStar Took 'Extreme' Measures to Block Cyber Threat." *Washington Business Journal*, March 29, 2016. Available at http://www.bizjournals.com/washington/news/2016/03/29/medstar-took-extreme-approach-to-block-security.html (accessed May 11, 2017).

Winton, Richard. "2 More Southland Hospitals Attacked by Hackers Using Ransomware." *Los Angeles Times*, March 22, 2016. Available at http://www.latimes.com/local/lanow/la-me-ln-two-more-so-cal-hospitals-ransomware-20160322-story.html (accessed May 11, 2017).

Table 2

Details of Some Recent Patient Data Breaches and Healthcare Facility Cyberattacks

Healthcare System	**Attack Date**	**Date Patients Were Notified**	**Number of Patients Affected**	**Source**
ABCD Children's Pediatrics	February 6, 2017	March 26, 2017	55,447	Crowe (2017)
Urology Austin	January 22, 2017	March 22, 2017	279,663	Crowe (2017)
Metropolitan Urology	November 28, 2016	March 10, 2017	17,634	Crowe (2017)
Plastic Surgery Associates of South Dakota	February 12, 2017	Not available	10,200	Monica (2017)
Daniel Drake Center for Post-Acute Care	Between July 29, 2015 and June 2, 2017	August 1, 2017	4,721	Monica (2017)
St. Mark's Surgery Center	Between April 13 and April 17, 2017	August 9, 2017	33,877	Monica (2017)
Kaleida Health	April 24, 2017	August 25, 2017	2,789	Monica (2017)
Family Tree Health Clinic	April 24, 2017	Not available	13,402	Monica (2017)
Medical Oncology Hematology Consultants, PA	June 17, 2017	August 2017	19,203	Monica (2017)
McLaren Medical Group	March 2017	March 24, 2017	106,008	Monica (2017)
Silver Cross Hospital	June 14, 2017	Not available	8,862	Monica (2017)

Sources:

Crowe, Jonathan. "Ransomware Attacks on Healthcare Providers Are Officially Being Reported as Data Breaches." Barkly, 2017. Available at https://blog.barkly.com/healthcare-ransomware-attacks-2017-data-breaches (accessed September 13, 2017).

Monica, Kate. "MI Computer System Health Data Breach May Involve Data of 106K." Health IT Security, 2017. Available at https://healthitsecurity.com/news/mi-computer-system-health-data-breach-may-involve-data-of-106k (accessed September 13, 2017).

Monica, Kate. "PHI of 13K Involved in Ransomware Attack at PA Health Clinic." Health IT Security, 2017. Available at https://healthitsecurity.com/news/phi-of-13k-involved-in-ransomware-attack-at-pa-health-clinic (accessed September 13, 2017).

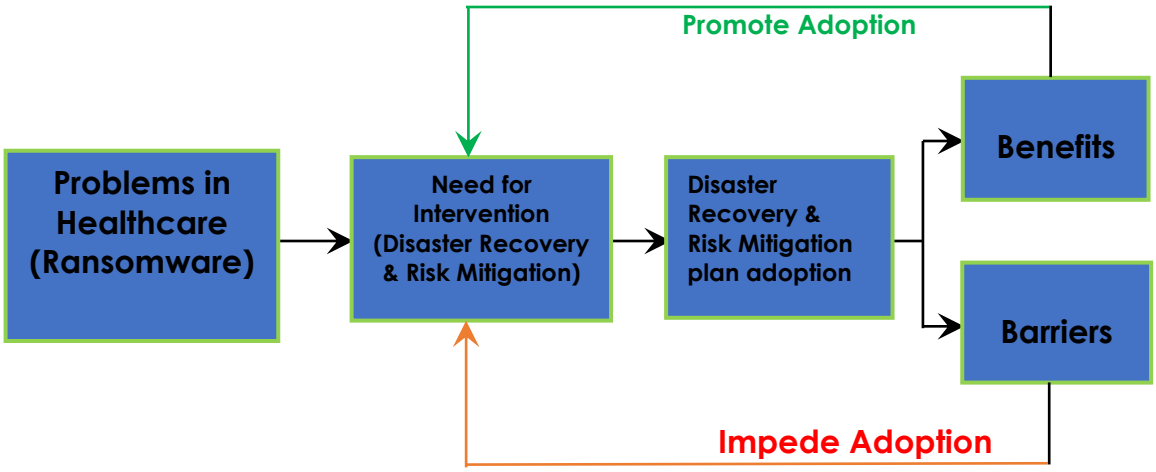
Monica, Kate. "PHI of 4.7K Ohio Patients Affected by Unauthorized EHR Access." Health IT Security, 2017. Available at https://healthitsecurity.com/news/phi-of-4.7k-ohio-patients-affected-by-unauthorized-ehr-access (accessed September 13, 2017).

Monica, Kate. "Ransomware Attack May Affect 10K Plastic Surgery Patients." Health IT Security, 2017. Available at https://healthitsecurity.com/news/ransomware-attack-may-affect-10k-plastic-surgery-patients (accessed September 13, 2017).

Monica, Kate. "Ransomware Attack May Impact 19K Oncology Hematology Patients." Health IT Security, 2017. Available at https://healthitsecurity.com/news/ransomware-attack-may-impact-19k-oncology-hematology-patients (accessed September 13, 2017).

Monica, Kate. "St. Mark's Ransomware Attack Could Affect 33K Patients." Health IT Security, 2017, Available at https://healthitsecurity.com/news/st.-marks-ransomware-attack-could-affect-33k-patients (accessed September 13, 2017).

Figure 1
Conceptual Framework



Source: Adapted from Yao, W., C. H. Chu, and Z. Li. "The Use of RFID in Healthcare: Benefits and Barriers." *Proceedings of the 2010 IEEE International Conference on RFID Technology and Applications (RFID-TA)* (2010): 128–34.

Appendix A

Questions asked in a Semistructured Interview with Paul English Smith, Vice President and General Counsel, Cabell Huntington Hospital, Huntington, West Virginia, an Expert in Healthcare Law, on August 26, 2016

- What are some of the legal implications involved in a ransomware incident?
- If the hospital is unable to provide critical 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 Semistructured Interview with Dennis Lee, Vice President and Chief Information Officer, Cabell Huntington Hospital, Huntington, West Virginia, 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 (e.g., email phishing)?
- In the event of a ransomware attack, what are the procedures for the response?
- What costs would be associated with response and recovery?
- What are some critical aspects of a malware prevention plan?
- In your opinion, when a hospital suffers a ransomware attack, would this be considered a HIPAA breach?