8-2021

IT Security Technology and Staffing Investments for Small and Mid-Sized Healthcare Organizations in Response to Increased Threats

Dylan Dudlext
of6764xd@go.minnstate.edu

IT Security Technology and Staffing Investments for Small and Mid-Sized Healthcare Organizations in Response to Increased Threats

A Thesis

Submitted to the Faculty

of the Department of Leadership Education

College of Education

of Winona State University

by

Dylan D. Dudlext

In Partial Fulfillment of the Requirements

for the Degree of

Master of Science

August 4, 2021

Contents

Chapter 1 Introduction

Research shows that over seventy percent of organizations have been identified as utilizing outdated security software when their networks were attacked (Connolly, 2019). Protecting data from unauthorized access and exfiltration is one of the core commitments of cybersecurity. Organizations in every industry must face the reality that the data they use to conduct business is valuable to other organizations as well as bad actors. As a result, industry leaders must ensure to take steps towards adequately protecting the confidentiality, integrity, and availability of organizational data. Striking the balance between keeping data safe and readily available, while not spending too much money to do so, is the challenge these industry leaders face while navigating an increasingly complex threat landscape. Healthcare is no exception and the uniquely valuable data and personal information needed in this industry continue to be more and more targeted, requiring investments in IT security.

Problem Statement

Cybersecurity concerns in the healthcare industry continue to rise and associated threats have increased as this industry continues to be a target (HIPAA Journal, 2020). Specifically, organizations are facing tough decisions beyond complying with regulatory requirements as they prepare to ward internal networks from more advanced threats. This issue is particularly difficult for small to mid-sized healthcare organizations who may not have sufficient budgets, resources, and/or dedicated information technology staff to address these issues in comparison to major medical centers.

Small to mid-sized healthcare organizations face unique staffing and technology decisions. In the face of recent cybersecurity threats, these decisions continue to be reactive, justifying the cost for new services, staff, or tools only after a cyber incident occurred. There

continues to be limited information on this subject due to the sensitive nature of cybersecurity decision making and with most of the information on security practices rising from a cyber incident or security breach making news headlines. According to Angst et al. (2020), with the combination of these headline making incidents and regulatory requirements, healthcare companies are placing IT security at the top of strategic agendas.

Background of the Problem

The Department of Health and Human Services' Office for Civil Rights (OCR) reported 3,705 healthcare data breaches of 500 or more records between 2009 and 2020. According to an article from an online publication, *The HIPAA Journal*, it concluded those breaches have resulted in the loss, theft, exposure, or impermissible disclosure of over 268 million healthcare records after compiling available information from OCR (HIPAA Journal, 2020). It is clear from the article that this trend has been increasing. The article describes this trend by showing that major breaches, involving 500 or more compromised records, were being reported at a rate of around one breach per day in 2018 and shows that by December 2020, this rate had already doubled (HIPAA Journal, 2020).

In addition to a consistent increase in reported breaches, a joint alert was made by the Cybersecurity & Infrastructure Agency (CISA), Federal Bureau of Investigation and Department of Health and Human Services in October 2020 regarding credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers (CISA, 2019). As the threat of breaches continue to rise, healthcare organizations are not prepared to defend against cybersecurity incidents. Leaders in this industry need to recognize and begin proactively mitigating these threats through investment in necessary resources, policies, and personnel before suffering a cybersecurity breach.

Purpose Statement

The purpose of this qualitative study was to identify the risk awareness and risk responses of small to mid-sized healthcare organizations due to increased cybersecurity threats to the healthcare industry.

Research Questions

The main objective of this study was the evaluation of the following questions. How has the recent increased threats of ransomware in the healthcare industry affected small and mid-sized healthcare organization's IT Security budget and staffing decisions? How aware are these organizations of recent threats to the healthcare sector?

Assumptions of the study

For this study, it was assumed that all healthcare organizations are facing increased threats and are taking actions to begin mitigating these threats as a result. Within healthcare, covered entities are obligated to secure the protected health information of patients and must make reasonable efforts to deploy technical, physical, and administrative safeguards to comply with regulatory requirements.

Limitations of the study

Organizations of all sizes have different exposure to and perception of these threats. There are diverse approaches to mitigation, limiting comparative qualitative review of information and resulting in potential inconsistent conclusions for this study. There was an expectation of a lower response rate for the survey due to lack of personal relationships with 4,000+ members. Organizations may have already been impacted by these threats or have leadership who perceive them to be real and tangible. Conversely, other organizations may be removed from these threats

and not act in a similar fashion to those who have already suffered a breach or other compromise of their data.

Delimitations of the study

Information from leaders in the industry was gathered from studies that draw conclusions from aggregate data or following a breach at a specific healthcare organization. Industry insight was to be limited to input from members of the H-ISAC community through use of a survey.

Definition of Terms

The following definitions are intended to aid in the understanding of this study and should be referenced when terms are mentioned throughout.

Breach

The Department of Health and Human Services (HHS) defines a breach as an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of protected health information (HHS, 2020).

Covered Entity

This is a term used in the HIPAA Privacy Rule, which refers to health plans, health care clearinghouses, and health care providers who must comply with requirements of the regulations (HHS, 2020).

Cybersecurity

The Cybersecurity & Infrastructure Security Agency defines Cybersecurity as the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information (CISA, 2019).

H-ISAC – Healthcare Information Sharing and Analysis Center

This is an online community made of healthcare cybersecurity leaders, designed for the efficient and timely sharing of relevant healthcare threats, vulnerabilities, indicators of compromise, best practices, and general communication amongst industry leaders.

PHI –Protected Health Information

The Privacy Rule under HIPAA defines PHI as all individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral (HHS, 2020).

Ransomware

A type of malicious software, or malware, that encrypts data on a computer making it unusable. A malicious cybercriminal holds the data hostage until the ransom is paid. Also, ransomware can be used by threating to destroy the victim's data or release it to the public (CISA, 2019).

Vulnerability

CISA describes vulnerabilities as flaws or errors in software, firmware, or hardware that can be exploited by an attacker to perform unauthorized actions in a system. Attackers or scammers may be able to take advantage of these errors to infect computers with malware or perform other malicious activity such as data exfiltration (CISA, 2019).

Summary

This chapter covered a brief introduction to the topic of cybersecurity in healthcare and provided an overview for the approach to this study. It went over the purpose, problem, background, and described the primary research question which drove the document's content. Additionally, this chapter served to cover the necessary assumptions, limitations, and

delimitations of the study. Lastly, all the key terms were clearly defined to aid in the understanding and interpretation of the content.

Chapter 2 Review of the Literature

Currently, many healthcare organizations are having to make necessary decisions beyond the actions necessary to comply with regulatory requirements. According to Angst et al. (2020), with the combination of those regulatory requirements and the headline making ransomware security incidents, many of these organizations are putting a focus on IT security in the strategic agendas used by leadership as they prepare to ward networks from more advanced threats. Cybersecurity concerns in the healthcare industry continue to rise and associated threats have increased as this industry continues to be a target (HIPAA Journal, 2020). This issue is particularly difficult for small to mid-sized healthcare organizations who may not have sufficient budgets, resources, and or dedicated information technology staff to address these issues in comparison to major medical centers. This chapter reviewed the history of the problem and provided a description of current trends.

History of the Problem

A modern definition of cybersecurity was created by three cybersecurity researchers Dan Craigen, Nadia Diakun-Thibault, and Randy Purse. After reviewing past definitions and current understandings of the term they concluded on the following definition, "Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights" (Craigen, 2014). The collective effort of this study to formulate the accumulative and disparate definitions into one coherent and succinct description help capture the history and current state of the cybersecurity problem. Healthcare organizations have been in a transformation process from predominately physically stored data into the modern and complexly vulnerable cyberspace in which data now exists.

The last decade presented organizations with the challenge of adopting historically paper-based documentation systems into the modern digital and electronic medical record systems. As the traversal of data takes place, the safeguards necessary to protect the information drastically change. Angst et al., described older hospitals which were established further in the past and whose data was largely collected on paper, as likely to be trailing other industries in the adoption of appropriate IT security by a wide margin (2020).

This study focused on the rising cybersecurity problems facing many organizations but seeks to do so through the lens of the healthcare industry. One concept Angst described is the use of symbolic adoption, in which an organization appears to be putting safeguards in place but not actually investing in the necessary resources. The authors explained it as being like a house with a beware of dog sign but not having a dog. The idea being that investment in the sign should be enough to ward off most thieves who would rather not risk it being true.

As organizations approach the necessity of protecting data in the digital age, some smaller and resource constrained organizations are seeking to appear to be making the investments without having to spend the money by utilizing what Connolly and Wall describe as symbolic IT (2019). Like the dog example above, organizations claim adherence to certain regulatory requirements but when audited they are found to be non-compliant. With the rise in recent breaches being tied to large fines from the Office for Civil Rights (OCR), organizations are time and again being found to not be in compliance with the expected and established requirements of regulations like the Health Insurance Portability Accountability Act (HIPAA), Payment Card Industry (PCI), Health Information Technology for Economic and Clinical Health Act (HITECH). One main cybersecurity threat which has the impact of revealing a lack of preparedness for organizations is known as ransomware.

Ransomware

In a piece titled *Taxonomizing Countermeasures*, Conolly and Wall described the ransomware landscape as a shifting and increasing threat (2019). The authors highlighted that over half of surveyed organizations at the time of writing confirmed being a victim of ransomware in the previous year of 2018. They described the healthcare industry as clearly leading the statistics as a target compared to energy, professional services, and even the retail sector. One major factor the pair highlight is that over seventy percent of organizations were identified as utilizing outdated security software when attacked and fifty four percent not having any security software in place (Connolly, 2019). This highlights the threat to all industries but specifically the difficulties faced by healthcare. Many health care organizations are not prepared to address these threats.

As Conolly and Wall researched further into the subject, they reached out to many facilities and reviewed available information on ransomware incidents. They found that many incidents occurred due to an organization's inability to monitor for and detect the threats in real time through use of antivirus (AV) software and firewalls which filter external content into internal networks (Connolly, 2019). They found a barrier to having the necessary software, hardware and updates to systems and networks was the costly potential of disrupting business operations. When systems are upgraded with AV and other patches to ward against new and emerging threats, some systems may work differently afterwards, presenting real and tangible risks to regular business operations. Lastly, even when costs were not a barrier, some unique applications or medical devices may not be able to function appropriately once upgraded.

The National Institute of Standards and Technology (NIST) in partnership the National Cybersecurity Center of Excellence (NCCOE) provided a special publication on the topic of

Securing Wireless Infusion Pumps (2018). It describes the unique challenge medical devices present when it comes to protecting data and IT networks from bad actors. The authors used infusion pumps as the focus, but many medical devices share the same inherent risks they described. They indicated modern wireless infusion pumps, like many medical devices, now connect to organizations IT networks, other devices, and the electronic health record to improve care delivery. However, the article was written to highlight the significant cybersecurity risks this connection introduced and the further associated safety risks infusion pumps present (O'Brien, 2018). Aside from the safety risks associated with a malfunctioning or tampered with medical device, these now serve as a potential vector into an organization's network, establishing that not only do organizations need the resource and expertise to secure network infrastructure but also any vended systems or machines they introduce to it as well.

Kruse and other researchers from Texas State University explore a systematic review of modern threats and trends in which they review extensive study materials on the subject to conclude two primary drivers for cyber threats in healthcare: rapid technological advancement and evolving federal policy (Kruse, 2017). They describe the industry struggling with new technology and security protocols, making them a high value target for cybercrime, emphasizing the measurable lag healthcare has compared to other leading industries in securing vital data. The researchers conclude that organizations focus resources for the maintenance of and protection of healthcare technology and patient information from unauthorized access, a challenge many organizations struggle with addressing.

Understanding Cybersecurity

Before an approach or solution can be agreed upon, organizations need to understand the cybersecurity problem fully. One article, written by multiple authors, titled, *Defining*

Cybersecurity, which was featured in the October 2014 *Technology Information Management Review,* attempted to clearly define cybersecurity. Using a detailed sampling of literature and established definitions, the team focused on identifying a more comprehensive and in-depth definition of the term cybersecurity that would account for its various applications. They identified and adapted nine definitions based on review of literature, which included non-technical aspects of security. Some of the definitions were from government entities like Department of Homeland Security and others were from University sources. They were not limited to American sources and included a definition used by Public Safety Canada. Stepping outside of the technical aspects of a cybersecurity definition appears to have allowed for more sources to be included in the review.

To adapt these into a unifying and encompassing definition, they took a thematic approach to recognize five areas in which they could categorize language. The first theme was "technological solutions". This theme was somewhat limited to the technology used to detect, mitigate, and investigate the second theme of "event". The second theme was much broader and accounts for both physical and technical events related to cybersecurity. The third theme was a group of concepts, "strategies, processes, and methods" which again incorporates many non-technical considerations and something unique to a given organization's size, budget, and industry. The fourth theme, "human engagement", speaks to the need to train and maintain a culture of awareness. Lastly, they identified "referent objects (of security)" as a theme as well (Craigen, 2014).

They describe the internet being a "scale-free network", essentially indicating that bad actors anywhere on the network can be expected to act in a similar manner (Craigen, 2014). They discuss the commoditizing of attack tools contributing to this aspect being adopted. This was

even more true today with the advent of script-kitties and the fee for service model of modern malware. This was an important consideration as the threats to large-scale organizations can still be faced by smaller ones. The reading gives a progression of a working definition and shares the feedback as to why it was criticized. It appears that as they reviewed and worked the definition, they were forced to continue to expand the language and move towards something less restrictive overall.

The definition shared earlier in this paper was the result of collective review, discussion, criticism and attempts to account for the broad range of cybersecurity. It accounts for the technical and non-technical, being broad enough to not be tied to one type of event that could be viewed as intentional, malicious, or accidental. It was unclear why they chose to use the de jure and de facto terms, but perhaps it was to help keep the definition succinct. The effect of these terms was to discuss property rights that may be tangible or perceived and impacted by an event.

As organizations begin understanding the scope of cybersecurity, by reviewing the content captured by Craigen's definition, they are identifying the areas requiring leadership's attention. Once these areas are identified, they can begin to address the issues and gaps by reviewing vendor and industry documents.

Staffing & Budgets and Leadership Awareness

Healthcare industry societies and associations, such as HIMSS (Healthcare Information Management Systems Society) and HCCA (Health Care Compliance Association), have surveyed their members to understand efforts related to staffing and budgets. For example, a 2020 HIMSS survey on cybersecurity revealed that only six percent of the information technology from their members' budget goes towards cybersecurity staff and systems (HIMSS, 2020). Additionally, the HCCA also surveyed their members to review budget and staff

benchmarking in 2020. The survey found that the larger the revenue an organization had corresponded with how large of a compliance team they staffed (HCCA, 2020). Despite surveys and information pointing to a lack of sufficient staffing and budgets, especially in smaller organizations generating less revenue, the cybersecurity community continues to lag in these areas due to a perceived lack of leadership awareness.

A recent study from ISC2 (International Information System Security Certification Consortium) surveyed security professionals. The study found that many of the professionals surveyed shared low morale due to lack of leadership awareness on cybersecurity concerns. The study also highlighted stress for security professionals stemming from cutbacks and changes to staffing related to cybersecurity (ISC2, 2020).

Aligning Industry Best Practices and Regulatory Requirements

In her industry briefing, Dr. Racovita highlights that the number of network connected medical devices has been constantly rising and that the personal medical information they expose has also been highly valuable. She indicated that the data healthcare organizations possess and utilize may be sought after even more so than financial information since it is used in medical fraud, the illegal acquisition of controlled substances and identity fraud. The briefing described the main approaches for cybersecurity: standards and policies, cyber labels, and risk-based approaches to focus on how much risk could occur and with what likelihood (Racovita, 2019).

The first approach of standards and policies was an area in which many organizations still struggle, OCR fines are often associated with a lack of administrative safeguards such as adequate policies and procedures. Having sufficient documentation in the form of updated and leadership approved policies, standards and procedures requires additional staff dedicated to the creation and maintenance of such documents. The next approach, Cyber labels, referred to the

creation and use of standardized information labels to aid organizations in securing medical devices as they introduce them to the environment. These labels would be created by the vendor and the utilizing organization would be able to quickly and easily identify the risks and necessary safeguards associated with the device.

Lastly, the risk-based approach was one already prescribed by the HIPAA security rule in which an appropriate assessment of the likelihood and impact of a risk to electronic protected health information must be conducted. Vendors want to avoid their brand being involved in headline making breaches and so have begun shifting efforts to educate and adhere to industry regulatory requirements. Healthcare organizations, both large and small, must make informed decisions on what safeguards, tools, and staff to invest in and what portion of the annual budget should be allocated to those efforts.

Summary

Organizations in the healthcare industry have historically taken a symbolic approach to cybersecurity, hoping that least-effort and cheap safeguards are sufficient to deter cyber criminals. However, many cyber criminals have begun to get more and more sophisticated and bold, approaching large and small organizations indiscriminately. This new approach was leaving unprepared healthcare facilities to suffer a breach, face paying ransom costs and or receive an associated regulatory fine. The small to mid-sized healthcare organizations are facing added challenges in acquiring necessary resources to do more than a symbolic security program, not being able to recognize the need for or afford the necessary software, hardware, and staff.

As we evaluate the history, threats, and trends of small to mid-sized healthcare organization cybersecurity decision making, an understanding of the appropriate methodology for conducting research on the topic was imperative. The next chapter explains how the research

was designed to evaluate the healthcare industry's response to increased cybersecurity threats and explore the necessary changes to staffing or security tools small to mid-sized healthcare organizations adopted in response.

Chapter 3 Research Methodology

Research Design

The research was conducted using qualitative methods, reviewing both scholarly and news articles related to the topic as well as gathering information via survey from a relevant population. The groups or communities observed were intended to include articles related to small to mid-sized hospitals and clinics, government agencies, as well as industry specific cybersecurity experts. These groups were accessed through online articles, resources, and supplemented by survey responses from members of the Health Information Sharing and Awareness Center (H-ISAC), which was described in further detail later in this chapter.

Poth and Creswell suggest that qualitative research be used when a problem or issue needs to be explored as opposed to relying on predetermined information from literature (2016). The rationale for using a qualitative approach for this study was to access up to date information related to recent threat alerts as well as to account for the sensitive nature of security related decisions. This information may be difficult to quantify, and most healthcare organizations are not likely to provide or discuss their vulnerabilities in a publication, survey, or study.

Over the course of the semester, information was collected from various databases, government announcements and news sources. Boolean operations designed to home in on the subject were utilized to identify current and relevant results from these sources. There was a focus given to reviewing articles which highlighted the increased threat to healthcare or described the lack of preparedness in the industry. Additionally, priority was given to more recent articles and those mentioning hiring decisions related to security threats. The survey was comprised of nine questions and covers respondent demographics, risk awareness, and risk response specific to the respondent's organization.

Sample and Setting

The setting for this study was the healthcare industry leaders from within the H-ISAC organization which was comprised of many organizations varying in size, complexity, and activity. Each of the 4,000+ members are in some way part of the healthcare industry whether as a provider, vendor, or other tertiary relation to healthcare. Geographically, this group was dispersed throughout the world but has a clear majority in the United States of America. This group was active in sharing information during any major cybersecurity events affecting healthcare and other industries. This includes the recent joint alert made by the Cybersecurity & Infrastructure Agency (CISA), Federal Bureau of Investigation and Department of Health and Human Services regarding credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers (CISA, 2019).

Additional examples of H-ISAC information exchanges include the sharing of indicators of compromise during zero-day events or during newly announced vulnerabilities for healthcare related devices or vendors. This community consistently discusses and shares guidance on policy, procedure, and industry best practices related to staffing, business or vendor relations, and security tools. Additionally, this group has consistent communication threads via email and an internal chat system which are both utilized to discuss the above topics more in depth. This study utilized a nine-question survey which was distributed to members and promoted by H-ISAC leadership for response.

Instruments

Survey responses were collected via an online tool which was made available via a listserv email and online chat correspondence to H-ISAC members. The link led to the Qualtrics survey tool where respondents could read consent information prior to agreeing to submit their

information. The survey covered three main areas: demographics, risk awareness, and risk response. Demographics was an assessment of the size and background of the organization which respondents belong. Risk awareness assessed organizational awareness of recent increase in threats to healthcare sector. Risk response gathered data on the technology and staff investments made by respondent's organization.

Data Collection

This research survey was intended to review any changes to staffing and investment in security tools made by small to mid-sized healthcare organizations due to increased cybersecurity threats to the healthcare industry. All data collected for this study was anonymous and was not linked back to any of the respondents identifying information. The survey utilized multiple choice, Likert-scale, and open-ended questions to review the three areas of demographics, risk awareness, and risk response.

Data Analysis

Using the Qualtrics tool, responses were reviewed and categorized based on respondent indicated demographics with a focus given to those from organizations of less than 2500 staff. The analysis was intended to identify unique themes and commonalities amongst respondents. Additionally, contrasting data was sought against the responses collected from respondents representing organizations larger than 5000 staff.

Summary

This chapter covered the methodology used for the qualitative research conducted. Additionally, it explained how the research design was utilized to evaluate the healthcare industry's response to increased cybersecurity threats and explore the necessary changes to

staffing or security tools small to mid-sized healthcare organizations adopted in response. Lastly, it explored the instruments and data analysis related to the captured survey information.

Chapter 4 Results

Introduction

This chapter provides an overview of the research sample and data analysis used in this study. The research questions used in the survey are displayed in a table for review. Details for each of the survey questions as well as responses are included in this chapter. Additionally, a brief analysis of the collected data was provided to highlight some basic themes identified.

Description of Sample

There were twenty-one H-ISAC members who participated in this study by completing an anonymous online survey. The survey was sent to four-thousand H-ISAC members, meaning there was less than one percent response rate. The participants were from organizations of various sizes and may have been from anywhere throughout the United States. The participants consisted of twelve individuals who identified as C-Level or Director of Information Security, five from Information Management Technology, three from Information Technology (Sys Admin, Network Architect, Workstation Support) and two Non-IT Incident Response Team members. Most respondents, thirteen in total, were from organizations larger than five thousand employees. The other nine respondents were from small to mid-sized organizations of less than five thousand.

Data Analysis

The survey consisted of three multiple-choice demographic questions to assess the size and background of the organization which respondents belong. Additionally, it contained three Likert scale questions to assess risk awareness by focusing on organizational awareness of recent threats. Lastly, the survey included three Likert scale questions and one open text question to gather data on the risk response by the respondent organizations regarding technology and staff

investments. Data was analyzed by tracking those that responded as small to mid-sized, under 2500 employees, against those that were over 2500 employees to identify trends and themes for each category. None of the respondents had fully outsourced security operations, half had dedicated staff and the remaining were a mix of dedicated cybersecurity or IT team members.

Table 1 details the responses from survey respondents regarding their organization's risk awareness and risk response related to recent increased threats to the healthcare sector.

Table 1

Survey Question	Response Count (%)			
	Strongly Disagree n=21	Somewhat Disagree n=21	Somewhat Agree n=21	Strongly Agree n=21
My organization provides adequate training and awareness to staff at all levels of the organization.	2 (10%)	3 (14%)	14 (67%)	2 (10%)
My organization participates in information sharing communities and ingests cybersecurity alerts from multiple vendor and government sources.	2 (10%)	0 (0%)	8 (38 %)	11 (52%)
Cybersecurity staff within my organization possess understanding of current and trending threats to the healthcare sector.	0 (0%)	2 (10%)	7 (33%)	12 (57%)
My organization has adequately invested in cybersecurity staffing.	5 (24%)	4 (19.0%)	9 (43%)	3 (14%)

My organization has adequately invested in cybersecurity technology.	2 (10%)	2 (10%)	10 (48%)	7 (33%)

Table 2 summarizes the investments made by each respondent's organization.

Table 2

Survey Question	Response			
	Staffing changes n=21	Technology/ Software n=21	Association/ Membership n=21	Outsourced service n=21
What are some of the investments or staff changes made by your organization due to emerging threats to the healthcare sector?	5 (24%)	8 (38%)	1 (5%)	4 (19%)

Most respondents, fourteen out of 21 (67%), somewhat agreed that their organization provides adequate training and awareness but only 10% strongly agreed. This was not surprising as security training and awareness has been one of the first security initiatives for most organizations. A combined five out of 21 (24%) somewhat or strongly disagreed that their organization provides adequate training and awareness indicating that a significant portion of organizations still have work to do in this area.

There was a high level of confidence that respondents' cybersecurity staff possess understanding of current and trending threats to the healthcare sector as only 10% somewhat disagreed and none strongly disagreed. This did not come as a surprise as many organizations rely on their cybersecurity staff to be the ones informed and protecting their computer networks.

In total, five out of 21 (24%) survey respondents strongly disagreed that their organization has adequately invested in cybersecurity staffing. This contrasted with the 3 out of 21 (14%) who strongly agreed. Additionally, when looking at cyber technology, we see that seven out of 21 (33%) strongly agree their organization has adequately invested compared to two out of 21 (10%) who strongly disagree. This points to organizations first investing in technology over people or staff investments. This was further supported by eight of the 21 (38%) respondents indicating that their organization was investing in technology and software compared to the five out of 21 (24%) who indicated staffing changes.

Summary

The survey results pointed to themes relating to staff and technology challenges facing smaller organizations compared to larger ones. One theme was the move to outsourced security services for larger organizations. Additionally, a theme indicating an understanding of cybersecurity became clear from the survey results. Lastly, most respondents were from larger organizations and a theme of adequate risk awareness and response was present in their responses. This chapter covered the results of the survey and some of the major themes it presented. Chapter 5 goes into a deeper review of these results and draws further conclusions.

Chapter 5 Discussion and Conclusions

The purpose of this qualitative study was to identify the risk awareness and risk responses of small to mid-sized healthcare organizations due to increased cybersecurity threats to the healthcare industry. Prior sections provided a review of cybersecurity, associated relevant literature as well as the results of conducted study. This chapter reviewed the findings of the study in further detail, explored themes identified for questions posed and described conclusions drawn by review of the data. This research study was conducted using qualitative methods, reviewing both scholarly and news articles related to cybersecurity in healthcare and utilized a survey with leadership.

Questions

The following questions were used to guide the study:

RQ1

How has the recent increased threats of ransomware in the healthcare industry affected small and mid-sized healthcare organization's IT Security budget and staffing decisions?

RQ2

How aware are these organizations of recent threats to the healthcare sector?

Themes

Data was collected through use of a survey to members of the H-ISAC community, ranging in professional level and size of organization. Three themes became apparent for RQ1 (1) technology and software investments, (2) staffing changes, and (3) outsourcing security services. Additionally, three themes were identified for RQ2 (1) information sharing participation, (2) cybersecurity staff understanding current threats, and (3) organizations utilizing adequate training.

RQ1 Discussion

This section addresses how the recent increased threats of ransomware in the healthcare industry affected small and mid-sized healthcare organization's IT Security budget and staffing decisions.

Theme 1: Technology and Software

Though there was a mix of specific technologies identified, most respondents described various security tools or staff being introduced because of increased risks of ransomware. This ranged from data loss prevention technology, used to detect the exfiltration of sensitive data, to multifactor authentication technology used to authenticate users are legitimate. Additionally, many respondents described introducing anti-phishing technology to protect their users from malicious emails, links, and attachments. As Angst et al., described we see the healthcare industry trailing in the adoption of appropriate IT security measures. Ransomware has become a catalyst to begin adopting technology other industries have been already been utilizing (2019).

Theme 2: Staffing Changes

The theme of organizations modifying their workforce through various methods was made apparent by survey respondents. Throughout the spectrum of organizations represented in the survey, a change in staffing was apparent. This goes against the recent HIMSS and HCCA survey findings in which many of those surveyed indicated a lack of priority in hiring in this area (2020). Some organizations are seeking to reallocate or repurpose existing staff to support cybersecurity efforts while others are creating new roles within their organization.

Theme 3: Outsourcing Security Services

The respondents who represent larger organizations indicated staffing changes related to outsourcing security operations to an external managed risk and detection company. The work

completed by Conolly and Wall would indicate that organization's inability to monitor for threats may have sparked interest in outsourcing this need to external organizations (2019). The result is seeking out a service as opposed to identifying, hiring, or growing the necessary talent.

RQ2 Discussion

This section addresses how aware organizations are of recent threats to the healthcare sector.

Theme 1: Information Sharing Participation

Respondents to the survey overwhelmingly indicated that their organization participates in information sharing related to cybersecurity. This practice ensures the latest information potentially affecting healthcare organizations is quickly learned and acted upon. Understanding a threat is present and necessary to begin effectively mitigating or protecting against it. Dr. Racovita describes the volume of medical devices increasing in the industry, requiring adequate information to address the unique risks associated with each device (2019). This increase in information sharing participation can likely be tied to the need for relevant and timely information on new risks and vulnerabilities to the healthcare sector's unique data and technology footprint.

Theme 2: Cybersecurity Staff Understanding Current Threats

The survey results also indicate that staff expected to ward their organization against cybersecurity risks are well informed and aware of threats to the healthcare industry. Though respondents indicated a mix of dedicated staff, mixed staff, and outsourcing, nearly all respondents answered indicating agreement that their cybersecurity staff were aware of the increase in risks to the healthcare industry. This aligns in part with the data found in the recent ISC2 (International Information System Security Certification Consortium) study which showed

contrasting awareness between certified professionals and their leadership. Those who are certified and dedicated are perceived to have adequate knowledge, even if their leadership do not.

Theme 3: Organizations Utilizing Adequate Training

With over eighty percent of respondents agreeing or strongly agreeing that their organization provides adequate training, a clear theme was demonstrated that organizations are putting in an adequate effort to train their staff. Connolly and Wall described the symbolic adoption of IT (2019) as organizations appearing to implement security measures when, they have not acted. This high amount of user response shows that many organizations aren't just putting in a training program to say they have one but are putting forth the effort necessary to ensure it is adequate.

Conclusions

The survey and resulting themes lead to two main conclusions. The first was that in response to the recent increased threats of ransomware in the healthcare industry, small to mid-sized organizations are investing more in cybersecurity technology, staff and even outsourcing their security operations when their budgets allow. The second was that healthcare organizations are aware of the recent threats to the healthcare sector because of their cybersecurity staff utilizing information sharing and threat intelligence to stay informed of current risks. As a result of this research, there are leadership implications that can be drawn from the conclusions.

Conclusion 1: Leadership Implications

Regarding RQ1, when considering the current investment in staff and new technology, healthcare leaders should take a Systems Thinking perspective to ensure adequate adoption. This means they should be engaged in the evaluation of security related events, patterns, and structure

to guide their decision making related to security investments and new hires. Identifying these throughout their organization helps to inform their choices prior to implementing new security hardware, software, or external business relationships.

Additionally, healthcare leaders should seek to utilize the change leadership concept of a structural framework, described by Bolman and Deal, known as the practice of aligning all parts within an organization to produce optimal efficiency (2020). This framework can be applied to any newly defined security roles, processes as well as any impacted organizational structures to ensure the smooth implementation and operation of security practices.

Conclusion 2: Leadership Implications

Regarding RQ2, an implication from this research was the importance of organizational communication and its impact on an organization's awareness of recent threats to the healthcare sector. Most surveyed respondents felt their organization's cybersecurity staff had a strong awareness of the risks and indicated they participate in information sharing organizations. These relationships may require funding for participation. For leaders to create a culture of security throughout their organization and beyond their cybersecurity staff, it will require effective communication on multiple levels supporting both internal and external exchange of information. Survey results point to respondents' healthcare organizations sharing an awareness of the increased threats facing the industry, which indicates they may already have effective organizational communication coming from their leadership.

Recommendations for Future Research

This study helped identify a shift in healthcare organizations investing more resources into cybersecurity staff and technology. Future studies may be able to measure how effective implemented changes organizations made in response to recent threats were in preparing them

for or preventing cybersecurity attacks. Additionally, there was an opportunity to evaluate the organizational challenges and total costs associated with implementing new processes in response to increased threats. Tracking the effectiveness of changes made by small to mid-sized organizations in response to recent threats can help inform decision making for other organizations and industries. Lastly, it would be beneficial to measure the impact or lack thereof for organizations that made investments against the organizations that elected not to do so or otherwise could not afford to.

Summary

All industry leaders are entrusted with ensuring adequate protection of the confidentiality, integrity, and availability of their sensitive organizational data. With the advent of new threats, the healthcare industry is now seeing a time of transformation in which healthcare leaders must navigate the appropriate response. Many are opting to invest in new technology, staff, and even external partnerships to prepare against the threat of ransomware and other cybersecurity risks.

Proactive communication to increase employee awareness and achieve active prevention of these risks, paired with the effective communication of necessary staffing changes may not prevent a cybersecurity risk on its own, though they are necessary components to prevent one from devastating the affected organization. The purpose of this study was to assess healthcare organizations' risk awareness and their associated risk responses. Specifically, it aimed to evaluate the response of small to mid-sized healthcare organizations due to increased cybersecurity threats to the healthcare industry. The study has drawn conclusions, evident across the healthcare industry and organizations of various sizes, showing an overall move toward investing in cybersecurity.

References

Angst, C., Block, E., D'Arcy, J., & Kelley, K. (2020). When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches," *MIS Quarterly*. delivery.php (ssrn.com)

Connolly, L. & Wall, D. (2019). The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomizing countermeasures. *Computers & Security.*

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review,* 4(10): 13-21. http://doi.org/10.22215/timreview/835

Cybersecurity & Infrastructure Security Agency (2019). *Security Tip (ST04-001): What is cybersecurity?* Cybersecurity & Infrastructure Security Agency https://us-cert.cisa.gov/ncas/tips/ST04-001

Cybersecurity & Infrastructure Security Agency (2019). *Alert AA20-302A: Ransomware activity targeting the healthcare and public health sector.* Cybersecurity & Infrastructure Security Agency https://us-cert.cisa.gov/ncas/alerts/aa20-302a

Cybersecurity & Infrastructure Security Agency (2021). *Ransomware fact sheet: What is it and what to do about it.* Cybersecurity & Infrastructure Security Agency https://www.cisa.gov/sites/default/files/2021-01/NCIJTF%20Ransomware_Fact_Sheet.pdf

Department of Health and Human Services (2020). Summary of the HIPAA privacy rule. *Health information privacy page*. https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

Department of Health and Human Services (2020). Summary of the breach notification rule. *Health information privacy page.* https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

Health Care Compliance Association (2020). Healthcare Industry Compliance Staffing and Budget Benchmarking and Guidance Survey. https://www.hcca-info.org/sites/hcca-info.org/files/2020-03/hcca-2020-benchmarking-guidance-survey.pdf

HIMSS (2020). 2020 Health Information Management Systems Society Cybersecurity Survey https://www.himss.org/sites/hde/files/media/file/2020/11/16/2020_himss_cybersecurity_survey_final.pdf

HIPAA Journal (2020). Healthcare data breach statistics. Healthcare Data Breach Statistics (hipaajournal.com)

International Information System Security Certification Consortium (2020). ISC2 Cybersecurity workforce study: *Cybersecurity professionals stand up to a pandemic.* https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.as

Kruse, C., Frederick, B., Jacobson, T., & Monticone, D. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. Technol Health Care. *Technology and health care: Official journal of the European Society for Engineering and Medicine*. https://doi.org/10.3233/THC-161263

O'Brien, G., Edwards, S., Littlefield, K., McNab, N., Wang, S., & Zheng, k. (2019). Securing wireless infusion pumps in healthcare delivery organizations: *NIST special publication 1800-8* https://doi.org/10.6028/NIST.SP.1800-8

Poth, C. N., & Creswell, J. W. (2016). Qualitative inquiry and research design: C*hoosing among*

five approaches. https://doi.org/10.1177/1524839915580941

Racovita, M., (2020). Industry briefing cybersecurity for the internet of things and artificial intelligence in the healthcare sector: *The PETRAS national centre of excellence for IoT systems cybersecurity* DOI: 10.14324/000.rp.10112770