2017

Examining the Risk Factors for Hospital Ransomware Attacks: A Qualitative Study

Cedric L. Truss
Medical University of South Carolina

EXAMINING THE RISK FACTORS FOR HOSPITAL RANSOMWARE ATTACKS: A QUALITATIVE STUDY

BY

CEDRIC L. TRUSS

A doctoral project submitted to the faculty of the Medical University of South Carolina in partial fulfillment of the requirements for the degree Doctor of Health Administration in the college of Health Professions

EXAMINING THE RISK FACTORS FOR HOSPITAL RANSOMWARE ATTACKS: A QUALITATIVE STUDY

BY

CEDRIC L. TRUSS

Approved by:

4/30/17
Chair, Project Committee   Jillian Harvey, PhD   Date

4/30/17
Member, Project Committee   Mark Mellott, PhD   Date

4/30/17
Member, Project Committee   Trudie Milner, PhD   Date

6/5/17
Dean, College of Health Professions   James S Zoller, PhD   Date

Acknowledgements

It is with the sincerest gratitude that I thank my family and friends for being supportive of me while I attain this doctoral degree. The past three years have been an excellent journey and I am happy to see this particular educational chapter come to an end. You all have believed in me and never doubted my ability to pursue this degree, but always provided words of encouragement that I will never forget. I am looking forward to seeing what the future will hold.

Thanks to Dr. Laura Forbes and Dr. Cathleen Erwin for encouraging me while as an undergraduate student at the University of Alabama of Birmingham to eventually pursue a doctoral level education. To the leadership teams at Research and Evaluation Group and Tier 2 Consulting Group in Atlanta, Georgia, I thank you all for the support and opportunities to be a member of your organizations and supporting my educational efforts with understanding while working full-time.

I would like to thank Dr. Kit Simpson for encouraging me to further explore this research topic after her course and turning it into my doctoral research project. I would like to thank my committee for all their help in guiding me through this entire process. Thanks to Dr.Mellott for providing his detailed feedback and input on the research as it relates to information technology and information systems. Thanks to Dr.Milner for her expertise from the view of a hospital executive to make this project relatable to the real world experiences of hospital leadership. I would like to give a special thanks to Dr. Harvey for always being available when needed and providing me with clear and solid

feedback throughout my research project. Without her guidance, I would not have been able to complete this project in a timely manner.

Abstract of Doctoral Project Presented to the
Executive Doctoral Program in Health Administration & Leadership
Medical University of South Carolina
In Partial Fulfillment of the Requirements for the
Degree of Doctor of Health Administration

EXAMINING THE RISK FACTORS FOR HOSPITAL RANSOMWARE ATTACKS: A QUALITATIVE STUDY

By

Cedric L. Truss

Chairperson: Jillian Harvey, Ph.D, Assistant Professor, Medical University of South Carolina
Committee: Mark Mellott, Ph.D, Adjunct Instructor, Medical University of South Carolina
Trudie Milner, Ph.D, Adjunct Assistant Professor, Medical University of South Carolina

Ransomware attacks have started to affect the hospital industry and cause major disruptions in operations. There are at least five successful ransomware attacks that have affected hospitals. The only way they were able to regain access to their systems were to submit payment via bitcoin to the entity that conveyed the ransom or recover their systems from backups. In this study, we identified risk factors from published reports for hospital ransomware attacks. This study employed a qualitative review of published news articles and reports that discussed the events of the ransomware attacks. This exploratory method is appropriate for new and emerging topics and used to compare written text to established guidelines or models. We used the NIST Cyber Security Framework to code content and analyze information from journal articles, memos, blogs, research studies and white papers that contained information reported by the hospitals.

Hospitals and media reports were not transparent in reporting detailed information surrounding the events of ransomware attacks. Overall, study results demonstrate that there are risk factors for hospitals to become targets for ransomware attacks.

Keywords: Ransomware, malware, cybersecurity, health information security, nist cyber security framework

Table of Contents

Page

I. INTRODUCTION

Background and Need

For many decades, the healthcare industry has lagged behind other industries in adopting and implementing information technology within their workflow. Information technology has begun to take a role in healthcare that it has never taken before. Professionals in healthcare can use technology and information systems as a way to improve their process in improving health care quality, access to care, and operational processes. In the past decade, hospitals have taken the dive into the information technology arena in implementing technology throughout their health systems. The use of information technology in health care has given access to providers to make informed decisions in a timely manner and allowed healthcare executives to make operational decisions. Information technology is defined as "a set of tools, processes, and methodologies and associated equipment employed to collect, process, and present information" (www.businessdictionary.com). This technology can be accessed via desktops, laptop computers and mobile devices.

In the past 10 years, the health care industry has gone through many changes in how they collect, store and utilize health information. From paper records, legacy systems to implementing new health information technology (HIT), organizations are able to quickly have access to a patient's entire medical history. Over the years there has been a large amount of funding and resources invested in health information technology by health systems and physician practices. The Office of the National Coordinator for

Health Information Technology (ONC) was established in 2004 through an executive order by former President George W. Bush, to coordinate the implementation and use of health information technology and the electronic exchange of health information. This establishment was later mandated through legislation under former President Barack Obama in the Health Information Technology for Economic and Clinical Health Act (HITECH Act) of 2009 (ONC, 2016). In an effort to provide assistance and support, the ONC established Regional Extension Centers (RECs) across the country, which would be a resource to health care organizations for electronic health record (EHR) implementation and Health IT needs. The centers are located in every region and serve as trusted advisors to their communities in providing expertise in the adoption and meaningful use of electronic health records (RECs, 2015). As there are many challenges and opportunities that are facing the healthcare industry, health information technology will play a part in integrating systems, providing efficiency patient-related data and providing access to care in underserved areas.

With the implementation of the Health Information Technology for Economic and Clinical Health (HITECH) Act in 2009, change in health care has become the new norm and can be quite an enormous task for many organizations to handle without support from subject matter experts. For many health care organizations, information technology is being implemented for many different reasons. There is a strong evidence base documenting the benefits of electronic health information technology. Health information technology is reported to contribute to organization efficiency, provider satisfaction, patient safety, medication adherence, and numerous other indicators of health care quality (Virga et al., 2012). In recent years, the health care industry has endured a major shift in operations and patient care with the implementation of information technology. In the past, organizations have relied on paper medical records to for documentation and use of health data, in which it took longer to review data and make effective long-term decisions. Implementing IT in health care has allowed for the use of electronic health and medical records, as well as other ancillary systems that collect and store patient information. In storing private and protected health information electronically, there are risks associated in those systems being compromised. For many years, the most common risk that has affected the healthcare industry has been data breaches where sensitive, identifiable patient data was accessed by an unauthorized individual. The most recent risk to the healthcare industry has been ransomware attacks that have caused hospitals to spend an outrageous amount of money to regain control of their systems.

In the hospital industry, health IT has become a reliable source in patient care. The U.S. Department of Health and Human Services (HHS) listed health IT as one of the top management and performance challenges and also noted that it also poses two major challenges: ensuring security and access. In terms of security, the department reports that guaranteeing the secure exchange of electronic information remains a top priority due to the rise of the Internet of Things (IoT), mobile health technology and use of ransomware by cybercriminals has contributed to privacy challenges. (Cohen, 2016). With the use of technology for healthcare, organizations need to be aware of the potential consequences that could possibly occur. The healthcare industry will always need to be proactive in how they monitor their systems with the amount of protected health information that are entered into the electronic health records.

Recently, Bitglass released a report from over 3,000 IT professionals on cloud security risks, priorities and capabilities. Fifty-two percent of organizations expect to increase their overall security budgets. Only 24% of organizations routinely monitor Saas and IaaS apps for security risks, compared to over 60% for desktops, laptops and the network perimeter. Only 36% monitor mobile devices. One in three of organizations reported that they had been hacked more than five times in the past 12 months double the rate from 2014. Eighty-seven percent of organizations were victims of at least one cyber-attack. Ransomware is a major concern, but 54% of enterprises managed to recover data without paying the ransom. For 37% of respondents, phishing is the top concern followed by insider threats (33%) and malware (32%). For organizations that have adopted the cloud, data encryption (72%), traffic encryption (60%) and access controls (56%) are the capabilities most in demand. (Marketwired, 2017).

Problem Statement

In recent months, there have been attacks against healthcare organizations through the use of ransomware attacks. Ransomware is considered to be a type of malware that restricts or limits access to a device or computer network until the user has paid the ransom (kaspersky.com). Although ransomware is a malware, there are multiple types that could affect a computer network system. At least five successful ransomware attacks on healthcare organizations are known: MedStar Health, Hollywood Presbyterian Medical Center, Methodist Hospital, Desert Valley Hospital, and Chino Valley Medical Center (Van Alstin, 2016). In these cases, hospitals lost access to patient records and the only way they were able to regain complete access to their systems were to submit payment via bitcoin to the entity that conveyed the ransom or successfully recovering their systems from backups. Bitcoin is a new payment system that is a completely digital currency. This is the first peer-to-peer payment network and there are no requirements for central oversite or middlemen (https://bitcoin.org/en/faq#what-is-bitcoin). Some organizations tried to restore their networks using their backup procedures, but unfortunately did not have luck and their only option was to pay the ransom via bitcoin. The attacks have generally been treated as individual cases. However, we should learn from medicine, and treat these events as early cases of a new epidemic in the health care system.

Prior to 2016, healthcare organizations were an unlikely target for ransomware attacks. It is a concern that the attention given to the Hollywood Presbyterian attack will lead to future attacks on the healthcare system (http://www.healthcareitnews.com/news/ransomware-wreak-havoc-2016-icit-study-says accessed 06/08/2016). Ransomware can attack desktop or laptop computers and mobile devices. Ransomware frequently can result in a pop-up demanding a monetary ransom in exchange for the decryption key. Security experts and law enforcement personnel do not recommend paying the ransom, however, some organizations do comply when the encrypted information is difficult to reproduce (Callahan, 2016).

The attacks that have taken place have locked down network systems, encrypting files and holding them hostage. For many hospital systems, their only choice to get their files released is to pay the ransom. Throughout research and literature reviews, it is forecasted that there will be an increase in ransomware attacks against healthcare organizations in the future. It is important that healthcare organizations review their current security policies and identify any gaps they may have and implement new policies. Additionally, organizations will have start utilizing best practices that will prevent them from being victims of ransomware attacks in the future. Failure on behalf of health care organizations to protect their electronic health records systems will cost them to spend more money over time due to their networks being compromised and held hostage by ransomware.

Research Question

What Are the Risk Factors for Hospital Ransomware Attacks?

Population

The study population for this research will include all hospitals that have been affected by ransomware attacks between January 1, 2015 and December 31, 2016 within the United States. Considering there have only been a few reported events during this time period, a review will be completed for each organization that has publicly available information about their attacks and the strategies they took to regain control of their systems.

Assumptions

An assumption made by this study is that all information is being reported in the news and in relevant literature. Considering that healthcare systems are fairly new to the digital and electronic age, we can expect to see more organizations affected by ransomware in the future.

II. REVIEW OF LITERATURE

Background

In today’s society, the majority of Americans depend on information technology in nearly every stage of day to day activities. From banking, to education, transportation and most recently, health care providers rely on technology for decision making and to provide patients with information. The way consumers utilize technology on a daily basis, everyone also needs to be aware of the security risks that could potentially arise from the exchange of personal information. The ideology of information security was not integrated early enough into systems and only recently has started to gain warranted attention. Consequently, it is important to identify and manage these masked weaknesses, referred to as systems vulnerabilities, and to reduce their harmful impact on the information systems integrity, confidentiality, and availability. These system vulnerabilities are exploited by attacks through hackers, which are becoming more targeted and sophisticated. In any industry, security risks must be identified, evaluated, analyzed, treated and reported properly. When a business fail to identify the risks associated with their technology use and other surrounding factors, they can subject their organizations to unforeseen consequences that may result in damage to the business. Although, risks are difficult to eliminate completely, it is possible for them to be reduced to acceptable levels. These acceptable risks are those that the organization decides to allow after an evaluation has been conducted to determine if the cost of treating the risks outweighs the benefits (Al-Ahmad & Mohammad, 2013).

Information security is particularly defined by three characteristics in which they are in place to protect information and systems from unauthorized access. These characteristics and their purpose are:

1. confidentiality- avoid unauthorized release of information
2. integrity- prevent unauthorized revision of information
3. availability- prevention of unauthorized withholding of information or resources

Considering most Americans input personal information into different applications using all types of technology, they are also in jeopardy of having information accessed by unauthorized parties. Consumers of technology cannot solely rely on applications to provide protection from vulnerabilities, but they must also be aware and take precautions in what information is shared and then can be exposed by hackers. Although the characteristics of security are available, organizations and technology users should be aware they exist for a reason and should consider what information they are making available and how they should keep it secured (Ferreira et al., 2010).

Organizations from every industry are potential targets of having secured information systems hacked by unauthorized users. The emersion of cybercrime took place in the late 1970s as the information technology (IT) industry began to take place. Over time, the cybercrime has become more refined and managed by the criminals that are responsible for the acts. The implementation of information technology for patient care has made the healthcare industry a prime target for cybercrime due to the availability of data containing sensitive information of the patients. To try and prevent the unauthorized access of sensitive information through cybercrime, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) implemented physical and technical safeguards. The physical safeguards include controls for workstation use and security, device, media, and facility access. The technical safeguards include the use of a unique identification, an emergency access procedure, automatic logoff, along with encryption and decryption of information. Although these safeguards are in place, there have been cases where cybercriminals were able to find ways around them (Kruse et al., 2017). In these cases, the criminals have used their knowledge, skills and abilities to intrude their way through networks virtually and lock them down using ransomware and then holding organizations hostage to their own information systems.

There are at least two dimensions to hospital risk of ransomware hijacking:

a) Risk factors related to IT security

b) Factors related to hospital characteristics

Using the Medical University of South Carolina’s library search resources, specifically the PubMed portal, an initial query of the database using the term “malware” , “ransomware” , and “health information security” returned a body of work that set the baseline from which additional queries were run. Due to the recent events that have taken place of ransomware attacks in hospitals, the literature review was selected for articles published between 1/1/2015 and 12/31/2016 and if there was free full text access available through the Medical University of South Carolina library search resources, specifically the PubMed portal.

The initial PubMed query using the term “malware” returned a total of 44 articles. From this query, 22 articles were selected for review. Of those articles, 20 did not meet the inclusion criteria of empirically based studies related to malware in hospitals. As a result, two were used in this review. Using the term “ransomware,” the PubMed database returned a total of 9 articles. From this query, two articles were selected for review. After removal of duplicates, one was used in this review. Using the term “health information security,” the PubMed database returned a total of 6020 articles. The query was refined by filtering the return to include only articles published between 1/1/2015 and 12/31/2016, with free full text access and with the term “health information security” in the title of the article. From this query, 5 articles were selected for review. Of those articles, 3 were used in this review. Articles were selected for review if the query terms appeared in the title or the abstract of the article, if the article was published between January 1, 2015 and December 31, 2016, and if the reviewer felt the article was contextually relevant and offered a unique/niche perspective on the subject area.

A. Ransomware

Ransomware has become a major issue that has begun to affect every industry in some manner. The adoption of information technology in healthcare has made the hospital industry prime targets of ransomware. Ransomware is intended to damage or disable a user’s access to a computer system unless the user pays the ransom. When the attack has been initiated, users have three options: 1) try to restore their data from backup; 2) pay the ransom; 3) lose their data. This article discusses how a socio-technical approach can address ransomware and outlined four steps that organization can take to secure their infrastructure: 1) health IT professionals need to ensure adequate system protection by correctly installing and configuring computers and networks that connect them; 2) the health care organizations need to ensure more reliable system defense by implementing user-focused strategies, including simulation and training on correct and complete use of computers and network applications; 3) the organization needs to monitor computer and application use continuously in an effort to detect suspicious activities and identify and address security problems before they cause harm; 4) organizations need to respond adequately to and recover quickly from ransomware attacks and take actions to prevent them in future. Additionally, the article also discusses recommendations from other sources, including the National Institute of Standards and Technology (NIST). (Sittig & Singh, 2016).

B. Malware

There are steps that organizations can take to detect core malware sites related to biomedical information systems. The authors of this article presented a method to locate malicious website attacks that attempt to attack biomedical information systems. The method discussed included creating a risk index that would be used to analyze the centrality between malware sites and it would eliminate the root of the sites by finding the core-hub node which could help reduce unnecessary security policies. The risk index is estimated based on the analysis of the various centrality measures and converting them into a single quantified vector. Through the use of the risk index, it was determined that the proactive elimination of core malicious websites resulted in an average improvement in zero-day attack detection of more than 20% (Kim, 2015).

More than three quarters of the health care industry affected by malware attacks (Ladika, 2016). The National Association of Insurance Commissioners (NAIC) hopes to create standards for laws and regulations governing data security and for investigations of data breaches. This move comes as a result of health care now being an industry that is targeted by ransomware attacks and hackers for information. Health care is being widely infected with malware and has faced ransomware attacks multiple times in recent years. In comparison to the financial services industry, health care seems to be an easier target because there are few defenses for the same amounts of data (Ladika, 2016).

C. Health Information Security

Many consumers' concerns regarding the security and privacy of electronic health records (EHRs). The authors conducted a study that would describe the perceptions regarding privacy and security of medical records and identify factors associated with the perceptions. The researchers used a nationally representative 2011-2012 survey and reported on adults' perceptions regarding privacy and security of medical records and sharing of health information between providers. In the study, 59.06% of the adults surveyed indicated they had concerns about the security and privacy of electronic health information. However, many are confident in the privacy and security of their medical records (Patel et al., 2015).

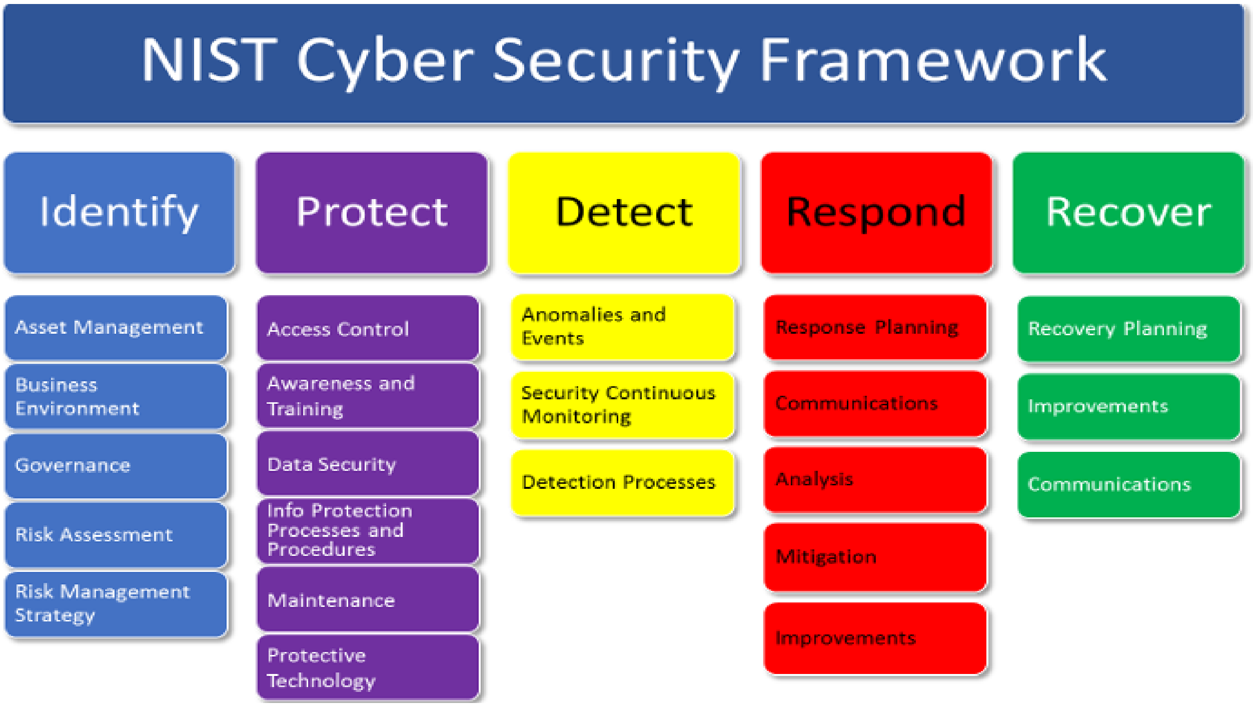
This article discussed how an information system for hospitals has the ability to improve access to clinical information and the quality of health care. The authors also discussion how the use of these systems have presented challenges and concerns over health information security. The research was to assess the status of information security in administrative, technical and physical safeguards in the university hospitals. Research was conducted through the use of surveys completed by information technology (IT) managers who worked in top ranked hospitals associated with medical universities. The data analyzed indicated the administrative safeguards were arranged at a medium level, whereas technical and physical safeguards were rated at a strong level. The researcher's recommendations for improving the administrative safeguards included implementing access control models and training users (Mehraeen et al., 2016).

While the majority of studies in this review are theoretical, or implementation studies, one study was to evaluated computerized health information systems (CHISs), information security risk management at hospitals in Iran (Zarei & Sadoughi, 2016). Researchers collected data from 551 hospitals in Iran through the use of a questionnaire that was designed to assess security risk management for CHISs at the concerned hospitals. It was discovered that 69% of the hospitals pursue information security policies and procedures in conformity with the Iran Hospitals Accreditation Standards. It was noted from the questionnaires that there were no significant structured approach to risk management at the hospitals that were studied. The research indicated there should be practical policies developed to improve information security risk management in Iran's hospitals (Zarei & Sadoughi, 2016).

Framework

In review of literature, there has not been an established security framework that is specific to the healthcare industry. The National Institute of Standards and

Technology (NIST) have developed a framework that allows organizations to better guide their cybersecurity activities. The framework was developed as a voluntary template that can be applied to nearly any industry and can be as flexible as needed to support an organization’s security policies. This framework will be used to guide the analysis of the hospitals which have experienced ransomware attacks and have reported information to the media.



NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

(Nichols, 2016)

The NIST Cyber Security Framework consists of five sections that an organization can use to develop their own processes to fall within those sections that will help mitigate any potential cybercrime within their network. Each section of the framework provides a different purpose and how it benefits the organization:

1. Identify- Cultivate an understanding for the organization to manage cybersecurity risk to the network systems, data and abilities.
2. Protect- Develop and implement safeguards that will guarantee secured delivery of services.
3. Detect- Develop and implement an algorithm that can identify instances of cybersecurity events.
4. Respond- Develop and implement an action plan that is deployed when a cybersecurity event is detected.
5. Recover- Develop and implement a procedure that will be followed to recover from any catastrophic cybersecurity events.

If each step of this framework is followed, organizations should be able to establish policies and procedures that will allow them to regain control of their systems and recover in a timely manner when an event has been detected. The healthcare industry can use this Framework to complement their current processes for cybersecurity risk. The Framework was not designed to replace existing processes, but as a resource that will help determine gaps and how to address them with improved solutions. Additionally, this Framework can be relied upon for the development of new cybersecurity programs as well as improving current programs (https://www.nist.gov/cyberframework).

III. METHODOLOGY

Research Design/Method

The study design employs a qualitative review of published news articles and reports to answer the study question. This exploratory method is appropriate for new and emerging topics such as ransomware in hospitals. Specifically, qualitative content analysis is used to compare written text to established guidelines or models (Gagliardi & Brouwers, 2012). The process will be employed as follows:

A. Identify data source
B. Compile and organize data
C. Begin first review of data
D. Begin second review of data
E. Analyze data through categorization and content analysis

Sample Selection

The sample chosen for this study includes reported cases of malware hijacking for ransom within the hospital industry. The study design employed a qualitative review of archival data to answer the study question. We use a multi-step approach to identify reports, popular press articles, blogs, letters and other sources describing the ransomware attacks in healthcare. First, we utilized the Medical University of South Carolina’s online library source, the PubMed portal, to query the database using the term “malware”, “ransomware”, and “health information security”.

The "advanced search" feature of the Google search engine was used to search for "ransomware in healthcare", narrowing the results by language (English) and region (United States). There were a number of hospitals in the United States attacked by ransomware between 2015 and 2016. We specifically searched the internet for these cases using the hospital name. These are the organizations who systems have been affected by malware and solicited a ransom to release control of the system back to the hospitals. We also searched specific professional organization websites for case reports and white papers related to the incidents, including HIMSS.

Data Collection/Procedure

A two-step process will be used: 1) Extraction of events from newspaper reports, blogs, IT newsletters and other written or recorded documentation in 2015 and 2016 through the online Google search engine; 2) Use of supplementary data sources on hospital characteristics to better describe the characteristics of the "victims" of the attacks.

Data Analysis

A two-step process was used to analyze the data: 1) Using qualitative content analysis the categories risk from the NIST Cyber Security Framework, each healthcare ransomware article was coded to identify the categories of risk affecting the individual incidents. Furthermore, any mentions of best practices, recommendations, or factors that prevented additional harm to the organization were coded as best practice guidelines to prevent ransomware. Qualitative and quantitative data was also captured to provide contextual summaries on each "victim". 2) The circumstances of each incident were compared and contrasted across all cases to the overarching risk factors and guidelines identified in the prior step.

Two researchers independently reviewed one case to determine appropriateness of the coding framework. A sample coding guide can be found in Table 1. Upon consensus, the risk factors framework was applied to all cases. At the completion of this process, descriptive tables and graphical displays of event characteristics related to a) IT security issues or risk factors and b) hospital characteristics and their relationship (if any) to the type of ransomware used in the event were created. This information will be used to inform healthcare leaders of areas of potential risk to and where the organization should review to strengthen the security of their network.

Table 1: Content Analysis Framework

	Victim 1	Victim 2	Victim 3	Victim 4	Victim 5
Identify					
Protect					
Detect					
Respond					
Recover					

Limitations/Delimitations

The study employed a qualitative review of archival data to answer the study question. This method was chosen as there are limited sources of published data on this subject and events are recent. The methodology allowed for a review of literature that was available to the public via online resources. The primary limitation of this study is the dependence on publication of the details of each ransomware case. In some cases, there was little description of the event and results. The results contained in this study are from the hospital industry in the United States that provided information to the media; therefore its transferability is limited.

IV. RESULTS

In total we reviewed data for five hospitals that were affected by ransomware attacks between 2015 and 2016 to determine if there was a trend between the hospitals that made them prime targets for the hackers. Table 2 reports the demographic characteristics of the organization and community associated with the hospital and where they are located. The research was conducted by employing a qualitative content analysis review of literature found through the google search engine. The analysis consisted of 18 articles, in which several reports provided information for multiple cases that were identified for this study. Content reviewed and analyzed included information from journal articles, memos, blogs, research studies and white papers that contained information reported by the hospitals. Due to the nature and events of the attack that crippled the Hollywood Presbyterian Medical Center network system, all of the additional reported cases referred to this isolated case and provided details of the hospital's actions to regain control of their systems.

Table 2: Demographic Characteristics of Hospitals

Organization	**Location**	**# Beds**	**Status**	**Population Size**	**Median Household Income**	**% Persons in Poverty**	**% Persons without health insurance under 65**
Hollywood Presbyterian Medical Center	Los Angeles, CA	434	Private Hospital	10,137,915	$56,196	16.7%	12.5%
MedStar Health							
MedStar Franklin Square Medical Center	Baltimore County, MD	378	Not-for-Profit	831,026	$67,095	9.1%	6.8%
MedStar Georgetown University Hospital	Northwest Washington, D.C.	609	Not-for-Profit	681,170	$70,848	17.3%	5.8%
MedStar Good Samaritan Hospital	Baltimore, MD	317	Not-for-Profit	831,026	$67,095	9.1%	6.8%
MedStar Harbor Hospital	Baltimore, MD	150	Not-for-Profit	831,026	$67,095	9.1%	6.8%
MedStar Montgomery Medical Center	Olney, MD	149	Not-for-Profit		$133,121	2.6%	3.8%
MedStar National Rehabilitation Network	Northwest Washington, D.C.	137	Not-for-Profit	681,170	$70,848	17.3%	5.8%
MedStar St.Mary's Hospital	St. Mary's County, MD	103	Not-for-Profit	112,587	$86,987	8.7%	5.0%
MedStar Southern Maryland Hospital	Clinton, MD	262	Not-for-Profit		$103,678	4.0%	6.5%
MedStar Union Memorial Hospital	Baltimore, MD	283	Not-for-Profit	831,026	$67,095	9.1%	6.8%

MedStar Washington Hospital Center	Northwest Washington, D.C.	926	Not-for-Profit	681,170	$70,848	17.3%	5.8%
Methodist Hospital	Henderson, KY	217	Not-for-Profit	46,253	$41,036	17%	6.5%
Desert Valley Hospital	Victorville, CA	148	Private Hospital	122,225	$45,894	26.0%	15.80%
Chino Valley Medical Center	Chino, CA	126	Private Hospital	85,595	$72,872	11.6%	13.5%

Case Studies of Ransomware Incidents

Hollywood Presbyterian Medical Center

Hollywood Presbyterian Medical Center is a private hospital located in the Los Angeles, California area. Table 3 provides demographic characteristics for this hospital. The organization offers a variety of services from emergency care to comprehensive cardiac care, as well as transitional and long term care and is fully accredited by the Joint Commission. In February of 2016, the staff at the hospital experienced issues with their hospital network system which opened an investigation by the IT department. The investigation revealed that the hospital network system had been hit by a ransomware virus and the system would be held hostage until the ransom was paid. The hackers responsible for the attack requested a ransom payment of 40 Bitcoins, the equivalent of approximately $17,000, from the organization to release hold of their electronic health system so they could resume patient care (Trubridge, 2017). During the time of the attack, it was impossible for healthcare professionals to adequately provide care to patients, electronically document patient care, complete lab work, share patient records and review medical history (McDonald, & Silberman, 2016). After ten days, the hospital leadership team determined that it was best to pay the ransom of 40 Bitcoins so that the organization could regain the access to their network system and resume normal patient care. The leadership team decided this was the most efficient way to restore the systems to restore normal operations (Stefanek, 2016).

Table 3: Demographic Characteristics of Hollywood Presbyterian Medical Center

Organization	Hollywood Presbyterian Medical Center
Location	Los Angeles, CA
# Beds	434
Status	Private Hospital
Population Size	10,137,915
Median Household Income	$56,196
% Persons in Poverty	16.7%
% Persons without health insurance under 65	12.5%

MedStar Health

MedStar Health, composed of 10 hospitals, is the largest healthcare provider in the Maryland and Washington, D.C. region. The organization provides aspects of academic medicine, research and innovation as well as a variety of clinical services for patient care (https://www.medstarhealth.org/mhs/about-medstar/#q={}). Table 4 provides demographic characteristics for this hospital. In March 2016, the hospital chain received complaints from users not being able to access their electronic information systems for clinical care. An investigation concluded that the hospital had become a victim of a ransomware attack. The attack included a digital ransom note where the hackers requested 3 Bitcoins, the equivalent of $1250, to unlock a single computer or 45 Bitcoins, the equivalent of $18,500, to unlock all of the computers. The research did not disclose which particular MedStar facility was the direct target of the ransomware attack. As a precaution, when learning one of their hospitals had become a victim of a ransomware attack, the organization acted quickly to take down all system interfaces to prevent the virus from spreading throughout the entire organization potentially causing severe damage. During this time, all facilities were directed to use back-up systems and revert to paper medical records for clinical care. Within 48 hours of the attack, MedStar's IT team had moved to fully restore the three main clinical information systems supporting patient care. Additionally, there were other clinical systems to be restored, but priority was given to those related to patient care. Research indicated Medstar Health used an application server that was vulnerable to hacking due to a misconfiguration that allowed for unauthorized access from users outside of the organization. (Ragan, 2016).

Table 4: Demographic Characteristics of MedStar Health

Organization (MedStar Health System)	**Location**	**# Beds**	**Status**	**Population Size**	**Median Household Income**	**% Persons in Poverty**	**% Persons without health insurance under 65**
MedStar Franklin Square Medical Center	Baltimore County, MD	378	Not-for-Profit	831,026	$67,095	9.1%	6.8%
MedStar Georgetown University Hospital	Northwest Washington, D.C.	609	Not-for-Profit	681,170	$70,848	17.3%	5.8%
MedStar Good Samaritan Hospital	Baltimore, MD	317	Not-for-Profit	831,026	$67,095	9.1%	6.8%
MedStar Harbor Hospital	Baltimore, MD	150	Not-for-Profit	831,026	$67,095	9.1%	6.8%
MedStar Montgomery Medical Center	Olney, MD	149	Not-for-Profit	*	$133,121	2.6%	3.8%
MedStar National Rehabilitation Network	Northwest Washington, D.C.	137	Not-for-Profit	681,170	$70,848	17.3%	5.8%
MedStar St.Mary's Hospital	St. Mary's County, MD	103	Not-for-Profit	112,587	$86,987	8.7%	5.0%
MedStar Southern Maryland Hospital	Clinton, MD	262	Not-for-Profit	*	$103,678	4.0%	6.5%
MedStar Union Memorial Hospital	Baltimore, MD	283	Not-for-Profit	831,026	$67,095	9.1%	6.8%
MedStar Washington	Northwest Washington	926	Not-for-	681,170	$70,848	17.3%	5.8%

Hospital	n, D.C.		Profit				

* Information not provided

Methodist Hospital

Methodist hospital is an acute care hospital located in Henderson, Kentucky. The hospital provides a range of services from general medical to surgical care for inpatient, outpatient and emergency room patients. Table 5 provides demographic characteristics for this hospital. In March of 2016, the hospital was hit with ransomware when it infected a computer through an attachment on a spam-email and attempted to spread throughout the network. The hackers provided a ransom note demanding 4 Bitcoins, equivalent to $1600, to unlock the infected machines for the hospital to return to normal (Trubridge, 2017). During this time, the hospital implemented their internal emergency alerts that placed messages on the homepage that indicated they were operating on an internal state of emergency (Pritts, 2016). The hospital took necessary steps to prevent the entire network from being infected by immediately shutting down all of the systems and transferring services to its backup system while the primary system was impacted with the ransomware virus (Kern, 2016). The initial reports indicated the hospital leadership team was considering paying the ransom to regain control of their systems. After five days of downtime, the hospital was able to recover and restore their systems from backups and did not pay the ransom that was being demanded by the hackers (Pritts, 2016). The hospital reported taking action of restructuring their network to minimize the potential for infection through a similar attack in the future.

Table 5: Demographic Characteristics of Methodist Hospital

Organization	Methodist Hospital
Location	Henderson, KY
# Beds	217
Status	Not-for-Profit
Population Size	46,253
Median Household Income	$41,036
% Persons in Poverty	17%
% Persons without health insurance under 65	6.5%

Desert Valley Hospital

Desert Valley Hospital, a member of the Prime Healthcare network, is a hospital located in the Victorville, California area. The hospital is an acute care medical center that provides state-of-the-art, health care to its community. Table 6 provides demographic characteristics for this hospital. In March of 2016, Desert Valley Hospital reported server disruptions that were determined to be associated with a ransomware attack. The reports made available to the public did not disclose the ransom amount the hackers were seeking. The hospital was able to shut down their systems to prevent the spread of the virus to the entire network (Pritts, 2016). Reports indicated that the organization was able to immediately implement their protocols and procedures to contain and mitigate the disruptions and the hospital was able to remain operational without impacting the safety of its patients (Snell, 2016). The hospital was able to quickly react to the ransomware attack indicating they had a good defense strategy to fight off the attack without having to pay the ransom.

Table 6: Demographic Characteristics of Desert Valley Hospital

Organization (Prime Healthcare)	Desert Valley Hospital
Location	Victorville, CA
# Beds	148
Status	Private Hospital
Population Size	122,225
Median Household Income	$45,894
% Persons in Poverty	26.0%
% Persons without health insurance under 65	15.80%

Chino Valley Medical Center

Chino Valley Medical Center, a member of the Prime Healthcare network, is a hospital located in the Chino, California area. The hospital provides emergency services as well as an intensive care unit and full radiological and laboratory services. Table 7 provides demographic characteristics for this hospital. In March of 2016, Chino Valley Medical Center reported having a disruption within their network server. After an investigation, it was determined that the organization had become a victim of ransomware attack. The research did not indicate a disclosed amount for the ransom. The hospital was able to shut down their information systems to prevent the virus from spreading and infecting the entire network (Pritts, 2016). Through research, reports indicated that the organization was able to immediately implement protocols and procedures that were beneficial in helping to contain and mitigate the disruptions which allowed the hospital to remain operational without impacting the safety of its patients and their electronic medical records and ancillary systems (Snell, 2016). The hospital had a good defense strategy in place that allowed them to fight off the attack without having to pay the ransom and was able to have control of their systems.

Table 7: Demographic Characteristics of Chino Valley Medical Center

Organization (Prime Healthcare)	Chino Valley Medical Center
Location	Chino, CA
# Beds	126
Status	Private Hospital
Population Size	85,595
Median Household Income	$72,872
% Persons in Poverty	11.6%
% Persons without health insurance under 65	13.5%

In table 8, we display a high-level view of the organizations and if they were at risk in the particular category. In using the NIST Framework to analyze the data, we were able to determine that all five (100%) of the hospitals met requirements in 3 of the 5 categories we indicated as risk factors. The hospitals performed well in the categories of “identify”, “protect” and “recover” when they were victims of ransomware attacks. The research concluded that hospitals were able to quickly identify that their systems had been hacked. The hospitals were also able to protect and eventually recover their systems by paying the ransom or through their backup systems.

There were 3 of the 5 hospitals (60%), that performed well in the "detect" category and only 2 of the 5 hospitals (40%) performed well in the "respond" category. The research concluded that the hospitals did not always provide detailed information surrounding the events of their ransomware attacks, which made it difficult to determine if the hospital was at risk for the category.

Of the hospital characteristics, there were no significant similarities that stood out among them that made their organization targets for the ransomware attacks. Hospitals were located in regions of the west coast, east coast and the south. The hospitals all ranged in sizes from small to large and were located in rural and urban areas. Due to the hospitals locations, it is difficult to speculate how and why the hackers selected the organizations identified in this study.

Table 8: Identified Risk Factors

Organization	Risk Factors					
	Identify	Protect	Detect	Respond	Recover	Total n(%)
Hollywood Presbyterian Medical Center	x	x	x	x	x	5 (100%)
*MedStar Health	x	x	x		x	4 (80%)
Methodist Hospital	x	x	x	x	x	5 (100%)
**Desert Valley Hospital	x	x			x	3

						(60%)
**Chino Valley Medical Center	x	x			x	3 (60%)
Total n(%)	5 (100%)	5 (100%)	3 (60%)	2 (40%)	5 (100%)	

Consists of multiple facilities

*****Prime Healthcare Facilities***

X Indicates information identified for this category from research

V. DISCUSSION

In total we reviewed data for five hospitals that were affected by ransomware attacks between 2015 and 2016. In conducting the content analysis, we learned that hospitals were not transparent in reporting detailed information surrounding the events of the ransomware attacks they encountered. There are no known reasons to justify as to why the hospitals only provided limited information to the public about their ransomware attacks. A speculation for the failure to share the information is the hospitals fear they may lose current and potential patients when they learn what has happened at the organization. With the hospital industry continuously learning about the challenges that are faced with utilizing information technology for clinical care, it's important to share this information so other organizations are aware of what happened and how the affected organization recovered from the attack. The primary risk factor among hospitals was the failure to properly update security patches to their network systems. The failure to complete this step made networks vulnerable to unauthorized users which resulted in the success of ransomware attacks.

The research of the individual cases always led back to the case of the Hollywood Presbyterian Medical Center attack in Los Angeles, California. The research provided detailed information about what this hospital experienced and the steps they took to regain control of their hospital network. Because of the risk of patient care involved during ransomware attacks, organizations should be aware of what vulnerabilities their organization have if any when it comes to their network systems.

Table 8, we displayed a high-level view of the organizations and if they were at risk for a particular category. In conducting the research, we were able to identify information for most of the hospitals in a majority of the categories. Both Hollywood Presbyterian Medical Center and Methodist Hospital provided information that was able to be applied to each of the categories. There is no link between these two hospitals that would indicate why more information was provided than the other hospitals. We were able to locate information on MedStar Health for all categories except the respond category. This particular case is a large health system that includes multiple hospitals, but there was a lack of information of their ransomware attack events. This could be potentially due to the health system not wanting to share detailed accounts with the public that would cause fear among the healthcare consumers in their region. Desert Valley Hospital and Chino Valley Medical Center are separate hospitals but fall under the Prime Healthcare network. In our research for these two hospitals, there was limited information that was useful to be applied to all of the categories, and this could be due to both hospitals being smaller in size compared to the other hospitals and fear of a reduction of their small patient population.

The amount of information available by both Hollywood Presbyterian Medical Center and Methodist hospital indicates that these organizations wanted to be open to the public about what their hospitals had dealt with and how they were able to overcome the obstacles. In healthcare, most consumers usually tend to visit hospitals that do are not reported negatively in the news. Events of ransomware attacks could potentially raise flags among healthcare seekers, instilling fear that the hospital is not safe with their information. However, the hospitals should be more transparent with reporting the information and informing the public of how they plan to prevent these types of events from happening in the future by being proactive with their information security program.

The results of this study support that there is no transparency in how organizations are responding and recovering from ransomware attacks. Due to the lack of information reported to the public of how the hospitals are reacting to these attacks, there are limitations in determining what the risk factors each hospital may individually have. The limited information from the hospitals prevents the healthcare industry from gaining knowledge that could potentially play a role in fighting the possibility of future ransomware attacks. Due to the healthcare industry not being veterans in IT when it comes to clinical care, we can expect to see an increase in ransomware attacks among the healthcare industry.

During the events of the ransomware attacks that targeted these hospitals, research indicated that information systems and networks were down between 48 hours and 10 days. When a hospital has to operate in a down-time situation, this could lead to other disasters for the organization. From the loss of revenue for their facility as well as placing patients at risk when it comes to their medical care, hospitals must be prepared to quickly recover from the event to a normal operating schedule.

Next Steps

What’s Next?

Ransomware attacks are not limited to hospitals in the healthcare industry. In the events that have taken place, the hospitals that have been victims of ransomware attacks were able to either pay the ransom or restore their systems from backups. In the case of

Hollywood Presbyterian Medical Center, they paid the ransom of $17,000 to regain control of their systems. If ransomware attacks continue to happen in the healthcare industry, we can expect to see them expand beyond hospital facilities and start to affect physician practices. Considering that physician practices are smaller than hospitals, we can speculate that a ransomware attack could be disastrous to the organization and could produce catastrophic results that could potential require the practice to shut-down operations completely and permanently.

Framework

The cybersecurity framework currently has five functions that organized activities by level with categories associated with each function. The functions organize activities at their highest level and aid in organization in managing its cybersecurity risk by organizing information enabling risk management decisions, addressing threads and improving by learning from previous activities (NIST, 2014). In the current framework developed by NIST, communications is listed as a category under the respond and recover function. Considering communications play a major role in the operations of a hospital, the framework should be modified for the healthcare industry to list this category as a function and placed between the protect and detect functions.

Policy Implications

In the cases of the ransomware attacks that have taken place, they have all affected electronic medical records by eliminating access by users to the systems. Most hospitals have purchased electronic medical record systems from major software vendors that have developed these systems for healthcare. As ransomware has begun to affect these systems, there is a need to determine who should be held accountable for this happening, whether it is the hospital or the vendor. It is speculated that ransomware attacks will continue to happen in the healthcare industry in the future. With this speculation, there is a possibility that the government will need introduce regulations that will hold the software companies responsible for the software systems they develop and sell to healthcare organizations. This could be due to the software companies not having tested their products thoroughly and making sure safeguards are in place that prevents unauthorized access by users that are outside the organization.

Recommendations

In light of past ransomware attacks, hospitals should start to review their networks on a consistent schedule, put new protocols in place and utilize best practices established by the cybersecurity industry. Taking these steps will allow the organization to frequently review their systems for any possibilities of vulnerabilities. In conducting a review of literature that discussed ways to prevent being victims of ransomware attacks, we selected recommendations and created a checklist for hospitals to utilize and validate their security program. See Table 9 for complete checklist.

- “Back up network/systems so recovery is easy” (Zetter, 2016) – This step should be taken so that in the event of a ransomware attack, the hospital can try and recover their systems without having to pay the ransom. In completing this step up on a daily basis, the hospital should be comfortable knowing that if they are affected, they could restore their systems from the saved backup from the previous day. This action could save the hospital thousands of dollars due to paying the ransom or a loss of revenue.

- "Review and validate server backup processes" (Mellen, 2016) – This step should be taken to verify the backup is complete and data is useful. In completing this action, the hospital will know that the precautions they are taking are useful and can be relied upon in the future if there is an event that causes for backup to take place. This process can be a manual or automated process that the organization can frequently test for the reliability of the backup.
- "Review your monthly patch management processes" (Mellen, 2016) –This step should be taken to ensure there are no vulnerabilities within the network. This action helps to mitigate potential risks to the integrity of the systems. Reviewing the processes ensures that they are continually effective to the organization in providing protection where needed.
- "Apply any new applicable security patches made available" (Zetter, 2016) – Complete this step to ensure all security patches are up to date. Automatic updates to software on computers and networks can happen without a user being aware, so it is important that this process is monitored on a monthly basis to ensure the safeguards in place will function the way they are designed to function.
- "Ensure that system software is up to date (operating system, browser plug-ins, etc.)" (Norton, N.D.) – This step should be taken to verify computers are not using outdated versions that could potentially place the hospital at risk of an attack. New viruses are always occurring, and when software is not updated

regularly, this could potentially lead to unauthorized access by hackers to infiltrate a device with multiple viruses.

- “Evaluate inbound spam and malware protection” (Mellen, 2016) – This step is done to ensure the software is properly protecting users. Spam and malware protection plays a major role in protection users and networks by filtering out things and allowing a user to review before allowing entry. This protects users that are normally connected to a larger network that will lower the possibility of an infection getting to a network through a single user.
- “Ensure security software is up to date with current subscription” (Norton, N.D.) – Complete this step to verify the software has the most recent release. Taking this action plays a role in saving the organization time and money to have to deal with events that were created due to the lack of security software. This has to be a regular practice for hospitals considering the amount of patient data that is shared electronically on a routinely basis.
- “Validate that you are leveraging the full set of protection features in your security product” (Norton, N.D.) – This is done to ensure the security software is functioning properly at a level of safety for the organization. In validating this information, it leads the organization to determine if they are not fully utilizing their security product at maximum capacity
- “Validate security management process, which includes a risk analysis to identify threats and vulnerabilities and implementing security measures to mitigate or remediate those risks” (HHS, 2016) – This is done to evaluate whether the procedures in place are current or should be updated. For the

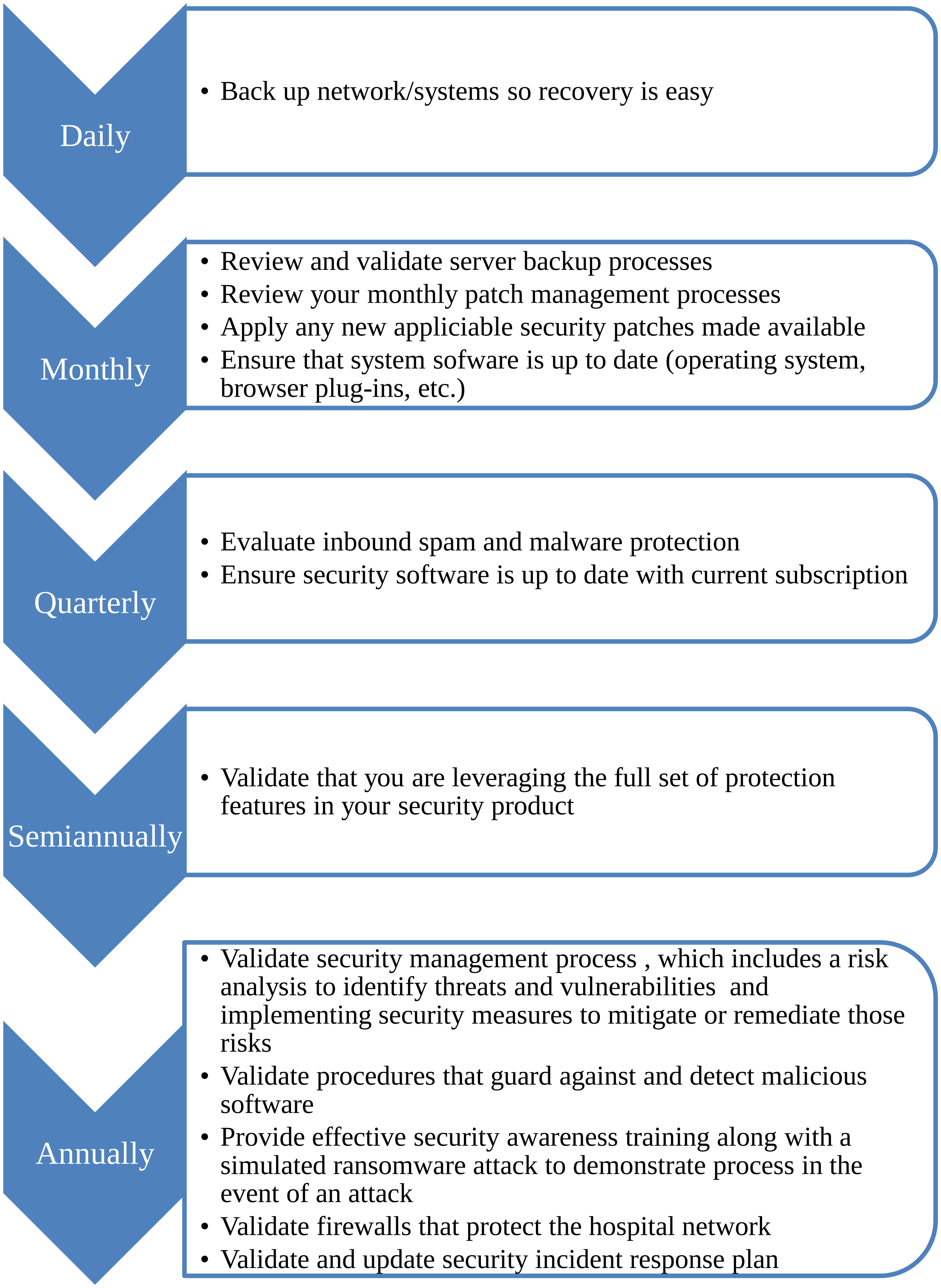
hospital industry, they should conduct these risk analyses to be sure that they are current and up to date with their security program and what actions they are going to take if they have to deal with potential threats to their systems.

- "Validate procedures that guard against and detect malicious software" (Alessandrini, 2016) – This should be completed to ensure procedures are current with any new known malware types. Taking the action in validating these procedures will provide the organization with the opportunity to prevent events that are malicious to the hospital.
- "Provide effective security awareness training along with a simulated ransomware attack to demonstrate process in the event of an attack" (HHS, 2016) – This should be completed so that staff is aware of what to look for, and what to expect in the event of the hospital having to revert to a down-time process due to a hacking event. Taking this action will give the organization exposure to what could potentially happen in the event they are faced with a ransomware attack and know how to quickly transition to operate in those types of situations.
- "Validate firewalls that protect the hospital network" (Weil, 2017) – This should be done to verify the hospital is protecting their infrastructure from unauthorized users. Taking actions to verify the hospital network is protected provides an extra layer of comfort and protection to the organization in knowing they are protected to a certain level.
- "Validate and update security incident response plan" (Mellen, 2016) – This should be done so there is documentation available to staff in the event of a

catastrophic disaster that can delay communication among the organization. Taking the action to validate and update the plan indicates the hospital is dedicated to providing a level of security to their organization and would like for everyone to be aware of what to anticipate and how they are expected to play a role during the time of an unforeseen event.

Although these are our recommendations to prevent becoming a victim of a ransomware attack, hospital leadership teams should require their IT departments to have a security program in place that remains current with the best practices that are suggested by the cybersecurity industry. The security program could be effective in preventing their hospital systems from being accessed by hackers. In using these recommendations, hospitals should keep in mind and be aware that only having these polices in place will not guarantee protection, but it is important that they actively follow the plans they have in place.

Table 9: Ransomware Attack Prevention Checklist



Daily	• Back up network/systems so recovery is easy
Monthly	• Review and validate server backup processes • Review your monthly patch management processes • Apply any new appliciable security patches made available • Ensure that system sofware is up to date (operating system, browser plug-ins, etc.)
Quarterly	• Evaluate inbound spam and malware protection • Ensure security software is up to date with current subscription
Semiannually	• Validate that you are leveraging the full set of protection features in your security product
Annually	• Validate security management process , which includes a risk analysis to identify threats and vulnerabilities and implementing security measures to mitigate or remediate those risks • Validate procedures that guard against and detect malicious software • Provide effective security awareness training along with a simulated ransomware attack to demonstrate process in the event of an attack • Validate firewalls that protect the hospital network • Validate and update security incident response plan

Future Research

The focus of this research was to determine what the risk factors for hospital ransomware attacks were based on a review of hospitals that were targets in 2015 and 2016. Additional research should be conducted to evaluate whether there are any direct characteristics that links hospitals together to be victims of ransomware attacks. Further research should be conducted to determine what hospitals are doing internally to prevent being targets of ransomware attacks and how they provide that information to the industry.

Conclusion

Overall, study results demonstrate that there are risk factors for hospitals to become targets for ransomware attacks. Hospitals have recently started to utilize information technology on a regular basis for patient care. In any industry, information systems and networks have the potential for vulnerabilities when they are not routinely evaluated to ensure there are no possibilities for hacking. Implementing the checklist proposed in this research provides hospitals with steps they can take at being proactive to lessen their chances of being victims of ransomware attacks.

REFERENCES

Al-Ahmad, W., & Mohammad, B. (2013). Addressing information security risks by adopting standards. *International Journal of Information Security Science, 2*(2), 28-43. Retrieved from http://search.ebscohost.com.proxy.cc.uic.edu/login.aspx?direct=true&db=a9h&AN=93598603&site=ehost-live

Alessandrini, A. (2016). RANSOMWARE Hostage Rescue Manual: https://www.wired.com/wp-content/uploads/2016/03/RansomwareManual-1.pdf

Bush, M., Lederer, A. L., Li, X., Palmisano, J., & Rao, S. (2009). The alignment of information

systems with organizational objectives and strategies in health care. International Journal of Medical Informatics, 78(7), 446-456. doi:10.1016/j.ijmedinf.2009.02.004

http://www.businessdictionary.com/definition/information-technology-IT.html

Callahan, M. E. (2016). What hospitals need to know about ransomware. *AHA News, 52*(5), 4-5. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=hch&AN=113495310&site=ehost-live

Census. (2017). United states census bureau: https://census.gov/

Cohen, J. (2016). HHS lists health IT as a top management challenge: http://www.beckershospitalreview.com/healthcare-information-technology/hhs-lists-health-it-as-a-top-management-challenge.html

Ferreira, A., Antunes, L., Chadwick, D., & Correia, R. (2010). Grounding information security in healthcare. *International Journal of Medical Informatics*, *79*(4), 268-283. doi:http://dx.doi.org.proxy.cc.uic.edu/10.1016/j.ijmedinf.2010.01.009

Gagliardi, A.R. and Brouwers, M.C. (2012). Integrating guideline development and implementation: analysis of guideline development manual instructions for generating implementation advice. Implementation Science 2012 7:67. doi:10.1186/1748-5908-7-67

HHS. (2016). FACT SHEET: Ransomware and HIPAA: https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

Kaspersky (2017).
https://usa.kaspersky.com/internetsecuritycenter/definitions/ransomware#.WBvRYsn-WxY

Kern, Christine. (2016). Backup and recovery systems allow Methodist hospital to regain control
after ransomware attack: https://www.healthitoutcomes.com/doc/backup-recovery-system-control-ransomware-attack-0001

Kim Dohoon D. (2015). Method for detecting core malware sites related to biomedical information systems. *Computational Mathematical Methods in Medicine, 2015* Retrieved from /z-wcorg/ database.

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology & Health Care, 25(1), 1-10. doi:10.3233/THC-161263

Ladika Susan S. (2016-12). Health care, an easy target, needs to get its guard up. *Managed Care (Langhorne, Pa.), 25*(12) Retrieved from /z-wcorg/ database.

Marketwired. (2017). Bitglass report: 87 percent of organizations report cyber attacks as breaches surge in 2016: http://finance.yahoo.com/news/bitglass-report-87-percent-organizations-120000940.html

Mehraeen Esmaeil E. (2016-2). Health information security in hospitals: The application of security safeguards. *Acta Informatica Medica, 24*(1), 47-50. Retrieved from /z-wcorg/ database.

Mellen, M. (2016). HIT Think How to prevent ransomware attacks:
https://www.healthdatamanagement.com/opinion/how-healthcare-providers-can-prevent-ransomware-attacks

McDonald, Alexandra A. &Silberman, Gregory P. (2016-08). Hospitals and Healthcare Systems Are the New Ransomware Target: How to Avoid Becoming a Hostage: http://www.jonesday.com/files/Publication/4009efd5-36ea-45eb-b8ed-e3aabd78643f/Presentation/PublicationAttachment/529d47d4-4a0f-4a52-9367-a2808b2df588/hospital%20ransomware.pdf

Nichols, Jeremy. (2016). Information security game plan: Is your information security program ready to go pro?: https://www.solutionary.com/resource-center/blog/2016/09/information-security-game-plan/

NIST. (2014). Framework for Improving Critical Infrastructure Cybersecurity: https://www.nist.gov/cyberframework

Norton. (N.D.). Ransomware on the rise: Norton tips on how to prevent getting infected: https://us.norton.com/ransomware/article

Office of National Coordinator (2016). https://www.healthit.gov/newsroom/about-onc

Patel Vaishali V. (2015-4-02). The role of health care experience and consumer information efficacy in shaping privacy and security perceptions of medical records: National consumer survey results. *JMIR Medical Informatics, 3*(2) Retrieved from /z-wcorg/ database.

Pritts, Gary. (2016). 2016: Hospitals targeted with Ransomware, patients harmed, losses incurred: https://eagleconsultingpartners.com/threat-intelligence/2016-hospitals-targeted-ransomware-patients-harmed-losses-incurred

Ragan, Steve. (2016). http://www.csoonline.com/article/3048825/security/ransomware-attack-hits-medstar-health-network-offline.html

Regional Extention Centers (2015). https://www.healthit.gov/providers-professionals/regional-extension-centers-recs

Sittig Dean F DF. (2016). A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks. *Applied Clinical Informatics, 7*(2), 624-32. Retrieved from /z-wcorg/ database.

Snell, Elizabeth. (2016). Healthcare ransomware cases highlight security needs: http://healthitsecurity.com/news/healthcare-ransomware-cases-highlight-security-needs

Stefanek, Allen. (2016). Letter from Hollywood Presbyterian Medical Center CEO:http://hollywoodpresbyterian.com/default/assets/File/20160217%20Memo%20from%20the%20CEO%20v2.pdf

Trubridge (2017). http://www.trubridge.com/sites/default/files/TruBridge___Ransomware_Prevention_Tips.pdf

Kaspersky (2017). https://usa.kaspersky.com/internetsecuritycenter/definitions/ransomware#.WBvRYsn-WxY

Van Alstin, C. M. (2016). Ransomware: It's as scary as it sounds. Health Management Technology, 37(4), 26-27 2p. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=rzh&AN=115717524&site=ehost-live

Virga, P. H., Jin, B., Thomas, J., & Virodov, S. (2012). Electronic health information technology as a tool for improving quality of care and health outcomes for HIV/AIDS patients. *International Journal of Medical Informatics, 81*(10), e39-e45. doi:10.1016/j.ijmedinf.2012.06.006

Weil, S. (2016). HIT Think How 4 key practices can prevent ransomware incidents: https://www.healthdatamanagement.com/opinion/how-4-key-practices-can-prevent-ransomware-incidents

Zarei Javad J. (2016). Information security risk management for computerized health information systems in hospitals: A case study of iran. *Risk Management and Healthcare Policy, 9*, 75-85. Retrieved from /z-wcorg/ database.

Zetter, K. (2016). 4 Ways to Protect Against the Very Real Threat of Ransomware: https://www.wired.com/2016/05/4-ways-protect-ransomware-youre-target/