CORE

Metadata, citation and similar papers at core.ac.uk

Provided by Beadle Scholar at Dakota State University

Dakota State University
Beadle Scholar

Masters Theses & Doctoral Dissertations

Spring 3-2019

Flashlight in a Dark Room: A Grounded Theory Study on Information Security Management at Small Healthcare Provider Organizations

Gerald Auger
Dakota State University

Follow this and additional works at: https://scholar.dsu.edu/theses

Part of the Databases and Information Systems Commons, Information Security Commons, Software Engineering Commons, and the Systems Architecture Commons

Recommended Citation

Auger, Gerald, "Flashlight in a Dark Room: A Grounded Theory Study on Information Security Management at Small Healthcare Provider Organizations" (2019). *Masters Theses & Doctoral Dissertations*. 329.
https://scholar.dsu.edu/theses/329

This Dissertation is brought to you for free and open access by Beadle Scholar. It has been accepted for inclusion in Masters Theses & Doctoral Dissertations by an authorized administrator of Beadle Scholar. For more information, please contact repository@dsu.edu.

FLASHLIGHT IN A DARK ROOM: A GROUNDED THEORY STUDY ON INFORMATION SECURITY MANAGEMENT AT SMALL HEALTHCARE PROVIDER ORGANIZATIONS

A dissertation submitted to Dakota State University in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in

Cyber Operations

March 2019

By
Gerald Auger

Dissertation Committee:

Kyle Cronin, Ph.D
Committee Chair

Aaron Heath, J.D.
Committee Member

Stephen Krebsbach, Ph.D
Committee Member

Judy Vondruska, Ph.D
Committee Member

Robert Warren, M.D. Ph.D
Committee Member

Julie Wulf-Plimpton
Committee Member

DSU
DAKOTA STATE

DISSERTATION APPROVAL FORM

This dissertation is approved as a credible and independent investigation by a candidate for the Doctor of Philosophy degree and is acceptable for meeting the dissertation requirements for this degree. Acceptance of this dissertation does not imply that the conclusions reached by the candidate are necessarily the conclusions of the major department or university.

Student Name: Gerald Auger

Dissertation Title: Flashlight in a Dark Room: A Grounded Theory Study on Information Security Management at Small Healthcare Provider Orgs

Dissertation Chair/Co-Chair: Date: 25 March 19

Judy Vandruska 4/18/19

Committee member: Date: ~~4/25/19~~

Committee member: Date: 3/28/19

Committee member: Date: 3/29/19

Committee member: Date: 3/29/19

Committee member: Julie Wulf Plimpton Date: 3/29/19

Original to Office of Graduate Studies and Research
Acid-free copies with written reports to library

ACKNOWLEDGMENT

This experience results in one individual recognized for the accomplishments of hard work and commitment, but without support, encouragement, and guidance from many distinguished people, this journey would have been materially flawed from the start. Nadine, your multi-faceted support as a wife and best friend were paramount in this effort, I love you. The support of Grayson and Callan to understand why Daddy had to do so much school work and miss out on activities. My greater family for your evergreen encouragement. To Bill for your ability to drive me beyond my self-perceived limits.

Sincere gratitude to the Chair and Committee Members for your time, expertise and guidance. This work is far better with your input, and I'm a stronger academic because of your tutelage. Kyle Cronin, special thanks for the last 18 months. You kept me on the rails. Thank you, Pauli family for your hospitality, support and guidance. Josh, you are the reason I started this PhD program. Wayne, you are the reason I finished.

Special thanks to Dakota State University faculty and staff. The high-quality experience and support allowed me to excel and develop professionally. To my cohort, our constant communication and (sometimes shared misery) was mentally and emotionally supportive.

Thank you to all the individuals and groups that have no idea of the impact and value you brought me in this effort. Thank you, The Midnight, FM-84, and Timecop1983 for providing the persistent soundtrack to the most demanding project I've ever undertaken.

ABSTRACT

Healthcare providers have a responsibility to protect patient's privacy and a business motivation to properly secure their assets. These providers encounter barriers to achieving these objectives and limited academic research has been conducted to examine the causes and strategies to overcome them. A subset of this demographic, businesses with less than 10 providers, compose a majority 57% of provider organizations in the United States. This grounded theory study provides exploratory findings, discovering these small healthcare provider organizations (SHPO) have limited knowledge on information technology (IT) and information security that results in assumptions and misappropriations of information security implementation, who is responsible for security, and what the scope of security is to address organizational cyber risk. A theory conveying the interrelationship among concepts, illustrating these barriers, is visually communicated. This research can be leveraged by researchers to further understand the dimensions of the identified barriers and by practitioners to develop strategies to improve organizational information security for this demographic. The study's findings may apply to SHPOs in other states as the criteria of South Carolina based SHPOs did not seem to influence the findings.

Intensive interviewing was conducted on nine SHPOs in the state of South Carolina to elicit their thoughts and perspectives on information security at their business, how decisions are made regarding information security, how threats and risks to their business are perceived, and to understand financial activities associated with providing information security at their organization.

The concepts and categories, and how they interrelate to each other compose the "flashlight in a dark room" theory. This theory claims the current IT and information security

knowledge of staff responsible for information security at these SHPOs produces a narrow scope of what is required for proper information security and informs their perceived cyber risk exposure. These personnel are only “seeing” what the flashlight illuminates in a dark room full of cyber risk. They are committed to secure their organization appropriately and are confident in their current cyber security posture. This causes an organizational cyber risk reality versus perception misalignment, resulting in unknown, accepted risk exposure.

SHPOs support information security and are motivated to be ‘as secure as possible’ with a strong emphasis on protecting their patient’s protected health information. This suggests if ‘the “overhead light in the dark room” could be turned on, and illuminate the scope of cyber risk, these organizations would begin to work toward implementing security controls that align to their actual cyber risk.

DECLARATION

I hereby certify that this dissertation constitutes my own product, that where the language of others is set forth, quotation marks so indicate, and that appropriate credit is given where I have used the language, ideas, expressions or writings of another.

I declare that the dissertation describes original work that has not previously been presented for the award of any other degree of any institution.

Signed,

Gerald Auger

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

Healthcare providers have a responsibility to protect patient's privacy and a business motivation to properly secure their assets (Bianchi, 2009; M. Smith, 2017). Despite motivation and regulation, these organization types struggle with adequate information security (Institute, 2016). Currently, it is not understood what issues and impediments are causing this state of inadequacy and limited academic research has been done in this specific area (Appari & Johnson, 2010).

Small healthcare provider organizations (SHPO), healthcare providers with 10 or fewer practicing physicians, are a subset of healthcare providers. These entities are subject to the same regulations and threats as large healthcare provider organizations, but with less human resources, data assets and resources associated with information and system privacy and security.

The following dissertation research project studies South Carolina-based SHPO information security decision processes from participants involved in these experiences to understand factors that are defining and driving the state of information security at SHPOs. The output of this effort was a theory, grounded in data, explaining the phenomena of why SHPOs struggle with effective information security programs.

Background

Information technology and Internet-access are ubiquitous in the healthcare industry today, especially with the incentives and motivations of governmental programs encouraging IT adoption (Jones, Rudin, Perry, & Shekelle, 2014). Threat-actors including insider threats, nation-states, cyber-criminals and competitors can disclose, destroy, modify or make unavailable ITvital assets causing harm to healthcare businesses (Coats, 2017). Information security controls are the mechanisms organizations can use to mitigate the risk of these threats (NIST, 2004).

Information security controls are designed to meet one or more of the three fundamental security objectives (Ross, 2013). These objectives are confidentiality, integrity and availability. Confidentiality ensures only individuals that are authorized to access a resource are allowed. Availability ensures authorized individuals can access a resource when they want. Integrity ensures the resources composition is not modified or destroyed in an unauthorized manner. These control objectives are required for healthcare provider organizations through physical, administrative and technical controls as defined by the Healthcare Information Portability and Accountability Act (HIPAA).

The United States healthcare industry creates, uses, manages and protects sensitive information. This industry’s data includes protected health information (PHI). The nature of what an individual discusses with a healthcare provider is personal. Furthermore, privacy of that information is expected and federally regulated. The information includes sensitive information such as an individual's medical history, drug use, sexual history, mental health history and diagnoses (Gostin, Lazzarini, Neslund, & Osterholm, 1996). This list is not exhaustive but demonstrates the criticality of properly securing the data from unauthorized disclosure while emphasizing the importance of timely access by authorized individuals.

South Carolina healthcare organizations’ intent to secure systems and protect patient information is not just a best practice for appropriate business responsibility, but all U.S. healthcare organizations are regulated by HIPAA. HIPAA includes explicit sections that document required security and privacy controls. This federal regulation, enforced by the U.S. Department of Health & Human Services (HHS), mandates business entities that handle PHI are subject to and must comply with HIPAA.

Presidential policy directive 21 (PPD-21) establishes the policy for “the United States to strengthen the security and resilience of its critical infrastructure against both physical and cyber threats” (House, 2013). HHS is designated as the sector specific agency for Healthcare sector (DHS, 2017b). HHS is empowered to develop a National Infrastructure Protection Plan (NIPP) healthcare sector-specific plan. Healthcare is identified in as a sector of the U.S’s critical infrastructure (DHS, 2017a). Direct patient care, encompassing SHPO, is defined in the sector-specific plan as a private sub-sector within the healthcare sector. The healthcare sector-specific plan defines goals focused on security and resilience of healthcare systems and services.

South Carolina SHPOs must comply with state regulations in addition to HIPAA federal regulation. South Carolina state regulations, defined in the Certified Industrial Hygiene and Certified Safety Profession Title Protection Act ("SC Code of Laws - Title 39 - Chapter 1 - General Provisions," 2018), require breach notification. Specifically the law states “a person conducting business in this State, and owning or licensing computerized data or other data that includes personal identifying information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of this State whose personal identifying information that was not rendered unusable through encryption, redaction, or other methods was, or is reasonably believed to have been, acquired by an unauthorized person when the illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to the resident”.

HIPAA requires controls that address security and privacy of information assets. The Certified Industrial Hygiene and Certified Safety Profession Title Protection Act (2018*)* requires response actions in the event of a privacy breach. The guidance for protecting critical infrastructure focuses on security and resilience of systems. All are important to consider when making information security decisions for a South Carolina-based SHPO.

Healthcare organizations utilize technology and operational processes to reduce cyber-risk, the risk of an adverse incident resulting in the compromise of one or more security objectives for a controlled resource (i.e. breach of a patient data, unavailability of a medical device), and address HIPAA requirements. Information security technology can include firewalls, intrusion detection systems and endpoint security applications. Operational processes can include recurring user account validity reviews, operating system patching and configuration management.

Small businesses have a high-likelihood of being targeted in a cyber security related attack. According to Ponemon (Institute, 2017), 54% of small businesses have suffered a data breach and 61% have suffered a cyber-attack within twelve months of the report. Furthermore, research conducted in 2016 showed healthcare organizations experience 11.4 cyber-attacks per year on average, about one every month (Institute, 2016). Victims can experience multiple impacts from a compromise including financial loss, reputational damage and operational degradation.

Kane (Kane, 2017) reported through the American Medical Association, in the 2017 annual Policy Research Perspectives, 57.8% of physicians work in practices with 10 or fewer physicians. Given a majority of healthcare providers are 10 physicians or fewer, this value is used as a defining factor to qualify the “small” attribute of a SHPO. SHPO is a large population of healthcare businesses that have a unique intersection of sensitive data, regulations to ensure security and privacy, a desirable target for cyber-criminals and resource constraints to properly secure it.

Problem Statement

Given these challenges and demands small healthcare organizations are subject to, implementing effective information security controls poses a challenge. 67% of healthcare organizations self-identify as not having a very effective cybersecurity posture, based on Ponemon's (Institute, 2016) research of 535 organizations, where 96% of respondents were from organizations less than 500 employees.

These organization types should be securing their data assets, yet the majority are not. There are multiple possibilities that could be the root cause of this state. For example, small healthcare organizations may not understand how to implement effective security controls, there may be a lack of resources to allow the implementation of effective security controls or there may be an intentional decision not to implement effective security controls. The lack of academic research in the underlying motivations of small healthcare providers information security program management decision processing leaves a gap in the literature exploring management's decision and support impact on overall information security control effectiveness.

The problem addressed by this study is why information security at SHPOs is not very effective despite external and internal factors that promote the opposite. Focused factors are associated with the environment and applicable circumstances that shape the culture, decisions and approach of SHPO's information security.

Purpose

The research explored South Carolina, small (less than 10 physician practices) healthcare providers' management perceptions of vulnerability to cyber-attacks and the motivations influencing their security control implementation decisions they take to safeguard their organizations.

The research utilized a Grounded theory research methodology with an interpretivist worldview. Grounded theory is a methodology pioneered by Glaser and Strauss in the late 1960’s that moved qualitative inquiry from a descriptive study into an explanatory theoretical framework, allowing for a deeper understanding of the studied phenomena (Charmaz, 2014; B. G. a. S. Glaser, A.L., 1967).

Grounded theory from a interpretivist worldview enables researchers to inductively develop a theory or pattern of meaning rather that start with a theory, as in a post positivist worldview (Creswell, 2014). A theory explaining the process that management at small healthcare businesses engage to implement, maintain and justify their information security decisions was contributed to the body of knowledge.

Significance

There is limited literature on information security practices in small businesses despite the significant footprint they compose within the U.S. economic landscape , specifically 99.7% of U.S. businesses with paid employees (Advocacy, 2017). SHPOs make up the majority of healthcare provider organizations in the United States, representing 57.8% of all healthcare providers (Kane, 2017). Furthermore anecdotal evidence shows a majority of information security professionals at organizations within the healthcare sector assess the current state of cybersecurity in healthcare as failing or barely passing (HealthcareInfoSecurity.com, 2017).

The exploratory findings from the research can be used by SHPOs to understand how to improve the organization’s information security posture and how the organization compares to other comparable population, geography and demographic healthcare organizations. This research can inform policy makers at multiple levels (i.e. organizational, local, state, federal) on decisions that impact regulation and best practices. It can also be used to inform information security decisions by leadership at SHPOs.

Grounded theory as an exploratory research methodology is appropriate to understand the current state of practice, the attitude and culture of these organizations and explains what is actually happening (McCallin, 2003). An exploratory research approach was appropriate in this context given this lack of understanding of this topic (Creswell, 2013, 2014). The research design leveraged the qualitative method of grounded theory to inductively develop a theoretical understanding of what is happening from an operational perspective within these organizations; generated from raw data gathered during interviews, memos and other essential methods required for grounded theory (A. Bryant & Charmaz, 2007).

Nature of Study

Business processes determining information security decisions are specific to individual organizations and are conducted through social processes (K. G. Smith et al., 1994). Management makes information security decisions for the organization based on the information available to address risk and regulations. Qualitative research provides for understanding of social phenomena, such as this decision process.

A qualitative research design was appropriate for this research area given the limited research in the area of small healthcare provider business information security, the increased potential impact of security control failure in the healthcare industry and the subjective factors that drive decision makers at small healthcare provider organizations.

Grounded theory specifically aligns with this area of research. It supports exploratory research, relies heavily on the experiences and interpretations of the participants in the setting. Unique to grounded theory, it allows the researcher to dynamically drive the direction of the study as areas of interest present themselves through concurrent data generation and analysis. This research freedom complements the inductive approach to data analysis. Additionally, grounded theory supports deductive data analysis, enabling researchers to retrospectively apply findings, such as a theory, inductively developed on previously executed interviews or memos to affirm the findings or provide input into tuning it.

Detail on this study’s research design are captured in the following table, attributes are based on Creswell’s (Creswell, 2014) model for qualitative constructivist proposal format and Saunders, Lewis and Thornhill (Saunders, Lewis, & Thornhill, 2009) “Research Onion” diagram. A brief value determined for each research design attribute is provided. A complete explanation for each attribute is in Chapter 3.

Table 1 - Research design properties

Attribute	Value
Philosophical worldview	Interpretivism / Constructivist
Qualitative design strategy	Grounded theory
Researcher role	Active participant and observer
Approach	Inductive
Choice	Monomethod
Time horizon	Cross-sectional
Data collection	Interview
Data analysis	Concurrent data gathering and analysis; Thematic coding and abstraction; Grounded theory systematic analysis methods
Research support software	Atlas.ti qualitative data analysis
Internal validity	Data triangulation

Research participants were recruited through canvassing techniques. Additionally, the principal investigator (PI) engaged with a South Carolina medical association to leverage the association's communication channels to promote the study and solicit participants.

Bounding the Study

The following describes the environment that the research was conducted, the types of participants that were solicited for data inputs and the aspects of the participants experiences that were under discussion. The sensitivity of the research topic included adherence to federal regulations, protection of patient information, financial losses and negligence. Each is a sensitive topic and may dissuade a participant from being forthcoming with complete, honest responses

(Saunders et al., 2009). Ethical considerations for this type of collected data and the approach to promoting complete responses are also detailed below and in the data collection subsection.

Setting. The study investigated SHPO and the processes management exercises to make information security decisions. Interviews were the primary method for data generation. Saunders (Saunders et al., 2009) provides guidance on conducting interviews to encourage participation, limit interviewer bias, and promote full responses. Interviews occurred via a teleconference medium, in accordance with approved Institutional Review Board (IRB) requirements.

Interviews were overtly audio recorded. Recording could have been omitted from an interview per research participant request in accordance with the research participant consent. No participant exercised this option.

Participants. Target research participants were individuals that work within management or leadership roles in small healthcare provider practices within South Carolina that are accountable for information security at the SHPO. If a SHPO has more than one individual accountable for information security, all accountable individuals were interviewed simultaneously to avoid gaps in responses or conflicting responses from separate interviews.

The constructivist approach to grounded theory places the researcher as a subjective active participant in data generation with the participant (Birks & Mills, 2015). The raw data from the participants ground any developed abstraction or theory, but it is the researcher's interpretation that constructs these abstractions and theories. Focus remained on understanding the meaning participants hold about the problem.

Events. This grounded theory study sought to understand processes engaged and influences into these processes for information security management at SHPO, specifically explicit activities involved in affecting the security posture of an organization.

Events in-scope were strategic level decisions that relate to the identification, protection, detection, response and recovery of business assets, including but not limited to patient health information, business support systems (e.g. payroll) and biomedical devices.

Processes. Processes in-scope are strategic level activities and management activities related to understanding what knowledge and inputs factors on informing management on strategic information security decisions are. Additionally, the operational execution of this strategic vision and the company culture associated with information security was investigated.

Ethical Considerations

Internal or sensitive information may have been disclosed during the research activity that could have caused harm to the research participant personally or to the organization the research participant represents.

Multiple techniques were employed to address these ethical considerations, convey trust and promote full, honest responses. IRB approval was sought prior to collecting any data. All research participants were required to listen and acknowledge an informed consent declaration that clearly communicates their rights and expectations to privacy as a participant in the study. Participants and their organization were de-identified. A mapping tool identifying participants and organizations with their unique study identifier was maintained with strict access controls and data at rest encryption. All data was protected in accordance with approved IRB requirements.

The researcher would have entered into a non-disclosure agreement (NDA) with research participants if the research participant organization required it. This assumes the NDA does not prevent any aspect of the data analysis or findings disclosure described in chapter 3. This was not exercised by any participants.

The researcher utilized a defer technique when a research participant inquired to the interviewer about the interviewer's views on a topic. For example, if a research participant asked, "what should I know about the HIPAA security rule". The researcher would reply "I do not want to influence your responses. I'll be happy to discuss upon the conclusion of this research study", to avoid researcher bias or influence on participant responses.

Definitions

Certain terms are used throughout this document that can have different meanings based on background, experience and perspective. Definitions for key terms are provided in Appendix A. The purpose of defining these key terms is to establish a common language within the scope of this research and its findings.

Assumptions

The researcher was an active participant in this research study. Additionally, the researcher was coding, abstracting and developing the grounded theory. The researcher's assumptions are therefore critical to identify both for the researcher and consumers of the study's findings.

Enumeration of these assumptions limit the researcher bias influence on the findings (Birks & Mills, 2015, p. 20). Researcher's assumptions were:

- Any previous healthcare experience by the researcher did not influence research participants.
- In-scope SHPOs' participants are for-profit entities.
- Healthcare provider organizations are making assumptions that IT staff are also handling information security.

- Healthcare provider organizations with inadequate information security controls would not want to know about it.

Scope, Limitations, Delimitations

The scope of this research is detailed in “bounding the study” section of Chapter 1. Grounded theory was used as an exploratory research method. This research applied to SHPO in the state of South Carolina. This research is assumed to be generalizable to other US geographies, but not to other healthcare entities that are non-providers such as clearinghouse and insurers. This research is assumed to be not transferable to these non-provider types because of the distinction that healthcare providers uniquely work with biomedical devices, have ownership of permanent medical records and provide treatment to individuals.

Grounded theory is a qualitative research method that uses inductive reasoning to develop a theory from observed data. This approach to research does not start with a hypothesis to test through deductive reasoning, but instead creates a theory that then can be used later in deductive reasoning-based research. This is an appropriate research method choice for this study given the limited research that has been conducted in this area.

Orthodox practice of traditional grounded theory requires no literature review prior to engaging in data generation and collection (B. G. a. S. Glaser, A.L., 1967) . The idea behind this approach is to reduce researcher bias into subconsciously fitting the data to fit existing literature instead of having the theory developed exclusively based on collected data. A literature review was conducted given this study was in support of a dissertation research project and a literature review was a required component of this project. Every effort to limit researcher bias was utilized to avoid this issue introduced by the literature review.

Chapter Summary

There are regulatory, ethical and pragmatic business reasons for small healthcare providers organizations to implement information security controls at their business, yet surveys and incidents have demonstrated this market is insufficiently addressing protecting its assets from realized threats, detecting when incidents have occurred and effectively recovering from these incidents without suffering significant impact.

Grounded theory is a research methodology that develops a theory based heavily on data collected from individuals experiencing the phenomena being studied, in this case individuals responsible for information security at small healthcare providers. Grounded theory provides a method to conduct exploratory research, an approach that aligns with the lack of research being performed in this area.

A literature review provides an understanding of what research has been done in this area to date and what factors shape the reality of the setting. The following chapter provides insight into the developments of small business information security and discuss the nuances a healthcare setting overlays on these types of businesses.

CHAPTER 2

LITERATURE REVIEW

Healthcare cybersecurity is a key public health concern that needs immediate and aggressive attention.

- (FORCE, 2017)

Information security within the healthcare industry is a complicated area of interest. There are several factors to consider including securing the systems that enable direct patient care (i.e. Electronic Health Records (EHR)), ancillary patient care (i.e. lab, x-rays), and business management (i.e. scheduling, billing). The data within these systems must also be secured from a security risk (e.g. integrity of a patient's drug allergies) and a privacy risk (e.g. a patient's HIV status). Regulation, threats, risks, vulnerabilities and impact must be considered for these systems and data when approaching information security program management.

Healthcare information systems (HIS), such as the EHR, are comprehensive repositories of patient care history, used not only by healthcare providers but also patients, family members, payers and others engaged in the business of healthcare, researchers, and government agencies. Unfortunately, this utility and data-rich environment attracts criminals (Luna, Rhine, Myhra, Sullivan, & Kruse, 2016).

Healthcare information systems and technology are complex. They are integrated, provide patient care and contain individual's personal health information. The security and resilience of these systems is important to individuals whose information is stored in the systems and to the healthcare professionals that rely on the information as a communication tool to provide care to patients. The healthcare provider is concerned with the security and resilience of these systems to comply with regulations and to provide quality patient care to patients. The confidentiality, availability and integrity of healthcare systems is therefore critical.

Small businesses within this sector have the same challenges and requirements as larger businesses with less access to financial and information security expertise resources.

The following literature review provides a review of regulations affecting the healthcare industry, the cyber threats, risks and controls healthcare providers must evaluate when making information security program decisions and the nuances of a small business.

Healthcare Information Security

Whitman and Mattord (Whitman & Mattord, 2011) define information security as “the protection of confidentiality, integrity and availability of information assets, whether in storage, processing or transmission; achieved via the application of policy, education, training and awareness, and technology”.

Systems and environments have security requirements defined by the organization that address the information security objectives. These requirements are implemented through security controls.

Rohn et al. (Rohn et al., 2016) defines a control as a measure intended to reduce risk to a level acceptable by management. IT internal controls at a governance level involve ensuring that effective IT management and security principles, policies and processes with appropriate compliance measurement tools to assess and measure those controls are in place and operate effectively (Rohn et al., 2016).

Controls have different associated costs and effectiveness for reducing risk, and categorically, controls can be physical, technical or administrative in nature (Herold & Beaver, 2004). Risk management allows for organizations to analyze and decide what controls to implement that reduces risk to acceptable levels (Peltier, 2005). The analysis and selection depend on business need and security requirements according to Barnard and von Solms (Barnard & Von Solms, 2000). The factors that influence security control selection were expanded by Otero, Otero and Qureshi (Otero, Otero, & Qureshi, 2010) to include cost of implementation, scheduling and resource availability. Furthermore, security control selection must consider the integration into operational processes as research has shown legitimate users will circumvent security for usability and benefit gains (Albrechtsen, 2007)

The Joint Task Force Transformation Initiative (Initiative, 2011) defined information security risk as “the risk associated with the operation and use of information systems that support the missions and business functions of their organizations”. Information security risk is based on the likelihood and impact of a threat being realized (NIST, 2012). The NIST Special Publication 800-30 revision 1 categorizes threats as one of the following:

- Hostile cyber or physical attacks,
- Human errors of omission or commission,
- Structural failures of organization-controlled resources (e.g., hardware, software, environmental controls), and
- Natural and man-made disasters, accidents, and failures beyond the control of the organization

There are multiple supported information security related threat taxonomies in the literature, some focused on the healthcare industry (Kotz, 2011; Landry, Pardue, Johnsten, Campbell, & Patidar, 2011; NIST, 2012). Security controls mitigate the event of a risk being realized, that is a threat exploiting a weakness resulting in a negatively impacting event.

Mandiant (Mandiant, 2016) reported the three most significant realized risk trends were business disruption attacks, massive data breaches of personally identifiable information (PII), and an increased in compromised networking devices.

These trends continue to plague the healthcare industry today. Business disruption attacks include ransomware, malicious software that encrypts system files and requires the system owner to pay a fee to a criminal to obtain the decryption key. Ransomware has significantly impacted the healthcare industry and is rampant in its application, accounting for over 70% of all malicious software attacks on healthcare providers from 2015-2017 (Verizon, 2018). The availability to systems and data is important for healthcare providers to provide patient care. This necessity is being exploited by cyber criminals through ransomware. Ransomware attacks on healthcare entities has increased significantly since 2016 with several notable attacks including MedStar and Hollywood Presbyterian (Davis, 2017; Hegwer, 2017; Kruse, Frederick, Jacobson, & Monticone, 2017; Millman, 2016).

Massive data breaches of PHI are regular occurrences in healthcare with over 1292 reported in 2015-2017 (Verizon, 2018). Luna et al. (Luna et al., 2016) supported this PHI/PII data breach threat trend with research showing data theft is the greatest threat to healthcare with the intended purpose being to commit identity theft.

Kruse et al. (Kruse et al., 2017) conducted a systematic literature review across three major medical research databases to understand current trends and threats to organizations within the healthcare industry. The research affirmed the healthcare industry struggles with new technology, especially with U.S. federal policy promoting an increasing use of technology by healthcare provider organizations, and security in response to evolving cyber threats. The research also stated the healthcare industry lags other industries in securing data, however the databases queried were healthcare-specific databases and the thirty-one papers included in the review did not include any papers explicitly evaluating the healthcare sector against other sectors.

Luna et.al (Luna et al., 2016) conducted a literature review on cybercrime themes and trends in healthcare across four research databases, resulting in nineteen papers being selected for inclusion. Two broad cybercrime areas, that were identified, are unauthorized access by internal parties possible because of known vulnerabilities in the system and external parties disclosing data beyond its intended scope of use.

Researchers “Independent Security Evaluators” (Evaluators, 2016) conducted a 24-month security assessment of 12 healthcare facilities and found that remote adversaries have a high likelihood of successfully exploiting healthcare systems showcasing the vulnerability and immaturity of healthcare organizations with respect to cyber security. Systemic causes of these weaknesses were identified as lack of executive support, insufficient talent, improper implementations of technology, outdated understanding of adversaries, lack of leadership, and a misguided reliance upon compliance (Evaluators, 2016).

“Independent Security Evaluators” (Evaluators, 2016) research highlighted the state of information security by finding even fundamentals are not being properly implemented including the development and adherence to policy and procedures, the lack of audit capability to assess the presence or effectiveness of security controls and the practice of deploying technologies insecurely and misaligned to enterprise architecture (Evaluators, 2016).

An independent research organization, The Ponemon Institute (Institute, 2016), conducted a survey in 2015 to gauge the state of cybersecurity in healthcare. The survey of 535 IT and IT security healthcare professionals. High level findings found that healthcare organizations experience on average almost one cyber-attack per month.

Eighty-eight percent of respondents worked for an organization with 100-500 employees. This organization size is more aligned to a medium-sized business per various definitions of business sizes. Therefore, this research while not excluding large and small-sized healthcare organizations, is heavily skewed toward medium-sized entities (Institute, 2016). Of note, the most common security incident noted in the Ponemon study (2016) was exploitation of existing software vulnerabilities. This infers organizations were not patching their systems and software (Institute, 2016). Finally, sixty-seven percent of respondents stated their cybersecurity posture was not effective because of a lack of coordination with other business functions (76%), lack of resources (73%) and cybersecurity not being a priority (65%) (Institute, 2016).

Fernando and Dawson's (Fernando & Dawson, 2009) research found conflict between healthcare providers and privacy and security controls. The research, based on a structured interview with twenty-six clinician respondents on healthcare information system privacy and security experiences, found efforts by clinicians to avoid conflict and emphasize patient care above privacy and security tended to result as security breaches. Also, privacy and security specific fiscal and regulatory factors conflicted with improved patient care outcomes.

Verizon's PHI Data Breach Report (Verizon, 2018) found of 1360 incidents, where data was either confirmed as disclosed or was at risk, 57.5% were caused by internal actors, as opposed to the commonly seen external actors. The report highlighted financial incentives and curiosity as the primary factors motivating insiders to abuse their access (Verizon, 2018). This is pertinent in the healthcare industry as several different medical related frauds may be perpetrated with a patient's medical record, and the curiosity to look at a family member or celebrity's medical record. Schoew's (Schoew, 2018) anecdotal research showed 18% of healthcare professionals would sell their healthcare credentials for $500-$1000.

Hoffman (Hoffman, 2015) claims the healthcare industry has been significantly impacted by poor information security controls identifying 90% of healthcare providers experienced a data breach within the period of 2012-2014. Healthcare is expected to continue to be a targeted industry given the value of healthcare data in illegal marketplaces and the continued increase year over year of cyber-attacks on healthcare entities (Hegwer, 2017; Kruse et al., 2017).

Poor information security controls and desirable data assets make healthcare an attractive target to cyber criminals. Symantec's survey (Symantec, 2017) reflected this increasing threat. In 2017, Healthcare saw an increase in malicious email containing malware from 1 in 396 emails to 1 in 204. This Symantec's survey (2017) data showed a 4.2% decline in PHI lost in breaches in 2016, although these statistics appear to be skewed by a major PII and financial breach related to the Friend Finder Network that experienced a breach of 412 million user accounts in 2016. The same report (Symantec, 2017) showed health services was the second highest percentage, 11.2%, of sectors experiencing breach incidents.

The anticipated sustainment in healthcare targeted attacks are supported by the proliferation of patient health data. Patient health data can be used by healthcare providers in multiple ways and duplicating electronic data is trivial. Additionally, medical systems are expensive to procure leading healthcare providers motivated to realize the maximum amount of value from the system regardless if underlying technologies go unsupported by vendors due to technology end-of-life (Hoffman, 2015).

The American Hospital Association (Association, 2016) highlighted the significance of proper cybersecurity in healthcare and the need for senior leadership to be thinking about it. They produced literature for their constituency that promotes the activity of healthcare organizations considering information security fundamentals such as cybersecurity planning, accountability and cyber insurance.

The Health Information and Management Systems Society (HIMSS), a global, cause-based, not-for-profit organization focused on better health through information technology, conducts an annual information security executive survey to gauge healthcare organizations current concerns, issues, and direction. The 2015 survey was completed by 297 professionals with information security responsibility at a healthcare organization (HIMSS, 2015). Eighty-seven percent of represented organizations identified information security as a higher business priority. This is supported with the metric that over half of these organizations have a Chief Information Security Officer (CISO) or other full-time employee with managing information security as a full-time responsibility (HIMSS, 2015). Meanwhile, the HIMSS survey results reinforced a common issue currently plaguing healthcare organizations. A lack of staffing and financial resources were key barriers to properly addressing information security. This translates to a lack of knowledge to implement or execute proper information security, and a lack of financial support via a lack of support from senior management, either from a miscommunicated narrative of actual organizational information security risk or a "tone-deaf ear” by management to accepted organizational risk (HIMSS, 2015).

Finally, research designed to understand the criticality of specific threats to healthcare information security, determined power loss was the most critical (Samy, Ahmad, & Ismail, 2009). Structured interviews were conducted on sixteen staff members across three different departments and with a variety of roles at a single healthcare provider in Malaysia.

Unfortunately, the generalizability of the research is suspect based on the fact all participants worked for the same healthcare provider. For example, it is possible that healthcare provider had experienced multiple power losses resulting in a skewed perspective of this threat to interviewees.

Governmental Factors

There are regulations healthcare providers must consider when making information security decisions and providing healthcare related service. Government incentives have resulted in the acceleration of healthcare providers adopting technologies and solutions that support their business function of providing healthcare, and additionally increases the risk healthcare providers are assuming by digitally storing sensitive data through increased access opportunity, an inability to detect unauthorized access and the ease with which many patient records can be compromised.

United States based healthcare providers are legally required to provide minimum security and privacy controls in their business practices. The Health Insurance Portability and Accountability Act (HIPAA) enacted into law in 1996 and updated in 2000 and 2003 to include the Privacy Rule and Security Rule, respectively, makes it mandatory for providers to implement policies and procedures focused on protecting patient health information ("HIPAA History," 2017).

Relative to information security requirements, HIPAA contains the security rule, the privacy rule and a breach notification rule. The security rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity through appropriate administrative, physical and technical safeguards ensuring confidentiality, integrity and availability of the electronic PHI (HHS.gov, 2017b). The privacy rule establishes a set of national standards for the protection of certain health information including an individual's past, present or future physical or mental health, the past, present, or future payment associated with provision of healthcare, or the actual provision of healthcare through controls around the access, disclosure and retention of that data (Assistance, 2003). The breach notification rule requires HIPAA covered entities and their business associates to provide notification to affected individuals following a breach of unsecured PHI (HHS.gov, 2013). These requirements introduce additional cost, man-power, expertise and time to properly implement, operate and continuously monitor. The Enforcement Rule was added to HIPAA in 2006 and authorized the Office of Civil Rights (OCR) to issue financial penalties for entity that fails to implement HIPAA privacy and security rule ("HIPAA History," 2017).

HIPAA requires security and privacy but does not offer any direction on how to systematically implement an information security program strategically or tactically. This has caused many healthcare organizations to make a “best effort” at securing systems and properly ensuring patient data privacy. “Best effort” is a product of resources, time and expertise a healthcare organization can commit to such an endeavor.

HIPAA federally requires healthcare providers to secure their data and systems. HIPAA was criticized for the lack of federal regulation compliance enforcement (Collins, 2007). Following criticism, the first penalty for HIPAA non-compliance occurred in 2008, 12 years after the law was put into effect.

The Health Information Technology for Economic and Clinical Health Act (HITECH) was passed in 2009 as part of the American Recovery and Reinvestment Act (ARRA) of 2009. HITECH had many impacts on the healthcare industry from a regulation perspective. It incentivized healthcare providers to improve IT infrastructure and encouraged the “meaningful use” of EHR systems. HITECH introduced the Enforcement Interim Rule that outlined a tiered structure to HIPAA violation financial penalties and increased the overall financial penalties themselves.

In 2010, in support of the HITECH EHR “meaningful use” regulation, the Center for Medicare and Medicaid Services (CMS) implemented a program providing financial incentive payouts to healthcare providers that meet criteria for efficient and patient-centered use of EHR solutions. Meaningful use was positioned to support timeliness of service and accessibility of patient records to authorized individuals ("HIPAA History," 2017). Demonstrating Stage 1, the initial stage, of meaningful use is based on fifteen core objectives plus five additional “menu” objectives. One of the fifteen is to "Protect electronic health information" and is measured by performing a security risk analysis annually and remediating or mitigating weaknesses discovered during risk analysis (HealthIT.gov, 2012).

The "meaningful use" initiative in HITECH Act has promoted and caused an increase in the use of electronic medical records, information technology within the healthcare setting and network reliance (Kruse et al., 2017). This incentive was so appealing that adoption rates of EHRs went from 12.2% in 2009 to 83.8% in 2015 (HealthIt.gov, 2018). This increase in technology expanded the attack surface that healthcare entities must protect and defend while increasing the volume of electronic medical data in existence. Maintaining meaningful use for quality improvement requires ongoing support for leadership and change management (Green et al., 2015).

The HIPAA Omnibus Final Rule was issued in 2013 and expanded the scope of HIPAA. It incorporates improved data security, ePHI access, the requirement of Business Associate Agreements (BAA), and breach notification requirements for both covered entities and business associates.

The 21st Century Cures Act was passed into law in late 2016. This law's purpose is "to accelerate the discovery, development, and delivery of 21st century cures, and
for other purposes". This law allows qualified, independent third-parties to be certification authorities for healthcare related software and systems. Specifically, the Act states third-parties certifiers are prioritized based on expertise in multiple areas, including security. It is worth noting this does not require a third-party vendor to have expertise in security though, as a situation may occur where a third-party certifier lacking expertise is the only one to compete and thus be the best option.

The Act bolsters information sharing while explicitly calling out the need to ensure security, calling for the assembly of a working group within one year of the Act passing to report on the allowance of use and disclosure of PHI for research purposes. The working group must have consideration for privacy rights implication and models for secure access of the data assets.

Organizations that suffer a breach of an individual's PHI are required to notify the individual within 60 days (HHS.gov, 2013). HHS OCR, the HIPAA enforcement office, utilizes general deterrence theory to promote information security practices with covered entities and business associates, such as healthcare providers. If a data breach impacts more than 500 unique individuals, the organization is publicly shamed on the HHS OCR breach portal website (HHS.gov, 2018a). HHS OCR enforcement has become highly visible, investigating large privacy and security breach cases and levying noteworthy financial penalties, including Advocate Healthcare for $5.5M and New York Presbyterian for $4.8M. It is interesting to note these material financial penalties may curb behavior, but in 2016 and 2015 only 0.0537% and 0.0339%, respectively, of HHS OCR PHI breach cases resulted in any financial impact to the investigated organization (HHS.gov, 2018b).

Presidential Policy Directive 21: Critical Infrastructure Security and Resilience Healthcare and Public Health directed the federal government to secure and make resilient organizations that are deemed critical infrastructure (House, 2013). This was set in policy through Executive Order 13636, Improving Critical Infrastructure Cybersecurity. This knowingly applies to both public and private sector organizations that align to critical infrastructure, such as financial institutions, power companies and healthcare providers. HHS is the sector-specific agency for the healthcare sector. Under this order, information security sharing communication channels have been established in the form of the National Health Information Sharing and Analysis Center (NH-ISAC). Additionally, the National Institute of

Standards and Technology (NIST) were empowered to develop a cybersecurity framework that could be implemented by critical infrastructure organizations voluntarily (Paul Proctor, 2016).

Healthcare providers leverage technology to provide patient care in many situations. The Food and Drug Administration (FDA) is the federal agency charged with governing biomedical devices functionality and security (Administration, 2018). Biomedical devices must receive FDA certification before they authorized to be utilized in clinical environments. The FDA (Administration, 2016) has released guidance around the secure operation and management of biomedical devices in “Postmarket Management of Cybersecurity in Medical Devices”. This document provides a reference to healthcare providers in the effective execution of medical device risk management, and the reporting and remediating of security vulnerabilities. The FDA is responsible for the security of biomedical devices, but the direction from the agency is presented in the form of guidance and does not have gravity to enforce compliance. This is most notably seen in the Postmarket Management of Cybersecurity in Medical Devices” where the first words of the document are “Contains Nonbinding Recommendations”.

There is also relevant South Carolina state law that applied to this research. South Carolina passed the Financial Identity Fraud and Identity Theft Protection Act in 2013. This law requires South Carolina organizations that suffer a data breach involving 1000 or more individuals’ personal information to notify the affected individuals and pay up to a $1000 per individual fine ("SC Code of Laws - Title 39 - Chapter 1 - General Provisions," 2018).

Healthcare Technology

Shekelle, Morton, and Keeler’s (Shekelle, Morton, & Keeler, 2006) systematic review of literature on technology in healthcare identified it has many applications and potential to reduce healthcare costs, improve the safety and efficiency of patient care and outcome. Goldzweig, Towfigh, Maglione, and Shekelle’s (Goldzweig, Towfigh, Maglione, & Shekelle, 2009) updated review of the literature showed these benefits continue to be seen with the addition of a positive financial impact for the healthcare provider business.

Healthcare technology is a diverse field. Dixon, Zafar, and McGowan (Dixon, Zafar, & McGowan, 2007) developed a taxonomy for healthcare information technology to support a searchable knowledge base that defines the interrelationships among health IT planning, implementation and evaluation. This taxonomy presents the potential scope a healthcare provider may possess for an information technology footprint to secure. The taxonomy, presented in table below, is based on inputs from a panel of medical information experts from across the United States (Dixon et al., 2007).

Table 2 - Healthcare information technology taxonomy (Dixon et al., 2007)

Major Category	Minor Category
I. Organizational Strategy	A. Financial
	B. Planning
	C. Process Change
	D. Implementation of Health IT
	E. Policy
II. Technology	A. Mobile
	B. Infrastructure
	C Security
	D. Standards
	E. Electronic Health
	F. Telehealth
	G. Health Information Exchange (HIE)
III. Value	A. Research

Major Category	Minor Category
	B. Evaluation Outcomes
IV. Laws and Regulations	A. Sample Legal Documents
	B. Privacy
	C. Security
	D. Government
V. Organizations	A . Professional Societies
	B. Payers
	C. Governmental
	D. Nonprofit Organizations
	E. Magazines
VI. Operations	A. Governance
	B. Project Management
	C. Systems
	D. Dissemination

In addition to traditional IT systems, disruptive technology, such as Internet-of-Things (IoT) and cloud-based systems are resulting in tectonic shifts in the way technology is integrated into businesses that introduces privacy and security concerns (O'Brien, Budish, Faris, Gasser, & Lin, 2016). Tarouco et al. (Tarouco et al., 2012) showed IoT devices are increasing in healthcare related usage, and may increase security risk. Furthermore, cloud systems are being utilized by healthcare businesses to offset cost and management of technology, but at the risk of storing sensitive data in other businesses' systems (Sultan, 2014).

The HITECH Act spurned a rapid computerization of healthcare providers, manifesting in a significantly high rate of implemented EHR systems (HealthIt.gov, 2018). Halamka and

Tripathi (Halamka & Tripathi, 2017) provide evidence that a primary end user, the clinicians, were negatively impacted by this rapid adoption. EHR vendors, while benefiting greatly from the legislative force to procure their products, were also impacted. Deficiencies for users and vendors have been identified in five key areas: usability, workflow, innovation, interoperability and patient engagement (Halamka & Tripathi, 2017).

Kruse et al. (Kruse et al., 2017) systematic literature review affirmed the healthcare industry struggles with new technology, especially with U.S. federal policy promoting an increasing use of technology by healthcare provider organizations, and security in response to evolving cyber threats.

In addition to a user base that demonstrates challenge integrating technology and an active role in circumventing security controls the technology may introduce, Green et al. (Green et al., 2015) showed the maintenance of the EHR after implementation requires continual expert technical support to address upgrades and security needs.

Management Impact

NIST Special Publication 800-37 revision 1, when addressing the importance of leadership to an organization's information security posture, states "Given the significant and growing danger of these threats, it is imperative that leaders at all levels of an organization understand their responsibilities for achieving adequate information security and for managing information system-related security risks" (NIST, 2010).

Peltier (Peltier, 2005) claimed support of risk management by senior management is a demonstration of its due diligence. He expanded on this claim by stating the role of senior management is to ensure necessary resources are effectively applied to develop the capabilities to meet mission requirements (Peltier, 2005).

Hoffman (Hoffman, 2015) highlighted the pivotal role senior management plays in enterprise adoption of information security controls, specifically taking a more active role in supporting and understanding information security elements of the business.

Barton, Tejay, Lane and Terrell (Barton, Tejay, Lane, & Terrell, 2016) showed the importance of the role senior management performs in assuring that information security is supported. This research found senior management's ability to shape beliefs and culture of staff, and to allocate resources and set priorities had direct impact on achieving effective information security in an organization (Barton et al., 2016). Barton et al. (Barton et al., 2016) also found that senior management belief in information security leads to greater participation in IT security governance by senior management. Francis, Xiaohong, Jinsheng, and Hong (Francis, Xiaohong, Jinsheng, & Hong, 2013) similarly showed “tone at the top” through visible and actionable support from senior management of an effective training and awareness program promotes adoption of new information security-enabled procedures and overall information security program success.

Eilon (Eilon, 1969) defined the decision process as the activity of analyzing information material, defining performance measures to determine how a course of action will be judged, enumerating and predicting possible outcomes, and selecting a course of action based on choice criteria. Healthcare provider’s leadership must make decisions when addressing information security risks and regulations.

Bhattacharya (Bhattacharya, 2011) found transactional leadership styles led to greater information security concern by staff at small businesses. A transactional leadership style rewards for compliant behavior and punishes for non-compliant behavior (Bass, 2008).

Small Business Challenges

57.8% of healthcare providers in the United States are small businesses and have 10 physicians or less (Kane, 2017). Healthcare-based businesses are managing the industry specific information security challenges discussed above.

Current research shows that small businesses are vulnerable to cybercrime and experiencing an increase in cyberattacks, compounding the challenge's magnitude (Institute, 2017). Small businesses are being increasingly targeted by cyber criminals because of their limited implemented security controls and the increased proficiency of criminals to automate web-based attacks (Chickowski, 2010).

Rohn et al. (Rohn et al., 2016) investigated information technology security practices of small businesses, through document review and semi-structured interviews, and found low levels of small businesses management awareness of information security threats increased the organizations vulnerability to information security breaches because of an unsupported optimism of the small businesses information security posture. Increasing awareness addresses the issue of misjudging current security posture but does not assure action to reduce risk. Johnson and Koch (Johnson & Koch, 2006) found even when small business owners are concerned and aware of cyber threats they are not willing to take action to defend or pay for protection.

Large healthcare organizations, much like any large business, can have specialized resources available that can be dedicated and focused toward an effort such as implementing an information security program. Small and medium-sized healthcare organizations, much like small and medium-sized businesses, are resource-constrained and do not have the opportunity to dedicate resources to programmatic information security to protect their data and assets (Bagwell, 2016). Unfortunately, medical practices with limited financial, technical, and organizational resources not associated with larger systems typically lack access to the necessary technical expertise, financial resources, and leverage with vendors to meet the needs of maintaining an EHR alone (Green et al., 2015).

Cybercriminals are targeting small businesses. Business email compromise (BEC) attacks, an attack where a criminal sends email impersonating a business senior leader to request a subordinate to take an action (i.e. transfer money), occurred on average 400 times every day, with small- and medium-sized businesses the most targeted (Symantec, 2017).

Van Ommen's (Van Ommen, 2014) quantitative research aimed to determine a causal link between a small businesses IT security implementation maturity and its security incident occurrence. He was unable to determine if there is a relationship between a small business's IT security maturity level and the number of incidents experienced by the business. This research was based on survey questionnaire responses and had a population of sixteen responses calling into question the validity of the results. Supporting the suspect validity of this research, Van Ommen (2014) states "the method of gathering data about the occurrence of IT security related incidents used in this study turned out not to be the best way available, but this study lacked the resources and time to perform a more thorough case study".

Conclusion

Much of healthcare organizations are small businesses. These organizations are at high risk of information security and privacy incidents. These organizations hold valuable data assets and are being targeted by cyber criminals for them, but often have limited financial, knowledge and technical resources to protect these assets sufficiently. Compounding the problem, federal incentive programs have resulted in a massive adoption of technology that was not always based on need or interest by the procuring organization, resulting in inadequate security controls; when small business users provide patient care with "misfit" technology, the ongoing maintenance of that technology may be low priority.

Moreover, there are many healthcare related, information security threats that must be considered when making risk related decisions. Disruptive technologies like Cloud and Internet of Things are expanding attack surfaces and distributing an organization's PHI storage locations. Internal and external threat actors, environmental, and natural threats may negatively impact a healthcare organization's ability to operate if not properly mitigated, avoided or transference.

Leaders of small healthcare businesses significantly impact the direction and actions taken by the organization. The information security attitude and culture promoted by these stakeholders shapes the approach the organization has toward secure practices. These leaders must account for federal HIPAA regulations, South Carolina law, and the availability needs of its systems and data for business operation needs. Unfortunately, they may have a false perception of information security threats and their organization's capability and capacity to address them. Low levels of small businesses management awareness of information security threats increase the organization's vulnerability to information security breaches because of an unsupported optimism of the small businesses information security posture (Rohn et al., 2016).

CHAPTER 3

RESEARCH METHODOLOGY

There are multiple methodologies to conduct research (Creswell, 2014). According to Bryant (M. T. Bryant, 2003), the research method a researcher chooses should be influenced by the nature of the questions being asked. This qualitative research studied the decision processes of small healthcare businesses information security program management to understand factors, motivations, influences and thought affecting these programs effectiveness.

This chapter provides greater detail into the research design structure and the appropriateness of the design. Grounded theory systematic design for application to this research is documented, providing an explanation of the tools that were used to develop a theory grounded in data. The data collection and analysis processes, including the interactions and expectations from participants is documented. A detailed explanation of how trustworthiness of the research is provided including provisions that are incorporated into the design to promote credibility, transferability, dependability and confirmability.

Research Methods and Design Appropriateness

Qualitative research has seen a significant adoption by the academic community over the last 30 years and is considered an accepted method of conducting research, especially exploratory research (Huberman & Miles, 2002). This research utilizes a grounded theory research methodology with an interpretivist worldview. Grounded theory is a methodology pioneered by Glaser and Strauss in the late 1960’s that moved qualitative inquiry from a descriptive study into an explanatory theoretical framework, allowing for a deeper understanding of the studied phenomena (Charmaz, 2006).

A qualitative research design is appropriate for this research area given the limited research in the area of small healthcare provider business information security, the inadequate security control implementation in the healthcare industry (Holtzman, 2017) and the subjective factors that drive decision makers at small healthcare provider organizations. An inductively developed theory explaining the process that management at small healthcare businesses engage to implement, maintain and justify their information security decisions was contributed to the body of knowledge.

Grounded theory specifically aligns with this area of research. It supports exploratory research, relying heavily on the experiences and interpretations of the participants in the setting. The researcher investigates areas of interest as they present themselves through concurrent data generation and analysis. This research freedom complements the inductive approach to data analysis and fits the need of a research area that is lacking significant academic research, such as this study (Birks & Mills, 2015).

Additionally, grounded theory supports deductive data analysis. Researchers can apply developing theories retrospectively to previously executed interviews or memos to affirm the findings or provide negative case analysis to refine the theory. The researcher believes understanding how these organizations are processing and implementing their decisions is understood through the analysis of their experiences, and that their reality of the phenomena is critical for informing any theory that provides an explanation to that process.

Grounded theory provides a systematic procedure for inquiry (Creswell, 2014). There are essential grounded theory methods, documented in the data collection and data analysis sections below, that are considered required to be used for a study to qualify as grounded theory (Birks & Mills, 2015). This bolsters the likelihood of quality, consistency and accuracy in adherence to the grounded theory research methodology. This does not guarantee grounded theory though as many studies claiming to be grounded theory are actually not for various reasons including non-inclusion of the above-mentioned required methods.

A primary method of data collection was intensive interviewing. Grounded theory is based on user experiences that can be gathered through interviews. The interviews were unstructured initially. A set of open-ended questions will be used to allow for free-flowing responses from participants. These questions can be found in Appendix B. The interviews transitioned to semi-structured as themes began to develop. Both methods are appropriate for exploratory studies that involve questions with complex answers that may vary from respondent to respondent (Saunders et al., 2009).

Interviews were transcribed to support qualitative data analysis processes and to strengthen descriptive validity. Participant responses were analyzed for codes, themes and categories in accordance with grounded theory processes.

Additionally, memos were generated throughout the research process. Memos are essential to generating a grounded theory and are treated as data as well. According to Lempert (Lempert, 2007) memos document the analytical interpretation of collected and analyzed data allowing researchers to organize analysis and findings while keeping it grounded in the data.

Population, Site and Sampling

Target organizations for this research are healthcare provider organizations within the state of South Carolina that have 10 or less physicians on staff. Target research participants are individuals that work within management or leadership roles in small healthcare provider practices within South Carolina that are accountable for information security at the SHPO. If a SHPO has more than one individual accountable for information security, all accountable individuals were interviewed in a focus group to avoid gaps in responses or conflicting responses from separate interviews. There are no age, gender, or ethnicity criteria for research participants.

The population sampling strategy utilized snowball sampling, a strategy of using referrals from research participants (Berg, 2004). All research participants met the criteria stated above, and the researcher asked current research participants to recommend potential candidates for the study. As the grounded theory methodology was executed the sampling strategy incorporated theoretical sampling, a classic sampling strategy of grounded theory. Glaser and Strauss (B. G. a. S. Glaser, A.L., 1967) define theoretical sampling as “the process of data collection for generating theory whereby the analyst jointly collects, codes and analyses his data and decides what data to collect next and where to find them, in order to develop his theory as it emerges”.

Grounded theory places the researcher as a subjective active participant in data generation with the participant (Birks & Mills, 2015). The raw data from the participants ground any developed abstraction or theory, but it is the researcher’s interpretation that constructs these abstractions and theories. Focus remained on understanding the meaning participants hold about the problem. It was possible through theoretical sensitivity that the scope of participants increased to include staff at participant organizations.

The study investigated SHPO and the processes management exercises to make information security decisions. Interviews were the primary method for data generation. Interviews occurred over an overtly recorded teleconference medium to facilitate convenience, support honest responses and reduce participant error. The rigidity of the research setting reduced research variability and promoted research participant comfort and privacy.

Charmaz (Charmaz, 2006) pointed out the orthodox accepted answer of how many participants are needed to reach saturation is not a number, but based on when gathering new data does not spark new theoretical insights. Therefore, this can be a small sample size, although the smaller the size and the larger the claim from the data, the greater scrutiny of credibility.

Creswell provides guidance to grounded theory researchers, based on Creswell's (2014) review of qualitative studies, finding grounded theory typically needs 20-30 participants for saturation.

Data Collection and Procedures

IRB approval was obtained prior to collecting any data. This research involved human subjects as participants.

All participants were provided a verbal informed consent detailing the purpose of this research, the type of research, why they were selected as a research participant, that participation was voluntary, the participant expectations, the duration of the participants engagement, the risks and benefits of participating, their right to withdraw from the research at any time, and how data was secured. Data security covers all attributes of the research, including the participants information, responses and data generated, and informs on how this data will remain confidential with purpose to protect the confidentiality, integrity and privacy of the data.

Research participants were required to listen and acknowledge a verbal informed consent prior to interviewing. The research was conducted in accordance with the consent terms.

The primary method of participant generated data collection was intensive interviewing. These interviews did not last more than one hour per session and occurred between September 2018 and February 2019. An essential method of grounded theory is the ability for concurrent data generation and analysis (Birks & Mills, 2015). Results from this study were presented in March 2019, and data was generated and added to refine the developed theory very late in the research process.

The researcher's intent was to use one-on-one interview format. If an organization had more than one individual accountable for information security, all accountable individuals were interviewed in a focus group. The research unit of analysis is the business thus the intent was to avoid partial or conflicting responses from being collected. Focus group interviews have pros and cons compared to individual interviews. Research has shown focus group interviews can provide a better understanding of complex processes because participants question and answer each other revealing more (Morgan, 1996). Additionally, Morgan (1996) points out the researcher can ask for experience comparisons allowing for richer understanding of the process.

There was a risk of not receiving full responses from a participant during a focus group interview. Participants may have been reluctant to share stories of not having followed policy, circumventing process or other incriminating behavior that could result in sanction. Smithson (Smithson, 2000) points out there is a risk of a dominant voice in focus groups which can prevent alternative perspectives and experiences from being disclosed. The selection of interview or focus group for each participant engagement depended on setting and research needs.

Grounded theory promotes unstructured and semi-structured interview question formats. Purposefully the researcher was attempting to generate data and interpret the interviewees experiences with minimal bias and avoid ‘forcing the data’ by using open-ended, unstructured questions to promote interviewee rich responses. Interpretive validity provisions were employed to promote trustworthiness and address bias. Interview sessions were overtly recorded.

Participants and participant organizations were afforded confidentiality for this study. A secured cross-reference document was developed to support the researcher's ability to organize collected data and to allow for follow-up with participants as-needed. The cross-reference document was protected in accordance with this research study’s data security standards.

It is important to point out, it was not possible in advance to tell where this grounded theory research would be directed, and the questions provided in advance may not have been sufficient to collect detail or focus on a salient, core point presented during an interview. The intention is this line of inquiry was followed. Any deviation from IRB approved protocols would seek out additional IRB approval before proceeding.

Data generated from participant responses was transcribed into Atlas.ti, a qualitative data analysis (QDA) software tool. Atlas.ti is a locally installed software package that assists researchers in coding and organizing data. Theoretical coding, category generation, comparison and abstraction were conducted within Atlas.ti. Research data security standards documented within this document apply to the data generated within Atlas.ti.

Memos are another essential method employed in grounded theory. Memos are write-ups of ideas generated during the grounded theory process (B. G. Glaser, 1998). Following Schatzman and Strauss (Schatzman & Strauss, 1973) approach to memo writing, multiple memo types were utilized (see table below).

Table 3 - Memoing standards (Schatzman & Strauss, 1973)

Memo Type	**Function**
Observational	Describe the actual events
Theoretical	Describe the researcher's thoughts about those events
Analytical	Thoughts from the data, or epiphany, reasons for codes, categories, theoretical sampling
Methodological*	Reminders about some procedural aspect of the research
Dissertation*	Ideas that relate to the dissertation, but are not grounded theory related (i.e. what defines a small business, literature review related)

* not part of Schatzman and Strauss approach, but extended by the PI for memo types

Glaser (B. G. Glaser, 1978) famously stated “all is data” in grounded theory. Memos are data; confirmed by Lempert (Lempert, 2007) as memos can be developed about earlier memos as abstraction is raised. Memos were developed throughout the research. They provided a chronological history of theory abstraction for retrospective investigation and support confirmability. Additionally, the researcher was able to utilize retrospectively the thought process and decision making from earlier parts of the research to understand how the current state of understanding was at that time versus the present when more information would presumably be available. As a theory began to develop, the researcher utilized memos to review initial participant interviews and engagements to affirm the theory's rigor or to modify the theory with the new insights obtained.

Memos were documented and managed within Atlas.ti. Research data security standards documented within this document apply to the data generated within Atlas.ti.

The role of the researcher is a factor in grounded theory research. Interview sessions position the researcher as a participant in the study. The researcher performs two roles: participant and observer. Participation manifested in engaging in conversation through a question and answer interview format. Observation manifested in noting situational aspects and settings.

Data Analysis

Analysis of data will be conducted throughout the project, starting early and occurring often. This concurrent collection and analysis are an essential method of grounded theory. Grounded theory's purpose is to develop a theory that is grounded in the data collected from those experiencing the process.

The grounded theory analysis process is systematic in nature. Birks and Mills (Birks & Mills, 2015) provide an informative diagram capturing this process (see Figure 1). This three-phased process begins on the bottom of the diagram with purposive sampling and works upward through the process until theoretical integration occurs producing a grounded theory.

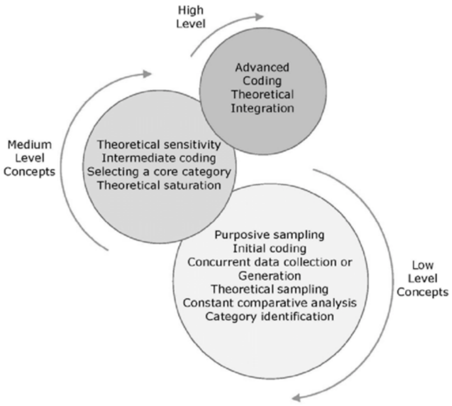

Figure 1 - Essential grounded theory methods (Birks & Mills 2015)

Phase one. Essential methods in the first phase are purposive sampling, initial coding, concurrent data collection and generation, theoretical sampling, constant comparative analysis and category identification.

Purposive sampling. Purposive sampling provides an initial set of participant criteria coupled with interview question direction. These initial interviews were wide in scope but targeted at small healthcare business information security management decision related processes. Recruitment materials designed to target small healthcare providers in South Carolina were disseminated via LinkedIn and Twitter social media platforms. Snowballing sampling was also be utilized following initial interview sessions, as noted above.

Initial coding. Initial coding of data was performed as data was collected. Concepts, themes, keywords, and language from transcriptions were identified and labeled. Coding provided a method to begin to identify patterns and areas of emphasis in the data.
Research participants responses were transcribed into Atalsti. Initial coding occurred on these generated data.

Concurrent data generation and collection. Concurrent data generation and collection, a key difference between grounded theory and other research methodologies, occurred throughout all phases. Data generation and data collection are methods to produce data for analysis, but contrast in that data generation involves the researcher directly engaging the data source to produce materials for analysis while data collection has little to no researcher influence on the data source (Birks & Mills, 2015).

Theoretical sampling. Theoretical sampling provides the mechanism to focus interviews and data collection to provide materials for comparative analysis to identify nuances of the process, continuing to ground any emerging theoretical value. Purposive and snowball sampling relate to the composition of the research participants in the study, however theoretical sampling is concerned with exploring and exhausting the composition of the emerging patterns and themes. Concepts and categories began to emerge as important or recurring. This began to direct an emerging theory and directed where to spend more time focusing during interviews.

Constant Comparative Analysis. Rigorous comparative analysis, another essential method of grounded theory, ensures the developed theory is valid and the path the researcher takes to discover it is directed by the data. Furthermore, this comparative analysis reveals gaps in the data, aspects of the process being studied that remain unexplained or unexplored (Charmaz, 2006). Participant to participant comparison were utilized as part of this method. Additionally, codes and categories applied to participants were compared to other participants to help identify emerging categories.

Category identification. Categories are conceptual elements in a theory (B. G. a. S. Glaser, A.L., 1967). Charmaz (Charmaz, 2006) extends this definition by stating categories explicate ideas, events or processes in the data, and may subsume common themes and patterns in several codes. Birks and Mills (Birks & Mills, 2015) point out it is the grouping of codes that "leads to the formation of categories as the researcher begins to identify explanatory, conceptual patterns in their analysis".

Phase two. Existing codes defined in phase 1 direct analysis for phase 2. The methods for analyzing data in the second phase of grounded theory, are intermediate coding, theoretical sensitivity, core category selection and theoretical saturation.

Intermediation coding. Intermediate coding is comparing codes with codes, codes with categories and categories with categories. Organization of codes and categories begins to occur during comparison and relationships among them are constructed. During intermediate coding, codes and categories may be split into more specific codes and categories and categories may become sub-categories of an encompassing category.

Theoretical Sensitivity. Birks and Mills (Birks & Mills, 2015) define theoretical sensitivity as the ability to recognize and extract from the data elements that have relevance for the emerging theory. Categories from phase 1 activities began to develop themes and emerging theories. These emerging theories were a lens to compare and analyze previous codes and interviews to shape the emerging theory. Categories including vendor reliance, what information security means to the business, and how responsibility is assigned all began emerging as theoretically relevant.

Theoretical Saturation. Straus and Corbin (L. Strauss & Corbin, 1998) define theoretical saturation as the point in category development at which no new properties, dimensions, or relationships emerge during analysis. Saturation has occurred when a defendable theory has been developed grounded in the data. The final interviews provided additional data points that resonated with the developed theory.

Core Category Selection. Constructivist's grounded theory texts define the core category as an identified category that connects categories, subcategories and occurs frequently (Birks & Mills, 2015). Earlier grounded theory texts put more emphasis on a core category being an explicit category while newer research in the constructivist grounded theory epistemology identify a core category as the interplay between categories and subcategories that provide the foundation for the developing theory (Charmaz, 2014). After identifying a core category and achieving theoretical saturation, phase 3 of Birks and Mill's (2015) model can be executed. This phase contains the grounded theory methods of advanced coding and theoretical integration. This research adopted Charmaz's (2014) definition of core category, using the primary categories and their interrelationship as the inputs to developing the theoretical ingratiation of a visual depiction of the theory.

Phase three. The final phase of a grounded theory study is composed of advanced coding and theoretical integration where the final theory is developed and refined.

Advanced coding. Advanced coding provides techniques for facilitating integration of the final theory. Advanced coding identifies connections between substantive codes developed during initial and intermediate coding. This provides an integration of the discovered data and the abstract concepts developed by the researcher.

A common method is to use a storyline to write the developed theory (Birks & Mills, 2015). The storyline explains the theory, implicitly explaining the studied phenomena. According to Charmaz (Charmaz, 2014) advanced coding is not a required method to successfully complete a grounded theory study, but can be useful.

Theoretical integration. Theoretical integration is the consolidation of abstracted theoretical data into a final grounded theory. Birks and Mills (Birks & Mills, 2015) define a theory as an exploratory scheme comprising a set of concepts related to each other through logical patterns of connectivity According to Strauss (Strauss, 1987) theoretical integration is the most difficult part of a grounded theory research study.

Critical to the entire process of grounded theory, memos are created, updated and reflected as the research goes from raw data to theoretical integration. Memos ensure independent review of the research and can show the analytic path taken to reach conclusions and provide the researcher the ability to reflexively analyze work performed during the entire project.

Ethical Considerations

There are strategic, ethical and personal issues in qualitative research when a researcher is a participant (Locke, Spirduso, & Silverman, 2014). The researcher addressed these issues reflexively using Creswell's (2014) approach by describing past experiences and how they may shape the researcher's interpretation of the study. This is especially relevant in constructivist grounded theory because the developed theory was not discovered as the methodology was originally intended, but was constructed through the interpretation of the data by the researcher (Charmaz, 2006). Therefore, the experiences and biases help shape the theory.

The researcher's perceptions of small business information security and the healthcare industry have been shaped by the researcher's professional and academic experience. The researcher has worked within the information security industry since October 2006 across multiple industries including federal, retail, services and healthcare. This diverse experience across multiple environments provides context of nuances for each sector. The researcher has worked within the healthcare industry since January 2016 as a senior information security analyst for a large healthcare provider in South Carolina. The researcher was involved in information security strategic planning, program management and risk assessment processes as a member of a healthcare provider information security office. The researcher has worked closely with senior leadership across all business functions, including compliance, finance, procurement, infrastructure and architecture.

The researcher believed the knowledge obtained through the researcher's professional and academic experience in the information security field coupled with the sensitivity the researcher has developed for the healthcare industry prepared the researcher with a contextual understanding of challenges and issues that may affect this demographic. However, the researcher has never worked specifically with SHPOs.

The researcher allowed the participants to shape the narrative of what the process was under study. The researcher experience was directly related to this area of study that makes researcher bias unavoidable. Every intention was made to be objective in collection and analysis, but it was the interpretation from the researcher's perspective that ultimately constructed the theory that was grounded in the data (Charmaz, 2000). Researchers' assumptions are captured in the assumptions section. Collected data and its objective grounding were closely monitored if developing codes, categories, and theories began to support the assumptions identified prior to the research effort.

Internal, sensitive or incriminating information may be disclosed during the research activity that could cause harm to the research participant personally or to the organization the research participant represents. Therefore, it was incumbent upon the researcher to instill trust and implement confidentiality processes to protect the participant. The researcher also explicitly informed participants not to disclose any known cyber incident experienced by the participant organization.

Multiple techniques were employed to address these ethical considerations, convey trust and promote full, honest responses. IRB approval was sought prior to collecting any data. All research participants were required to read and acknowledge an informed consent form that clearly communicated their rights and expectations to privacy as a participant in the study. Participants and their organization were de-identified. A mapping tool identifying participants and organizations with their unique study identifier was maintained but with strict access controls and data at rest encryption. All data was protected in accordance with the research data management plan. Where applicable, participants were afforded the opportunity to review, clarify and provide corrections on summaries of themes and codes from their interview session.

The researcher would enter into a non-disclosure agreement (NDA) with research participants if the research participant organization required it. This assumed the NDA did not prevent any aspect of the data collection, analysis or findings disclosure.

The researcher utilized a defer technique when a research participant inquired the interviewer about the interviewer's views on a topic. For example, if a research participant were to ask, "what should I know about the HIPAA security rule". The researcher would reply "I do not want to influence your responses. I'll be happy to discuss upon the conclusion of this research study", to avoid researcher and participant bias.

Research Trustworthiness

The reliability and validity of this qualitative research findings are dependent on the rigor applied to the research design to ensure trustworthiness of the findings. Much research has been performed in the area of defining constructs and provisions to ensure trustworthiness (Guba, 1981; Lakshmi & Mohideen, 2013; Shenton, 2004; Sikolia, Biros, Mason, & Weiser, 2013), (Marshall & Rossman, 2014; Maxwell, 1992).

Lakshmi and Mohideen (Lakshmi & Mohideen, 2013) provide a definition of internal and external validity. Internal validity encompasses whether the results of the study are legitimate because of the way the groups were selected, data was recorded, or analysis performed. External validity, often called "generalizability", involves whether the results given by the study are transferable to other groups (i.e. populations) of interest.

Qualitative research requires trustworthiness through validity and reliability to support the credibility of the research (Golafshani, 2003). Validity and reliability are achieved through multiple criteria. Guba's (Guba, 1981) four criteria for assessing trustworthiness are credibility, transferability, dependability and confirmability. Sikolia et al. (Sikolia et al., 2013) focuses these four criteria to the realm of grounded theory research. Relative to this research, the criteria addressed below uses Sikolia et al.'s (2013) identified steps to improve trustworthiness across these dimensions:

Credibility. Credibility refers to the accuracy with which collected data matches the multiple realities of the phenomena being studied and aligns with internal validity (Sikolia et al., 2013). Credibility of this research is addressed below in the internal validity section, using Maxwell's (Maxwell, 1992) sub-categories of internal validity to support the methods employed to ensure internal validity and credibility.

Transferability. Transferability refers to the applicability of one set of findings to another setting and aligns to external validity (Sikolia et al., 2013). Grounded theory uses concurrent data collection and analysis. As abstraction occurs and a theory begins to emerge, previously collected data is compared to the developing theory to disprove aspects of the theory or refine the theory. Once theoretical saturation occurs, the transferability of the research is strengthened.

Exhaustive detail of this research in a dissertation format and the documentation of supporting memos from the study supports transferability. These artifacts will be available upon request to any researcher wishing to understand, dispute or reproduce this work.

The final report includes methods used for data generation and collection, analysis techniques performed and abstraction efforts. Individual and organizational participants were not disclosed as part of this external validity activity due to privacy and agreed upon conventions with research participants.

Dependability. Dependability refers to the accuracy that the collected data represents the changing phenomena over time and is consistent over time, researcher and analysis techniques, and aligns to reliability (Sikolia et al., 2013). Memos were documented to record researcher interpretations, research progress, participant interactions and other research related activities. These memos provided an account of the progress and path taken from raw data collection to grounded theory creation (Charmaz, 2014). Providing a historical account of the research progress strengthens dependability (Sikolia et al., 2013).

Confirmability. Confirmability refers to the objectivity of the research and the ability for another researcher to confirm the same findings presented with the same data set. Similar to dependability, memos providing a rich historical account of the researches progress will be recorded and available with the research findings. This account provides to any outside researcher the complete context and steps this researcher processed through for repeatability or validation.

Further supporting qualitative research trustworthiness, Maxwell (Maxwell, 1992) provides five validity criteria to consider in this research paradigm as identified in the credibility aspect. They are descriptive, interpretive, theoretical, evaluative validity and generalizability. Maxwell points out evaluative validity is not central to qualitative research and the basis of this research is grounded entirely in the data. This research makes no claim to evaluate the things studied to strengthen evaluative validity. Relative to this research, the criteria for the remaining four aspects is addressed below:

Descriptive Validity. Maxwell (Maxwell, 1992) identifies this validity attribute as the most important aspect of validity in a qualitative study because all other validity aspects are dependent on the descriptive validity. Descriptive validity is the factual accuracy of the data to ensure the accounts of interviews and observations are not distorted or falsified. Descriptive validity is concerned with physical or behavioral events rather than their meaning to the participants (Kaplan, 1964).

Interviews were audio-recorded by the researcher. This ensured the ability to validate the accuracy of transcription. Upon completion of transcription, a review was executed to verify the transcription is consistent with the interview.

Interpretive Validity. This research studies the experiences of the subjects participating in the studied processes. Interpretive accounts are grounded in the language of the people studied and rely as much as possible on their own words and concepts (Maxwell, 1992). Interpretive validity does not only apply to the conscious concepts of a participants, but can pertain to unconscious intentions, beliefs, concepts and values (Maxwell, 1992).

Contributing to the credibility dimension of trustworthiness in grounded theory, Sikolia et al. (Sikolia et al., 2013) identifies techniques from the literature to promote interpretive validity utilized in the research including directing inquiry to expand on emerging theory and using participants language in the emerging theory.

Theoretical Validity. Maxwell (Maxwell, 1992) identifies two major attributes of theoretical understanding. The first is the degree of abstraction from the actual studied phenomena. The second is the interpretation of the participants account as an explanation. He points out that theoretical validity is applying a theoretical construct to support explaining a relationship among concepts being studied. While he states theoretical validity “depends on whether there is a consensus in the community concerned with research about the terms used to describe the phenomena”, grounded theory looks to define a theory based on data collected from participants involved with the studied phenomena. As research progresses and theoretical abstraction occurs, theoretical sensitivity will be employed to direct interviews and research participants will define the concepts being identified and will accept or reject the relationships as they begin to emerge.

Generalizability. Generalizability refers to the extent an account of a situation can be applied to other settings and population (Maxwell, 1992). A requirement of grounded theory is theoretical saturation. Theoretical saturation is the situation where additional data collected does not add to or refute any part of the developed theory (Birks & Mills, 2015). Theoretical saturation therefore indicates for a population of a similar demographic the theory would be applicable, and therefore generalizable. Extending the theory to other populations where variables of the demographic are changed to test the applicability of the theory is left as future work.

Provisions developed by Shenton (Shenton, 2004) provide techniques to strengthen qualitative research internal validity. Several of these provisions were implemented in this research study. These provisions and the applicable to this research are:

- Adoption of well-established research methods (i.e. grounded theory)
- Data triangulation - This research intended to interview at least nine participants. Any data that drives theory will be from multiple sources. Triangulation is defined as "a validity procedure where researchers search for convergence among multiple and different sources of information to form themes or categories in a study" (Cresswell & Miller, 2000).
- Honesty from respondents - Addressed in participant, site and sampling section of this chapter
- Negative case analysis – Grounded theory does this by the nature of its approach to refine the developing theory and concurrently apply collected data to it to ensure appropriateness.

- Thick descriptions of experienced phenomena - Charmaz's (2014) approach to grounded theory uses action verbs in all coding and categories to promote thick descriptions and provide narrative capabilities to theories as they emerge.
- Researcher background and bias disclosure - The researcher's relevant background and experience are documented in this research design. Researcher assumptions and the role of the researcher have been documented above. Efforts to limit researcher bias were explicitly utilized.
- Frequent debriefing sessions - This research is part of a dissertation project, therefore the PI has a chair monitoring and supervising all research activities. Throughout the research process the chair was debriefed and had the opportunity to inject comments and concerns to avoid issues with trustworthiness.
- Reflective commentary - Grounded theory uses memos as a foundational element of the research design. These memos are created throughout the research process and provide the capability for reflection on thought processes, findings and research process for all elements of the research study.

Participant and Research Bias

Interviews between a researcher and participants constitute a major component of collected data. Considerations related to the researcher and the participant must be addressed to mitigate the suspicion of the research findings appropriateness. These considerations and their corresponding mitigations are listed:

Participant error. Participant error are factors that adversely impact how a participant performs. This could result from a participant being interviewed while their boss is in the room and wanting to not answer honestly or completely. This risk was mitigated with multiple techniques. First the researcher ensured only those participants that are accountable for information security at the participant organization are involved during the interview session. Secondly, the participants had an opportunity to review and verify responses for accuracy. This follow up provides an opportunity for the participant to correct or expand on any responses.

Participant Bias. Participant bias is any factor that produces false data. Participants may not be truthful in their responses for multiple reasons including providing responses they believe to be desirable to the researcher or socially acceptable. The researcher mitigated this risk by ensuring effective communication to participants of the purpose of the study, the necessity of full and truthful responses, the anonymity of the participants involvement in the study, and confidentiality being applied to their responses.

Researcher Error. Researcher error is any factor that alters the researcher's interpretation of the data. Validity aspects of the research study were utilized to limit researcher error. Additionally, memos were recorded throughout the entire study to provide a chronological history of research progress and theory development.

Researcher Bias. Researcher bias is the influence on a study based on the researcher's assumptions or desire for the study's results. Researcher bias was a legitimate risk that was addressed to maintain trustworthiness of the study findings based on the researchers experience in the information security field and the healthcare industry.

The research study's PI worked for a medical university within the state of South Carolina, effectively a competitor to participants businesses. Two approaches were incorporated into the research design to address potential conflict of interest and introduction of researcher bias. These approaches were:

- Verbal informed consent disclosed this association to research participants.
- Research participants were provided aggregated, anonymized data of the research findings upon conclusion of the research.

These activities were designed to avoid any conflict of interest or scrutiny over the validity and reliability of the results from this study.

Assumptions

Assumptions the researcher had about what may be discovered during the study or what factors are influencing information security program management decisions are documented in the research design. The PI had no prior experience with SHPOs and therefore brought no assumptions of findings into the research.

The following lists researcher assumptions:

1. Small business health care providers are aware of HIPAA
2. Small businesses are aware of the necessity of implementing security controls but due to a lack of understanding on how to implement or a lack of understanding on the scope of threat vectors, choose not to implement.
3. Availability is the primary security objective of interest to small business health care providers.
4. Healthcare providers recognize HIPAA as applicable legislation, but value it as ‘not having teeth’ and therefore do not feel compelled or motivated to comply.
5. The experience of a cyber-attack on an organization makes the hypothetical a reality and shifts attitude of information security control priority to a small business.
6. Small businesses believe they are too small a target to cyber criminals to be targeted.

Any findings that align with predisposed assumptions were validated with additional rigor to verify the applicability of the finding.

Limitations

The definition of small within the context of SHPO is a limitation elected by the researcher. There is currently limited research on small healthcare providers and there is no consensus-based, accepted definition for healthcare provider organization sizes. Healthcare providers organization size are measured multiple ways depending on the organization or research group measuring them. SBA bases size on generated revenue, dependent on business-type as defined by the North American Industry Classification System (NAICS). Healthcare providers, specifically “Offices of Physicians (except Mental Health Specialists) NAICS Code: 621111” are considered small if they generate less than $11M annually (SBA, 2018). It is not unreasonable to consider a 10-physician healthcare provider in a very affluent region, offering very expensive procedures to exceed $11M annually. This would exclude them as a SHPO, despite their staff size.

The American Medical Association (Kane, 2017) conducted research and found that more than half of all healthcare providers in the United States have 10 or less physicians on staff. This quantified value represents a majority of healthcare providers in the United States and is a staff headcount consistent with an organization that would be in the target demographic. Therefore 10 physicians or fewer on staff was defined as part of the demographic requirement for in-scope research participant organizations.

The PI lived in Charleston, SC. Limiting research participants location to South Carolina was a geographical limitation of the researcher’s ability to reasonably conduct research.

Chapter Summary

This chapter documents the research protocol for this study. It presents a detailed description of the population to be included in the research, the methods to collect and generate data, and the methods for analysis documented. Research findings aligned to the identified processes.

The research approach utilized interviews, focus groups, memo writing, concurrent data generation and analysis as methods to develop raw data. The PI was positioned as a participant in the research, conducting unstructured interviews initially and transitioning into semi-structured interviews after thematic categories begin to develop from initial and intermediate coding activities, allowing individuals to share their views. The immersion into the setting of the participant and the open-ended approach to interview questions provided participants unfettered opportunity to express subjective meaning of their experiences (Crotty, 1998).

There was little research on information security at SHPO, requiring exploratory research. Grounded theory is a suitable research methodology for exploratory research designs. This research has a defined research participant population and setting for conducting the interviews, the primarily employed research method. Grounded theory provides systematic data analysis procedures that were executed to process through the grounded theory methodology.

Research trustworthiness, ethical considerations and biases were accounted for and were documented to provide rigor to the final research deliverable.

CHAPTER 4

FINDINGS AND DISCUSSION

Introduction

This qualitative research studies factors affecting cyber security decisions at SHPOs in South Carolina. Grounded theory techniques were utilized to inductively develop a theory explaining the operational processes associated with these decisions and why these organization types have challenges securing their assets.

This exploratory research provided visibility into an area currently with little literature. Additionally, it can facilitate additional informed research for SHPOs.

This chapter presents the key findings from nine intensive interviews with personnel accountable for information security at their organization. The key findings interrelationship is discussed to support the theory generated from the grounded theory methodology.

First the composition and execution of the research is presented. This includes details on research participants, operational execution of the research, and the evolution of the coding activities during research. Next six key findings are presented that directly support and interrelate with the developed theory. Following this, the developed theory is presented and explained in totality. This chapter ends with discussion of the theory and key findings.

Further promoting confidentiality, any reference to third-party vendors in this report are replaced by fictitious company names based on the Greek alphabet (i.e. Alpha, Beta).

Methods

Research Participants. IRB approval was required for this research due to the inclusion of human subjects. Dakota State University IRB reviewed this research protocol and determined the best course of action would be for the Medical University of South Carolina (MUSC) IRB to provide this function. IRB approval was issued by MUSC for this research. IRB approval can be referenced in Appendix C.

An IRB approved social media marketing campaign was initially used for participant solicitation. Additionally, the researcher contacted the president of the South Carolina Medical Group Management Association (SCMGMA), a professional association composed of healthcare practices from across South Carolina (SCMGMA, 2019). This is an ideal association to identify in-scope participants. The PI engaged leadership at SCMGMA to share the research study and act as a medium for soliciting their members as research participants. Six of the research participants were either directly acquired through this organization or from snowball sampling from a participant initially identified through SCMGMA.

There were fourteen candidates that were engaged for participation (see Table 4). There were nine research participants interviewed for this study. Some participants were from the same city, but the population represented a diversity of areas within South Carolina. Furthermore, the participants represented a range of healthcare provider organization types including, but not limited to, pain management specialists, dermatology, and surgical practices.

The state of South Carolina is geographically divided into four regions: Upstate, Midlands, Lowcountry, and Pee Dee. The figure below from SCDHEC illustrates the allocation of these regions (SCDHEC, 2019). The participant table below includes the region of each participant.

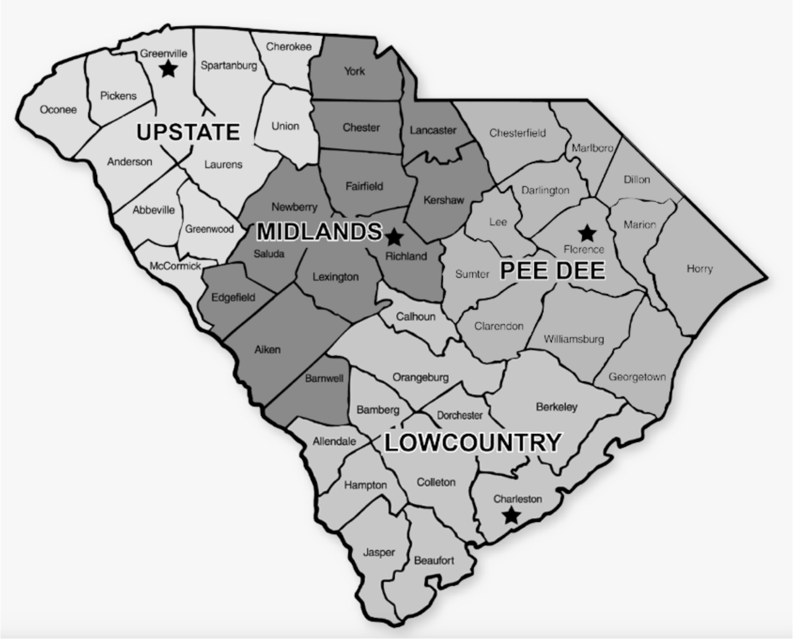

Figure 2 - South Carolina regions

The following table provides demographic data of the information security responsible personnel (IRP) participant population and assigned pseudonyms. Unexpectedly multiple candidates spoke with me during recruitment and were interested in participating. However, they did not attend the interview during our scheduled window and failed to ever respond to further communication.

Table 4 - Participant demographics

ID	Name	IRP Role	SHPO Type	SC Region	Status
1	"PR1"	Practicing Physician	Otolaryngology	Pee Dee	Expressed interest to referring participant (snowballing) on multiple occasions; Unable to establish communication to recruit.
2	"PR2"	Director of Operations	Family Medicine	Pee Dee	Initially believed to meet participant criteria, but had more than 10 providers.
3	"PR3"	Practice Administrator	Pain Management	Midlands	Study Participant
4	"PR4"	Practice Manager	Pain Management	Pee Dee	Did not attend interview. Ceased communication.
5	"PR5"	Practicing Physician	Rhinoplasty	Lowcountry	Study Participant
6	"PR6"	Managing Director	Polysomnography	Pee Dee	Study Participant
7	"PR7"	Practice Administrator	Dermatology	Midlands	Study Participant
8	"PR8"	Practicing Physician	Anesthesiology	Lowcountry	Study Participant
9	"PR9"	CFO	Oncology	Lowcountry	Study Participant
10	"PR10"	Practice Administrator	Dermatology	Lowcountry	Study Participant
11	"PR11"	Practice Administrator	Dental	Lowcountry	Did not attend interview. Ceased communication.
12	"PR12"	Practice Administrator	General Surgery	Pee Dee	Study Participant
13	"PR13"	Manager	Dermatology	Pee Dee	Expressed interest to participate. During scheduling, ceased communication.

ID	Name	IRP Role	SHPO Type	SC Region	Status
14	"PR14"	Practice Manager	Clinic	Lowcountry	Study Participant
15	“PR15”	Practicing Physician	Anesthesiology	Upstate	Expressed interest to participate. During scheduling, ceased communication.

Research Execution. All interviews were executed in accordance with IRB requirements. All interviews were conducted over the phone via a WebEx connection and lasted between 45-60 minutes. The ability to conduct a “face-to-face” video teleconference was offered and only one participant elected to participate. All other interviews were audio only. All interviews were recorded, and the participants were aware and agreed to being recorded.

Every interview began with a preamble to ensure participant rights and awareness. This preamble was IRB approved. The preamble was:

> Thank you for your time and speaking with me. I am a doctoral candidate. I currently work at the Medical University of South Carolina, researching small business healthcare cybersecurity decision processes. I would like to talk in generalities to get an understanding of the types of security issues you may face. I do not want to know explicitly if your company has had a successful breach or experienced a successful cyber-attack.
>
> The information provided will remain strictly confidential and you will not be identified by your answers. You and your company’s name will not be disclosed in any way. Data will be compiled with no individual responses tied to your name or any identifying information about you. I would like to record this interview. All information disclosed during our conversation will be kept in a

secure location. You may choose not to answer any question. Do you have any questions before we get started? Are you willing to participate?

I will begin recording this interview session now.

A semi-structured interview protocol was utilized to manage the interview. The interview guide, Appendix B, had ice breaker questions, information security program questions, ending questions, and probes to elicit more information. Information security program questions were focused on threats, financial factors, regulatory influences, and decision-making processes. If a participant mentioned an item that was an emerging concept, based on coding practices, probes were used to explore this topic further.

Completed recordings were transcribed and imported into Atlas.ti, a qualitative data analysis tool. Analysis began immediately following the import of the first interview. Analysis continued throughout entire research execution.

Coding. Coding provides a method to begin to identify patterns and areas of emphasis in the data. Concepts, themes, keywords, and language from transcriptions are identified and labeled. Initial coding covered a large area of topics. Several codes identified initially did not persist through research analysis. Codes that did not persist were either absorbed into like codes that captured the essence of the concept or were isolated codes that were interesting but did not support or resonate with emerging categories.

The researcher began comparing and contrasting the codes themselves after initial coding the first 4 interviews. There were over 100 codes at this phase of analysis. Reviewing codes and abstracting them with regards to what the code was referring to or a property of resulted in the emergence of categories. These categories, called code groups in Atlas.ti, served as logical grouping of codes. This further allowed for analysis and logical thinking of what was happening in the data. Subsequent interviews followed the same protocol, but areas of emergence would be further probed for properties and dimensions from the participant if they surfaced during the interview.

Codes were compared to codes to determine if they were different codes, but conceptually the same. If they were conceptually identical, the codes were merged. An example of this was “hacker as a threat” and “fear of someone out there on the Internet attacking us” being merged to “hacker as a threat”.

Codes were compared to concepts, concepts to categories, categories to categories, concepts to concepts to promote abstraction of concepts and understand relationships among these pieces as the coding process progressed.

The activity of coding interviews then comparing and contrasting codes to codes and codes to categories happened several times throughout the research. As coding continued several thematic areas began to emerge. Grounded theory seeks a core category to allow for further analysis to refine and illuminate. The core category is the relationship and propagated assumptions SHPOs have about their IT providers coupled with the organizations narrow concept of what comprises information security.

Codes and categories were revisited to analyze their property or value with respect to this core category. Following the identification of the core category, codes that did not relate were disregarded during further analysis. Previously coded interviews were revisited following core category to identify data that relates. This was a useful activity as each time reviewing transcripts with a different perspective or focus resulted in “seeing” more relevant data points.

At the completion of the research there were 136 codes and 17 categories. These codes and categories can be referenced in Appendix D.

Findings

A data summary table, Appendix G was constructed based on Bloomberg and Volpe (Bloomberg & Volpe, 2012) with emergent categories that provided dimension to the core category. The descriptors were: risk-based program, security seen as privacy, Trust IT vendor with security, reliance on vendor, risk analysis performed, self-confidence in security program effectiveness, support for HIPAA, support for operating in a secure and compliant manner. These descriptors drove the findings documented below. Based on these findings, a theory was developed that explains why information security at SHPOs has limited effectiveness despite internal and external factors.

The final three interviews utilized the same interview guide used as previous interviews. However, as theoretically relevant topics would come up, such as the reliance and trust of the vendor, the participants perspective of how security related to privacy, and the execution of risk analysis activities were all further discussed to support theoretical sensitivity and saturation.

Six major findings that directly support the constructed theory emerged from the study. These findings are:

1. **Limited IT and information security knowledge -** An overwhelming majority of participants (7/9 or 78%) self-identify as having limited understanding of IT and information security.
2. **IT vendor trust and reliance -** An overwhelming majority of participants (7/9 or 78%) trust and are reliant on their IT vendors explicitly for IT knowledge and expertise and implicitly for information security knowledge and expertise.
3. **Assuming IT vendors provide security -** A majority of participants assume security (6/9 or 67%) is inclusively part of IT and therefore is provided by their IT vendor.

4. **Narrow definition of security -** A significant number of participants (5/9 or 56%) have a narrow view of information security, seeing it as a privacy or confidentiality activity only.
5. **Information security program confidence –** Nearly all participants (8/9 or 89%) are confident in the effectiveness of their currently constituted information security program and have internal drive to invest and add controls to reduce risk to acceptable levels.
6. **IT is outsourced –** Nearly all participants (8/9 or 89%) outsource their IT operations.

The following provides supporting data for these findings. The utilized research methodology employed intensive interviews from participants living the experiences. Quotations from the participants are utilized to illustrate the nuances of the findings. Specific quotations are not selected because they best make the case for the finding (i.e. "cherry-picking") but are selected to represent the attitude of the participant population relative to the finding.

Finding 1. An overwhelming majority of participants (7/9 or 78%) self-identify as having limited understanding of IT and information security. Several participants explicitly shared this admission and others implicitly did through describing their reliance on their outsourced IT vendors to support their business and business decisions. None of the participants responsible for information security at the businesses were acting in an IT role or had an IT education related background. Many saw the inclusion of IT as a necessity for operating their business.

Many participants shared varying responses about their knowledge base of IT and information security, all which indicated a gap. PR12 described her knowledge with technology specifically as: "I'm not good with technology. I mean, I put up with it because we have to do it" (PR12).

The individual responsible is often times a business manager and administrator who “owns” the responsibility despite the gap in knowledge. This results in guessing best course of action. PR7 shared her responses when staff members approach her about rules on inter-organizational communication of PHI:

> I’m not an IT expert so I have to make the best decisions that I can and sometimes it’s more on the safe side even though it might be okay I just say maybe don’t do that until I have further information on how to do that appropriately. I’d rather be safe than sorry. (PR7)

Most participants have not sought additional information security education to make better decisions, but rather relied entirely upon their IT vendor. Some participants commented hearing about information security related events from the news or colleagues, but this is only incidental. PR9 shared on what information he uses to stay informed on information security: “I keep up with, you know—every now and then I’ll read newsletters just enough to be dangerous and get scared with the cyber security and all of the breaches that are out there” (PR9).

Multiple participants commented on the rate that technology evolves exceeds their ability to gain knowledge in it. This factor promotes the persistence of these individuals having limited IT knowledge. Participants indicated they have several areas of responsibility that makes maintaining an understanding of IT and information security very difficult. PR7’s comments illustrate this reality when asked if information security was not a priority at her business:

> I maybe a little bit yeah I would say but not intentionally not a priority not that I know it’s a risk but I’m going to kick it to the bottom of the list but I think the physicians have a lot on their plate and I guess it’s my job to worry about that and figure out how to make sure’s safe and secure and all that.

> I handle a lot of different areas it's hard to be an expert in every single area I got to be an expert in the financial side of it in using our bookkeeping software and speaking with the accountants and making sure we're on the up and up about with their bookkeeping software and our taxes in the way I'm processing payroll and paying our physicians and then I have to worry about the operational side is my clinic functioning properly are we efficient. Am I, you know that I have to worry about the customer service part of it are my patients happy are we training in retraining our front desk employees about how to handle tough situations with patients and get them what they need.
>
> Then I'm worried about speaking with my attorneys and thinking about legal risk and then there's the cyber part I think it's difficult to be an expert in every area's and think about all the stuff and I think with the cyber part of it is that a changes and evolves so much faster then anything else that it's difficult to keep up with that also (PR7)

Multiple participants shared comments at the end of interviews that the activity of the interview resulted in an increase in knowledge about information security. Specifically, one participant stated: "Doing this discussion with you has certainly helped me to think about that collect my thoughts on that" (PR5). Another participant shared specifically: "No, you have asked some good questions made me think about things and how we do things" (PR6). Another commented:

> Yeah I guess there are several things that I haven't sat and talked about cyber security this long in my role maybe ever, but yeah I think you are making me think about it harder than I did before and what I need to do about it. I think

> I've been a little bit more reactive to things then more proactive it is a big deal but yeah I don't think I've ever talked or thought about it this long or hard so. (PR7)

The finding of limited IT and information security knowledge for IRP supports Finding 2.

Finding 2. An overwhelming majority of participants (7/9 or 78%) trust and are reliant on their IT vendors explicitly for IT knowledge and expertise and implicitly for information security knowledge and expertise. One participant that this finding did not apply to was fully "on paper" and did not utilize IT as typically seen in today's SHPOs. Detailed in Finding 6 below, no participant businesses had in-house IT staff; nearly all outsourced their IT business needs, except one with no IT. Particularly given the limited IT knowledge of respondents, the amount of trust and reliance on the IT vendor is significant. Indeed, all participants conveyed their reliance on their IT vendor in their business operations. In fact, one participant shared that since the IT vendor handles security, the business therefore implicitly trusts the vendor to implement effective information security controls at their practice: "Again the IT firm handles that, so I trust them. They know to what degree we need to be protected" (PR6). This trust and reliance were not founded on contractual protections or described thoroughness of the IT vendor's approach to information security but rather on the IT vendor's positive reputation within the local business community.

In addition, several participants shared their business need to rely on their IT vendors because of their own limited knowledge and broad scope and priority of the participant's responsibilities. PR12 commented:

> That's my responsibility here in the office: to make sure that things run smoothly within the office. When it comes to technology and cyber security I

> have to—because I'm not familiar with it I have to rely on companies like Alpha and Beta that they're doing their job. (PR12)

PR12 later in the interview made a comment that indicated her reliance on their IT vendors was an appealing relationship: "We don't want to be thinking about technology. We just want to know that our technology's working, that the patients are safe" (PR12).

PR7's comments echoed many participants, further supported by finding one: "But I guess it was my background in healthcare administrations. I rely heavily on my vendors to help me make sure my stuff is safe". (PR7)

Further developed in Finding 3, IT vendors are not only trusted and relied upon for IT but also information security. PR9 commented:

> I generally rely on my IT guy here that I really trust. I usually ask him, if he suggests a particular mitigation strategy, to give me a couple of vendors and the pluses and minuses of both as well as the cost of each, and then we move forward based on that information. (PR9)

When further questioned as to why IT vendors are trusted and relied upon for security, many participants indicated this was simply "trust," transitively extending positive experiences and reputation in IT to provide security services. Perhaps IT vendors reinforce this trust by "talking security" to practice's representative, who unfortunately has limited knowledge of the topic. Therefore, the IT vendor may legitimize their position as knowledgeable, reliant, and trustworthy despite their actual information security knowledge level. PR9's comments directly above were followed up with the question "why do you trust the vendor?" PR9 stated: "You know, it's hard to put your finger on it, but sometimes you can just talk to somebody and just realize that they know what they're doing" (PR9).

The implicit trust extended to IT vendors was often seen as an assumption of acceptable levels of execution. PR5 commented on how cyber security factored into his decision on trusting a vendor:

> I guess there were a couple decisions. Did they seem legitimate company, it wasn't something a little bit shady and I had questions, so I kind of put that trust in there that they were going to follow through with whatever the standard for information technology and security and just trust that was there to start with, for me personally I don't know the specifics and ins and outs that would be done on a technical level. So, I wasn't really interested in asking those questions to make comparisons, for me it was more about the product itself. (PR5)

All participants are forced to extend some level of trust to third party vendors since they outsource their IT operations. Trust and reliance seem tightly coupled for the participants with respect to their IT vendors. Furthermore, it seems the greater the general reliance the greater degree of trust about information security is required. While a majority of participants indicated they collaborate on information security decisions with their IT vendor, they acknowledged that the IT vendor was the driver of the decision itself.

Finding 3. A majority of participants (6/9 or 67%) assumed information security to be part of IT and therefore provided by their IT vendor. The IRP's limited knowledge of IT and information security fosters the trust and reliance in their IT vendor. This extends the perceived scope of the IT vendor's service offering to include security.

It was unknown by most participants if contractual language with IT vendors included explicit terms for security related services. IT vendors are providing and maintaining technology (i.e. workstations, servers, printers, network devices) that most often have some security controls fundamentally incorporated. For example, it is fairly standard for any modern workstation to require a username and password to login to the computer, and also for critical applications to be user-specific password protected. This is an information security control and one that an IT vendor would be associated with from a participant's perspective. This results in participants making the association of their IT vendor with information security as a general fact, despite the fact that information security extends beyond IT to include operational and administrative controls.

One participant comment concisely echoed many of the participants position: "Again the IT firm handles that, so I trust them. They know to what degree we need to be protected" (PR6). While PR6 stated he collaborated with his IT vendor on information security related decisions, he made multiple comments suggesting the collaboration was more of a governance role. Strengthening this commonality, PR7 shared "...from our cyber security in general I rely a lot on my IT vendor…" (PR7).

Another participant's comments clearly demonstrated the implicit extension of security to the IT vendor. When asked how cyber security related investment decisions are made and what evidence or metrics are leveraged to inform that decision, PR9 shared:

> I generally rely on my IT guy here that I really trust. I usually ask him, if he suggests a particular mitigation strategy, to give me a couple of vendors and the pluses and minuses of both as well as the cost of each, and then we move forward based on that information. (PR9)

The IRP's limited knowledge of IT and information security fosters the trust and reliance in their IT vendor. This extends the perceived scope of the IT vendor's service offering to include security.

Finding 4. A significant number of participants (5/9 or 56%) have a narrow view of information security, seeing it as a privacy or confidentiality activity only. A majority of participants had a primary cyber security concern of suffering a data breach and their focus for security control was around protecting the confidentiality of PHI, often referred to interchangeably by participants as patient information.

Participants responded in different ways about their cyber security concerns, but the majority were concerned with a patient privacy breach and compromise of confidentiality. PR9 discussed his fear with physicians at his practice losing their mobile phone because (against policy) they text patient information and this could result in a breach. PR12 discussed her concerns of having patient information on a display or print out, face up on desk and being seen by unauthorized parties. PR7 put it plainly when asked her primary concern from a cybersecurity perspective: "Primarily I am always worried about my patient's information" (PR7).

Interpretation of HIPAA by the participants demonstrated it was viewed as regulation to promote privacy and confidentiality of PHI. This further supports the motivation of the practices to seek out controls to promote confidentiality. HIPAA has both a security rule and a privacy rule. Based on participant responses, the security rule has the goal of achieving and maintaining confidentiality in support of the privacy rule. PR5 shared his thoughts on HIPAA that demonstrates the scoping of his interpretation of the legislation:

> There are things that I guess are sort of these rules that have to be followed or penalties for not following those, that seem maybe not strict but the potential harm in having that information get out into the wrong hands is really

> significant. And I do believe personal health information is very something that is critically important to protect. It’s something that should be private and should be held private especially as technology evolves over the years it becomes very hard to kind of keep up with all that. (PR5)

Some participants discussed protected staff information and financial information as assets to secure, but patient information was regularly referenced by participants as the critical asset requiring security.

Finding 5. Nearly all participants (8/9 or 89%) are confident in the effectiveness of their currently constituted information security program. This was an unexpected finding given that research suggests healthcare businesses identify as having shortcomings in information security posture (Institute, 2016; Martin, Martin, Hankin, Darzi, & Kinross, 2017).

Many participants believe their initial and continuing information security controls and posture are adequate. Participants (6/9 or 67%) stated they would make changes as needed but in more of a reactive manner than proactive manner, or to say it bluntly, nothing bad has happened that they are aware of so their information security must be appropriate. PR12 commented:

> Cyber security doesn’t really come around here. that’s why it’s so—it’s kind of weird. Because I’m like yeah, we really don’t think about that. I mean, we did. We have everything in place. I’m sure changes are going to happen, you know, but they don’t happen like instantly. Something needs to happen it’ll happen…. Now, if the computers are running slow or if we feel like somebody hacked, that’s when, you know, we start thinking about oh, shoot, something’s happening, you know, we need to get in touch with our IT department or, you know, cyber, you know, security and stuff like that. But we don’t really—it’s

> not something that we think about. Now, maybe because we’re confident that we are safe. (PR12)

Finding 3 justifies this finding in that participant organizations are viewing the scope of their IT vendors responsibility to include security. The IRP accepts security is properly addressed through their IT vendor, whom has established the IRP’s trust and reliance (Finding 2). Therefore, the IRP feels confident in the information security posture.

When discussing with PR6, who stated his IT vendor handles information security, what the frequency for meeting and discussing information security was between the IRP and the IT vendor, it was revealed that security was initially technically implemented and normal operating practices were to hold security related meetings in an ad hoc reactive nature to incidents.

> Yes, it's more ad hoc as needed most of the time when we have conversations it’s because maybe the Internet you know there's a problem with one of the servers or something not the server maybe one of the backups, somethings wrong with it. Or we have, we use software that does diagnostic testing sometimes it's problems with that that we have to work out those problems can pop up about anytime but with our firm though they have a firm grasp on what we need and what we expect and they're very good at taking care of our needs so it’s the security part is not one that comes up a lot because we have the understanding that we need to do whatever it takes to make sure we're secure. I think, again I lean heavily on them to make sure we, everything is good I have confidence that they follow the best practice. (PR6)

Based on PR6's responses, the ad hoc services are related to traditional IT functions (i.e. break/fix) and less information security risk management. This underlines likely misplaced confidence in the program while highlighting why the misunderstood perception would be made.

Some participants were confident in their current security program while contradictorily stating they knew of gaps in their security and areas of improvement but choosing not to take action to mitigate. Specifically, when asked about his practice's security control effectiveness PR5 stated:

> I think they are effective, they are fairly effective in practice, but there are things that could certainly be improved upon for sure that probably the most succinct way to answer that. Like I said we haven't had any issues, or at least nothing I'm aware of and I would assume if there were anything of consequence or significance that would have had showed itself.
>
> I know we have the most basic things in place, I feel comfortable with that. But there are certainly weak points or points where we may not be following exactly the right protocols or things like that that need to be improved upon. I wouldn't say it isn't perfect, certainly. I don't think you can ever say anything is perfect because it needs to evolve, but I wouldn't say the security protocols are great. I would say they are good, they have been effective and are currently effective the way we are using them but certainly need to be reviewed and improved upon. Even if I didn't think that now, I would at least from time to time, whether its annually or whenever, there's an importance to looking at that more routinely. (PR5)

Two participants were confident in their security program's effectiveness while acknowledging there was room for growth.

Finding 6. Nearly all participants (8/9 or 89%) outsource their IT operations. This includes IT professional services and cloud-based software solutions (e.g. EHR). This finding applied to all participating practices, except for one that was fully "on paper" and did not utilize IT as typically seen in today's SHPOs.

This business decision is rooted in the organizations needing IT for business operations. Outside of clinical operations most participant organizations outsource ancillary services including payroll, legal, marketing, etc.

Outlined in Finding 3, the IT vendor has high importance and impact on the security of the organization. Participants are not evaluating IT vendors for their security ability or ensuring security is factored into contract language. Often times the relationship is based on a trusted referral. Only one organization had elected to have a dedicated IT outsourced staff member present on-site full time to provide timely access to an IT resource.

Theory

The "flashlight in a dark room theory" is based upon research findings, utilizing grounded theory methods. The overarching theory shows organizations outsource IT operations in a trusting and reliant relationship, confident their IT vendor is effective, partially due to their own limited technology and security knowledge. Security is implicitly perceived as an IT function and through transitive properties organizations establish confidence in the effectiveness and appropriateness of their security implementation. This results in an organization's perceived cyber risk exposure not aligning with its actual exposure

Metaphorically speaking, organizations are using a flashlight in a dark room of cyber risk. The space that is illuminated represents their understanding of what cyber risk is and the controls they have implemented to mitigate the risk, but this does not account for the cyber risk that is not illuminated.

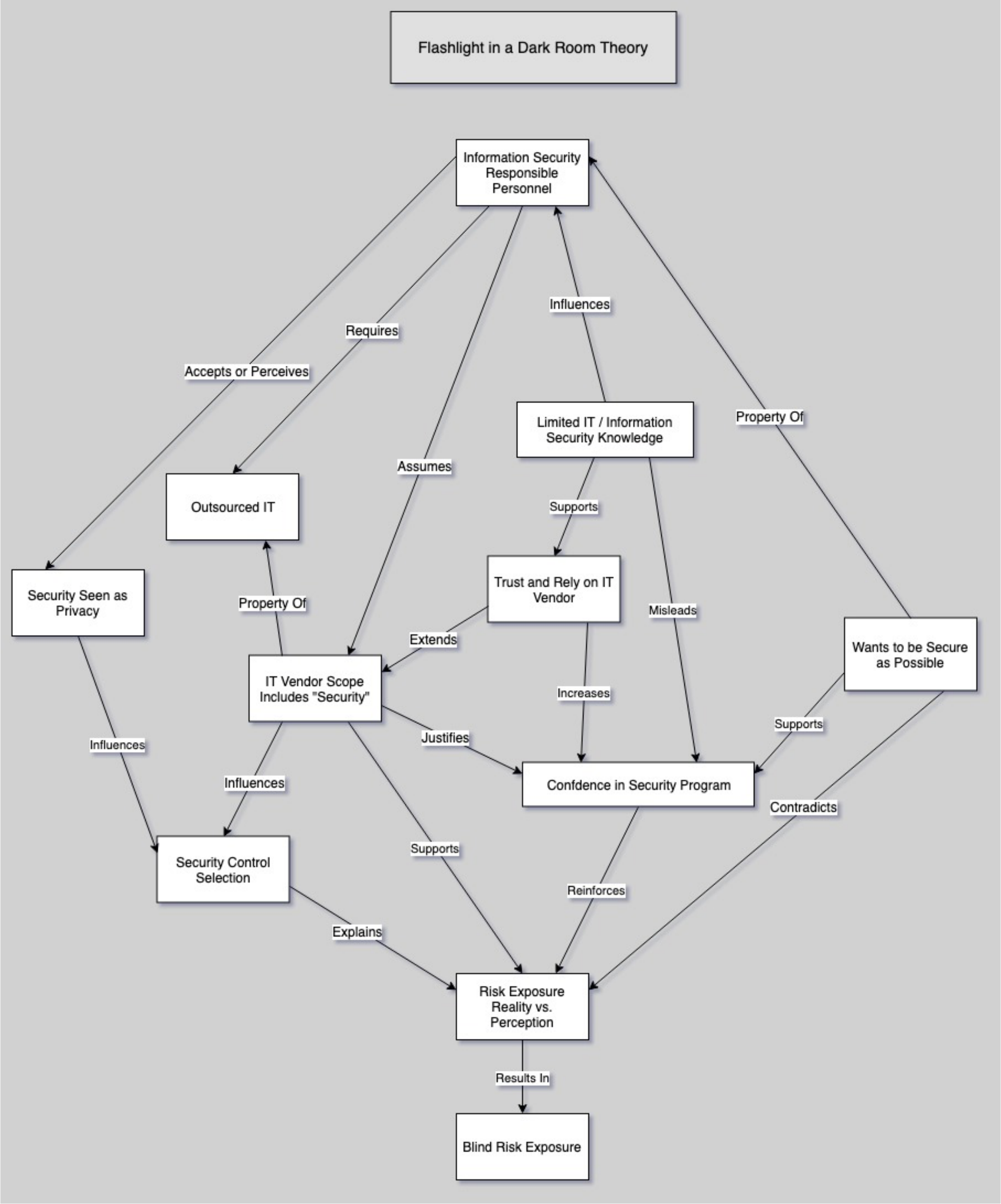
Flashlight in a Dark Room Theory
Information Security Responsible Personnel
Influences
Requires
Accepts or Perceives
Property Of
Limited IT / Information Security Knowledge
Assumes
Outsourced IT
Supports
Trust and Rely on IT Vendor
Security Seen as Privacy
Property Of
Misleads
Extends
Wants to be Secure as Possible
IT Vendor Scope Includes "Security"
Increases
Influences
Supports
Justifies
Confdence in Security Program
Influences
Contradicts
Security Control Selection
Supports
Reinforces
Explains
Risk Exposure Reality vs. Perception
Results In
Blind Risk Exposure

Figure 3 - Flashlight in a dark room theory

The theory is presented in a quasi-entity-relationship diagram (ERD). The entities and relationships in the diagram refer to findings or thematic areas that emerged from the research. The following explains in greater detail the entity and relationship elements in the diagram.

The IRP represents the research participant interviewed. Recall this research required the interviewing of the individual that is responsible and accountable for information security at the practice. This was always an individual that did not have formal IT training.

Limited IT and information security knowledge were a universal characteristic of the IRP. This was self-proclaimed explicitly by some participants and implicitly by others. This concept influences how the IRP understands the scope of security and the function of IT within the context of an organization's information security program.

IRPs consistently demonstrated a desire to be as secure as possible meaning their organizational information security controls are sufficient to protect the organizations data assets and to be compliant with HIPAA.

The limited related knowledge to the IRP supports the finding that IRP's trust and rely on IT vendors. This trust and reliance results in the IRP having confidence in their security program's effectiveness. This further supports the IRP's confidence in their program because they are actively engaged to ensure the organization is as secure as possible, which they perceive as a truth. The IRP sees the scope of the IT vendor's work to include security activities. This is resultant from technical security controls being implemented by the IT vendor and being interpreted by the IRP as the scope of required security controls to "be secure".

IRP's perception of what represents security for their organization is often perceived as privacy controls and security controls that protect the confidentiality of patient information. This is reinforced via prominent news stories of healthcare-related data breaches resulting in financial penalties to healthcare organizations and experienced incidents of privacy breaches for IRPs.

The scope of the IT vendors statement of work for participant organizations is perceived to include security by the IRP. Furthermore, perception of security to the IRP is seen as controls that mitigate risks that threaten confidentiality. Thus, security control selection implemented at the organization is influenced to address breach of confidentiality and seen as an IT matter.

The security control selection, the narrow perception of what security means to the IRP, the assumption of security being addressed by the IT vendor, and the confidence the IRP holds in the SHPO's security program explains the IRP's perception of risk exposure being misaligned with the organization's real risk. This misalignment answers why SPHOs do not have very effective information security controls despite internal and external factors.

Discussion

This research set out to understand why information security at SHPO is not very effective despite internal and external factors promoting the opposite. This area of research is limited, with very little literature looking at information security for these business types. Therefore, it made logical sense to utilize a qualitative research methodology to explore this space and understand the dimensions of the problem and develop a theory to explain what is actually occurring to create this phenomenon.

The purpose of this section is to provide the researcher's interpretation of the findings. These interpretations are informed by the findings themselves, the complete interview experience the researcher had with each participant, the researcher's own world views and professional experience, and the current literature.

Nearly all participants acknowledged their limited knowledge of IT. Finding 1 includes both IT and information security as the limited knowledge area, but most participants were unable to distinguish between the two topics with any level of accuracy.

IRPs are responsible for several facets of the business operations including technology. Kruse et al. (Kruse et al., 2017) show the healthcare industry struggles with new technology. The voiced frustration by some participants indicated technology was a losing proposition to stay knowledgeable on: “cyber changes and evolves so much faster than anything else that it’s difficult to keep up with that” (PR7). IRPs want technology to support the organization's mission and they “don’t want to be thinking about technology” (PR12). Implementing security is inclusive this delegation. Therefore, they not need to be IT or information security knowledgeable.

An interesting and unexpected observation was the increase of information security knowledge for the participant simply from participating in this research study. Multiple participants commented at the end of the interview on their level of attention they have given toward information security at their organization and their heightened awareness to remedy that going forward. This may result in increased cyber security activities. However, Johnson and Koch’s (Johnson & Koch, 2006) survey-based research showed (industry-agnostic) small businesses, will not take action to remediate information security risk if made aware of it.

An ancillary observation noted four research candidates that chose not to participate. This is within their rights as candidates, but the manner in which they chose to not participate was interesting. All four candidates engaged in positive communication regarding the research study and their desire to participate. Two of the candidates, PR13 and PR15, ceased communication altogether when it reached the stage of scheduling an interview. Two of the candidates, PR4 and PR11, scheduled interviews with the PI, but did not show up for the interview. All four participants never responded to any further communication from the PI which included two communications regarding scheduling (PR13, PR15) and two communications regarding failure to attend the agreed upon meeting time for the interview (PR4, PR11).

The demographic of these four organizations are similar to the nine participants in this study. Many other participants found speaking with the PI during the interview increased their awareness of information security. There is not enough data and it was not the objective of this research study to determine why these participants ceased communication and did not participate.

The basis of participants knowledge of information security was the perceived interpretation of HIPAA, real-life cyber incident experience, cyber incidents in the news, or stories from colleagues. This knowledge was often related to a confidentiality compromise such as stolen work papers from a car or snooping on a patient record without just cause. This reinforced the findings of limited knowledge in the space and the emphasis and nearly singular objective focus of security control selection to ensure confidentiality.

Mayer, Davis, and Schoorman (Mayer, Davis, & Schoorman, 1995) identify the three factors of trustworthiness as ability, benevolence, and integrity. Participants were very trusting of their IT vendors. The IT vendors had significant privileged access to the participants organizational information assets and business operations, but not once did a participant mention any concern about their IT vendor from an organizational risk perspective.

The limited knowledge participants have in IT and information security increases their assigned value of ability of their IT vendor. Increasing the ability value therefore increases the trustworthiness of the vendor to the participant.

Many participants related the quality and reliability of their IT vendor to the timeliness, accessibility, and the stability of the organizations IT. When asked if information security was a factor in selecting their IT vendor, PR6 said: “Well I mean just their experience with them being timely being a good firm being up to date on current practices that are best practices all of these are factors in our decision to choose them as our IT firm.” (PR6). Therefore, an IT vendor is reliable if they ensure the organizations computers are fixed in a timely manner if they break and that they can be reached easily if needed. This is equated with IT vendor competence. Per Mayer et al. (Mayer et al., 1995) work this IT competency establishes trustworthiness.

Information security implementation is being seen as an IT exclusive issue by the IRP, despite the participants referencing non-IT related controls such as training and awareness for staff on secure practices and policy development. When PR14 was asked what information security responsibilities he had, his response was "We have a cyber person" (PR14), referring to the organization's IT vendor.

As previously discussed, limited knowledge of IRPs coupled with the assumption that IT vendors are information security experts corroborates SPHOs view security is inherently achieved through IT management, and the responsibility of the IT vendor. The two Venn diagrams below illustrate perception and reality:

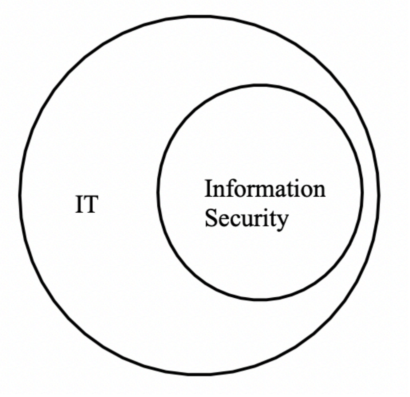

Figure 4 - Perception: Information security position within an organization

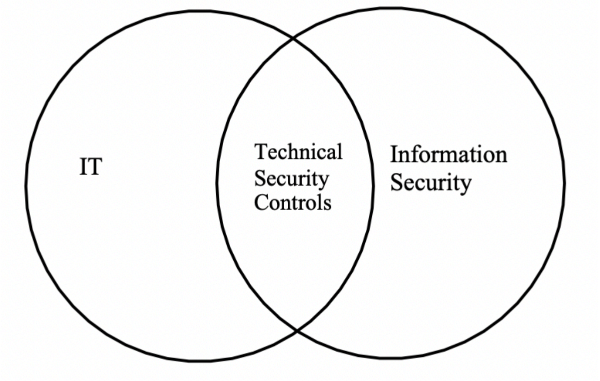

Figure 5 - Reality: Information security position within an organization

Bagwell (Bagwell, 2016) showed small businesses are resource-constrained and do not have the opportunity to dedicate resources to programmatic information security to protect their data and assets, therefore IRPs may see the IT vendor providing information security as a cost-savings and the ability to be proactive about security in the face of resource scarcity.

HIPAA is often discussed in the context of a privacy breach. HHS' OCR maintains a public website of all healthcare industry related privacy breaches over 500 records, a so-called 'wall of shame'. The concept of not sharing personal information with unauthorized individuals is very easy to comprehend. Multiple participants cited related examples when discussing their organizations own security controls. The following exchange highlights the unconscious association with how security and security effectiveness is perceived:

> Interviewer: For the security controls you guys do have in place how effective would you say they are? (PI)
>
> PR6: I hope I'm not jinxing myself, but I think they're very effective we haven't had any type of breach or hack (PR6)

This coupled with the IRPs limited information security knowledge to be aware of the threat landscape suggests they see protecting the confidentiality of patient information as the focus of the HIPAA and their own security program.

Many participants shared their organization had never had a security incident. This indicates a conflict with Hoffman (2015) who published 90% of healthcare providers have suffered a data breach between 2012-2014. This conflict may be in the way participants viewed security incidents. One exchange highlighted this as PR8 shared his organization has never had a breach, but then quickly qualified it:

> Interviewer: How effective do you think your security controls are? (PI)
>
> PR8: I think they're 100% effective. (PR8)
>
> Interviewer: Okay. (PI)
>
> PR8: Never had a breach. (PR8)
>
> Interviewer: Okay. (PI)
>
> PR8: Never had a breach—a reported breach. (PR8)

Participant organizations are willing to invest in security and introduce controls to be compliant or "do whatever it takes to make sure we're secure" (PR6). Multiple participants noted cost was a factor in making information security decisions but would be willing to spend what it takes to be reasonably secure. Highlighted by the "flashlight in a dark room" metaphor, the areas of risk and the threats the participants are aware of have controls implemented to mitigate the risk to perceived acceptable levels. Finding 1 that pointed out that limited knowledge of IT and information security misleads IRP's confidence in their program because for the limited knowledge of risks and controls they are aware of; the IRP's are addressing them. This suggests how they have confidence in their security posture.

A recurring concept heard from multiple participants was the need to outsource IT because of its criticality to the business and the ability for it to be wholly delegated. Participants ranged from business managers, practice administrators, C-level personnel, and managing directors. All participants had responsibilities to their organization that included a diverse range. One participant shared "I handle a lot of different areas it's hard to be an expert in every single area" (PR7).

An overwhelming majority of participants (7/9 or 78%) were not implementing a risk-based security assessment to inform what controls they should be implementing and the risk reduction value. Technical controls appeared selected based solely on IT vendor recommendation.

Two of the participants had transcended from this risk exposure reality and perception misalignment through execution of a security risk assessment activity. This activity informs on risks to the SHPO from relevant threats and security controls to reduce those risks. This activity affects the participants limited IT and information security knowledge and resulted in the implementation of a risk-based security program that is continually monitored and evaluated.

Conclusion

SHPO are interested in being secure and protecting patient information appropriately. The foundational issue with these organizations' approach to information security is the coupling of two issues. First the narrow scope the IRP's identify as the composition of information security. Secondly the SHPO's assumption of outsourcing information security by outsourcing of IT services.

The “flashlight in a dark room” theory was presented to metaphorically explain the phenomenon. Six key findings were presented that were inductively discovered through grounded theory techniques and theoretically saturated from research participants.

A discussion of the findings and their potential implications was provided to help shape the impact and results of these findings.

The following chapter provides the conclusion to the research dissertation. Each finding and the theory itself have warranted conclusions that are logical and clearly explained. Doable and actionable recommendations for SHPOs are provided to address the discovered barriers. Limitations to the research study are provided. Finally, recommendations for future research are suggested.

CHAPTER 5

CONCLUSIONS

Introduction

This research effort has explored information security practices of small healthcare practices. This area of research is very limited, and this study's intent was to qualitatively understand how information security is perceived and approached through the experiences of the responsible individuals operating in this space. Intensive interviewing techniques, informing a grounded theory methodology, fostered the development of a theory explaining how information security is implemented, operated and maintained at these organizations.

This chapter presents conclusions based on the findings and analysis presented in Chapter 4. Recommendations for both policy development and practical actions for these organizations are provided. Several areas of future research are suggested. Limitations to the research are presented to assist in validity and bounding the theory. Finally, given this research was an eighteen-month effort, researcher reflections on the study and its findings are presented.

Conclusions

Responsibility for a function with limited knowledge. The first finding of this research is the limited knowledge in IT and information security that the responsible individual in the practices possesses. These individuals' knowledge base is primarily clinical and business operations.

SHPOs should expect IRPs to become knowledgeable in IT and information security, at minimum from an awareness perspective. Assigning responsibility of a business area to an individual with no knowledge in the area is risky; businesses might not choose to do this if they knew the scope of information security and associated risks. Meanwhile, the IRPs acknowledged their limited knowledge, but were generally uninterested in learning more about information security.

Nevertheless, IRPs must increase their knowledge of IT and information security to better inform the organization across all facets of the information security space. Increasing knowledge expands the concept of security objectives, affects security control selection, and allows the IRP to properly understand the role their IT vendor is providing from an information security perspective and where gaps exist.

IT expertise and information security expertise are not equivalent. The second finding is that SHPOs trust and rely on their IT vendors to have IT knowledge and expertise, and because IRPs associate information security with IT, they assume IT vendors are information security experts.

Many security controls are associated with architecting and configuring IT in a secure manner. This may suggest why IRPs mistakenly assume IT vendors provide for the information security needs of their organization.

IRP's should expect IT vendors to be knowledgeable on IT with respect to functionality that provides some information security capabilities, but should not assume the IT vendors are otherwise information security knowledgeable. For example, an IT vendor should know how to configure a firewall (a network device for controlling data flow into and out of an organizations IT infrastructure), but it must not be assumed the vendor knows how to configure a firewall securely.

Perceptions that IT vendor contracts cover information security. The third finding is that SHPOs assume IT vendors provide comprehensive information security as part of their service offering. IT vendors will unavoidably be engaged in implementation of some security controls for an organization, such as configuring computers to require a username and password for login. This does not mean the security controls are comprehensive, appropriate, or even adding significant risk-reducing value.

IRPs should view information security and IT as separate business aspects. Information security should help inform IT on how to configure security features in technology and to what extent of security to implement. Information security does have entanglements with IT but is not exclusively IT.

Understanding the scope of information security. The fourth finding is the concept that IRPs are thinking of information security with the lens of only one security objective - confidentiality, in compliance with the HIPAA privacy-related regulation.

IRP's must not view information security as a privacy activity. They must understand that the scope of information security includes availability, integrity and confidentiality objectives as reported by Whitman and Mattord (Whitman & Mattord, 2011). Expanding awareness will inform the IRPs about what threats and risks exist and what controls can be implemented to address them.

Desire to implement appropriate security. The fifth finding is the confidence in the effectiveness of participants currently constituted information security programs, and their drive to invest and add controls to reduce any identified risk to acceptable levels. Therefore, the key is to identify the very real risks.

IRPs may be willing to secure their organization if they were aware of evident threats and risks. Indeed, even a brief phone interview about information security, or discussions within professional organizations, might be the catalyst for a deeper threat assessment. Such an activity would metaphorically be "turning on the light switch" in the dark room of risk the IRP is looking at with a flashlight. This conclusion does conflict with Johnson and Koch's (2006) research that suggests if a small business owner knows about a security risk, they are not willing to take action to defend or pay for protection; however, their research was for home-based small businesses and was not focused on healthcare operations.

Outsourcing services will continue. Finally, the sixth finding is the consistency with which SHPOs outsource IT and nominally information security. In fact, they are generally not really outsourcing information security, but believe they are through the IT vendor outsourcing services.

SHPOs should identify that IT and information security are separate business aspects and outsource appropriately. Some IT vendors do provide in-depth information security services as an additional service, but SHPOs must understand when this is additional, and be certain that contract language is clear and meets the SHPO's information security needs.

Regardless of any outsourcing of information security services, SHPOs must ensure they address information security as a critical business function, that includes certain elements (e.g. operational controls) that must be practice-implemented and enforced. Otherwise, IT operations will continue to have potentially significant, unaccounted, and implicitly-accepted risk.

Recommendations

The following recommendations are based on the findings, analysis and conclusions presented in this dissertation. They are presented for two perspectives: policy and practice. Policy is to inform the industry and legislators on making macro changes that may improve the information security effectiveness for SHPOs. Practice recommendations are intended for SHPOs to implement to align risk perception and reality, thus allowing them to have visibility into their organization's information security risk profile.

Policy. Education materials related to implementing appropriate information security at small healthcare practices and designed for audiences with limited IT and information security knowledge should be developed to effectively communicate ways to implement information security. Efforts in early 2019 are already being seen to implement this recommendation. Chua et al. (Chua, 2018) through the Healthcare & Public Health Sector Coordinating Councils produced the "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients" report that provides more accessible language and guidance from previous healthcare industry information security guidance.

Currently the HHS' OCR is tasked with ensuring compliance with both the HIPAA privacy and security rules. This Office audits for compliance and has levied severe monetary penalties (HHS.gov, 2018c). OCR's guidelines for small healthcare practices are vague in this researcher's opinion; OCR should provide clear expectations for compliance with the HIPAA security rule for SHPOs.

Currently OCR has two events that initiate an audit of a SHPO (HHS.gov, 2017a). One is a submission of a SHPO HIPAA non-compliance event to HHS' OCR. The other is a proactive audit conducted by the OCR. The most recent phased activity audit occurred in 2016 and audited less than eight-tenths of 1 percent of healthcare providers in the United States. Reference Appendix E for details on how this value was determined. This indicates that SHPOs that are not involved in a submission and are not involved in the OCR audit have no event that would initiate a review of security control selection with respect to HIPAA requirements. HHS could investigate policy to require healthcare providers to annually submit attestations of foundational security control implementation through a standardized method. This same approach of reporting is implemented for federal agencies annually reporting on Federal Information Security Management Act (FISMA) compliance, a security and privacy standard comparable to HIPAA, to the Office of Management and Budget as required by law (Congress.gov, 2014). This would provide HHS with data points to support rapid audits in the future and provide SHPOs with awareness to the scope of information security controls to consider at their organization, thus addressing the limited IT and information knowledge finding.

Practice. SHPO should seek explicit information security outsourced services to ensure appropriate information security is implemented at the organization, thus assessing actual organizational cyber risk.

A risk-based security program should be adopted to promote purposeful, value-add security control selection for organizations. This will also allow organizations to be aware of their current risks, prioritize risk remediation, and mature their information security program. This recommendation is further supported by an initial observation from 2/9 of the SHPOs in the research study. These two organizations had implemented a risk-based security program and were informed by this approach on the larger scope of information security needs at their organization.

Healthcare organizations should engage their medical malpractice insurance carriers to determine the availably of cyber insurance riders. Two participants mentioned their malpractice provider offered this, but had not added it to their policy.

Limitations

Chapman, Hadfield, and Chapman (Chapman, Hadfield, & Chapman, 2015) point out a demographic-related limitation with qualitative research that applies in this study. The demographic for the research population was constrained to SHPOs with fewer than ten providers in the state of South Carolina, and may not apply to larger practices, or those in other regions or states. In addition, the urban/rural distribution of this research sample may not be otherwise applicable. Five participating SHPOs were from the Charleston, SC area. While the specialties of participating SHPOs were diverse (dermatology, pain management, neurology and general practice), many other specialties were not represented; this is also a constraint of the population demographic. Finally, all participating SHPOs were medical/surgical practices. This excluded other healthcare provider types, including but not limited to psychotherapy, dental, alternative, and tribal.

Sikolia et al. (Sikolia et al., 2013) identifies three techniques to promote interpretive validity of qualitative research. These are participants reviewing and verifying the transcriptions of their interview, participants guiding the direction of the interview, and using participants language and responses in the emerging theory. Research participants limited their ability to commit to participation outside the interview activity. Therefore, participant verification of transcriptions was impossible, a potential research limitation.

The IRB prohibited in-person interviews. All IRPs were interviewed over the phone (audio only, recorded). This prevented any ability to record and analyze physical or non-audio behavior. Such observations are elemental to Maxwell's (Maxwell, 1992) descriptive validity, and their recording and analysis were part of this study's original methods, but could not be done.

Per Price and Murnan (Price & Murnan, 2004), another threat to the internal validity of a study occurs when respondents do not respond truthfully to items on an instrument. However, efforts were taken to encourage participant truthfulness in this research, as documented in chapter 3. Indeed, this researcher believes that the research participants were honest and truthful in their interviews; their responses were certainly "internally consistent." Moreover, it may be that the four "drop-out" IRPs did so because they were troubled about the "truths" they would otherwise share about their SHPO. In any case, this must be included as a potential limitation of the study, that might be mitigated in future research by some external validation of IRP responses.

Another limitation was the participant population size. Nine participant organizations were included in this study. Creswell (2014) suggests 20 participants for a grounded theory study and Charmaz (2006) suggests 25. Charmaz does state in an interview that Glaser, one of the originators of grounded theory, suggested grounded theory could be done with as little as 3 interviews (Gibbs, 2015). This limitation was addressed by adhering to grounded theory methods to achieve theoretical saturation for the developed theory.

Future Research

This research study was exploratory to help cast a light on a specific area of study with minimal literature. Although it was able to answer the question of why SHPOs struggle with information security. The following future research ideas will help inform on this theory's applicability, investigate practices that may address the issues this study introduces, and provide inputs to policy makers.

IT vendor information security knowledge and implemented security controls. There were some identified technical security controls implemented by IT vendors at the SHPOs. Research focused on the knowledge of and actual security controls implemented by the IT vendors could reveal the areas of risk that are commonly addressed by these organizations. This could identify common explicit information security gaps at the SHPOs.

Same study, different state(s). This study was constrained to the state of South Carolina. State specific regulations did not have material effect on the research participants. Participants referenced federal regulations and did not mention state regulations when discussing information security regulations affecting their decisions and businesses. These findings may or may not be generalizable to the small healthcare practices in all states.

Same state, controlled demographics. This study did not discriminate on demographics for the participant organizations. Healthcare providers in rural, suburban, and urban areas may have different priorities, information security attitudes, or resources. Introducing a constraint on the participant demographic may lead to insights into subtle differences or needs for specific healthcare organization types. This can inform policy makers and information security responsible individuals to design and execute tailored reform.

Measure the degree of limited knowledge in IT/ information security. The finding of limited IT and information security knowledge for IRPs was a material finding that underpinned the overall theory. There was no investigation or analysis of the level of their knowledge. A validated instrument to measure the level of knowledge for these IRPs in IT and information security would be appropriate to better understand what "limited" means in this context.

Evaluate IT vendor contracts to assess security language. Another finding of this research was the assumption IRPs make about the scope of work their IT vendors are responsible for executing. The inclusion of information security in this responsibility was sometimes mentioned in the contract, per the participants. An evaluation of contract language of IT vendors that provide IT services to healthcare providers to determine if information security is included, and to what degree.

Researcher reflections

Education is for improving the lives of others and for leaving your community and world better than what you found it.

-Marian Wright Edelman, *The Measure of Our Success, 1992*

This doctoral program was entered with the intention of making an information security related contribution to small businesses. These business types are often marginalized when it comes to research, best practices, and resources compared to their enterprise-sized counterparts. I had no idea when I started this journey the direction it would take. Focusing on healthcare is satisfying because it is an industry that lags among others for information security practices, has a complicated struggle between timely information for clinical decisions and availability, integrity and confidentiality considerations.

Many of the assumptions made at the onset of this research were proven wrong. I am optimistic that the general attitude and passion the participants I spoke with implies that once they 'turn on the light' they will improve their organizations overall information security. While an optimistic notion, perhaps even brief IRP interviews about their practice's information security could be the spark that could start a fire of improving small business healthcare information security in a meaningful way.

I was pleasantly surprised with the interest that participants had in speaking with me about information security at their practice. I found them rather forthcoming. Moreover, it appeared that the interviews led to their increased perception of value in knowing more about information security. Indeed, despite their "status quo" outsourcing of information security to their IT vendors, many participants expressed interest in reading this dissertation upon publication to gain further understanding of how information security is being addressed in their demographics.

I hope this effort serves this community and provides a foundation for future research to be performed given this research's exploratory nature.

REFERENCES

45 CFR § 164.501 - Definitions., (2004).

§ 164.304 Definitions., (2011).

Administration, U. S. F. D. (2016). *Postmarket Management of Cybersecurity in Medical Devices*. Retrieved from https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf

Administration, U. S. F. D. (2018, May 30, 2018). Medical Devices. Retrieved from https://www.fda.gov/MedicalDevices/default.htm

Advocacy, U. S. S. B. A. O. o. (2017). Frequently Asked Questions About Small Businesses. In.

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security, 26*(4), 276-289. doi:http://dx.doi.org/10.1016/j.cose.2006.11.004

Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: current state of research. *International journal of Internet and enterprise management, 6*(4), 279-314.

Assistance, H. C. (2003). Summary of the HIPAA Privacy Rule. In: Office for Civil Rights.

Association, A. H. (2016). Cybersecurity and hospitals. In.

Bagwell, M. A. (2016). *Organizational Decisions about Cyber Security in Small to Mid-Sized Businesses: A Qualitative Study*. Northcentral University,

Barnard, L., & Von Solms, R. (2000). A formalized approach to the effective selection and evaluation of information security controls. *Computers & Security, 19*(2), 185-194.

Barton, K. A., Tejay, G., Lane, M., & Terrell, S. (2016). Information system security commitment: a study of external influences on senior management. *Computers & Security*. doi:http://dx.doi.org/10.1016/j.cose.2016.02.007

Bass, B. (2008). M., The Bass Handbook of Leadership. *Theory, Research & Managerial Applications, 4th edition, New York.*

Berg, S. (2004). Snowball Sampling—I. In *Encyclopedia of Statistical Sciences*: John Wiley & Sons, Inc.

Bhattacharya, D. (2011). Leadership styles and information security in small businesses. *Information Management & Computer Security, 19*(5), 300-312. doi:http://dx.doi.org/10.1108/09685221111188593

Bianchi, A. (2009). An overview of the impact of the American Recovery and Reinvestment Act of 2009 on the HIPAA medical privacy and security rules. *Tax Management Compensation Planning Journal, 37*(9), 227-236.

Birks, M., & Mills, J. (2015). *Grounded theory: A practical guide*: Sage.

Bloomberg, L., & Volpe, M. (2012). Completing Your Qualitative Dissertation. Completing Your Qualitative Dissertation (p. 344). In: Sage Publications, Inc.

Bryant, A., & Charmaz, K. (2007). *The SAGE Handbook of Grounded Theory*: SAGE.

Bryant, M. T. (2003). *The portable dissertation advisor*: Corwin Press.

Chapman, A., Hadfield, M., & Chapman, C. (2015). Qualitative research in healthcare: an introduction to grounded theory using thematic analysis. *Journal of the Royal College of Physicians of Edinburgh, 45*(3), 201-205.

Charmaz, K. (2000). Grounded theory: Objectivist and contructivist

methods. In N. K. D. a. Y. Lincoln (Ed.), *The Handbook of Qualitative Research*. Thousand Oaks, CA: Sage Publications, Inc.

Charmaz, K. (2006). *Constructing grounded theory*: Sage.

Charmaz, K. (2014). *Constructing grounded theory*: Sage.

Chickowski, E. (2010). Protect Your Small Business Against Cyber Attacks.

Chua, J. B., Daniel; Cummings, Allana; Decker, Erik; Finn, David; Nordenberg, Dale; Riethmiller, Erika. (2018). *Health Industry Cybersecurity Practices:*

Managing Threats and Protecting Patients. Retrieved from https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf

Coats, D. (2017). *Worldwide Threat Assessment of the US Intelligence Community*. Retrieved from https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf

Colleges, A. o. A. M. (2017). *2017 State Physician Workforce Data Report*. Retrieved from https://store.aamc.org/downloadable/download/sample/sample_id/30/

Collins, J. D. (2007). Toothless HIPAA: Searching for a private right of action to remedy privacy rule violations. *Vand. L. Rev., 60*, 199.

Congress.gov. (2014). S.2521 - Federal Information Security Modernization Act of 2014. Retrieved from https://www.congress.gov/bill/113th-congress/senate-bill/2521

Cresswell, J., & Miller, D. (2000). Getting good qualitative data to improve. *Theory into practice, 39*(3), 124-130.

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches*: Sage publications.

Crotty, M. (1998). *The foundations of social research: Meaning and perspective in the research process*: Sage.

Davis, J. (2017, 2017-03-20). Ransomware rising, but where are all the breach reports? Retrieved from http://www.healthcareitnews.com/news/ransomware-rising-where-are-all-breach-reports

DHS. (2017a). Healthcare and Public Health Sector | Homeland Security. Retrieved from https://www.dhs.gov/healthcare-public-health-sector

DHS. (2017b). What Is Critical Infrastructure? | Homeland Security. Retrieved from https://www.dhs.gov/what-critical-infrastructure

Dixon, B. E., Zafar, A., & McGowan, J. J. (2007). Development of a taxonomy for health information technology.

Eilon, S. (1969). WHAT IS A DECISION? *Management Science (pre-1986), 16*(4), 18.

Evaluators, I. S. (2016). *Securing Hospitals: A research study and blueprint*. Retrieved from www.securityevaluators.com

Fernando, J. I., & Dawson, L. L. (2009). The health information system security threat lifecycle: An informatics theory. *International Journal of Medical Informatics, 78*(12), 815-826. doi:http://dx.doi.org/10.1016/j.ijmedinf.2009.08.006

FORCE, H. C. I. C. T. (2017). *REPORT ON IMPROVING CYBERSECURITY IN THE HEALTH CARE INDUSTRY*. Public Health Emergency Retrieved from https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf

Francis, A., Xiaohong, Y., Jinsheng, X., & Hong, W. (2013). A Survey of Security Standards Applicable to Health Information Systems. *International Journal of Information Security and Privacy (IJISP), 4*(7), 22-36. doi:10.4018/ijisp.2013100103

Gibbs, G. (Producer). (2015, January 25, 2019). A Discussion with Prof Kathy Charmaz on Grounded Theory. Retrieved from https://www.youtube.com/watch?v=D5AHmHQS6WQ

Glaser, B. G. (1978). *Theoretical sensitivity: Advances in the methodology of grounded theory*: Sociology Pr.

Glaser, B. G. (1998). *Doing grounded theory: Issues and discussions*: Sociology Press.

Glaser, B. G. a. S., A.L. (1967). *Discovery of grounded theory: Strategies for qualitative research*. New York: Aldine.

Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The qualitative report, 8*(4), 597-606.

Goldzweig, C., Towfigh, A., Maglione, M., & Shekelle, P. G. (2009). Costs And Benefits Of Health Information Technology: New Trends From The Literature. *Health Affairs, 28*(2), w282-w293. doi:10.1377/hlthaff.28.2.w282

Gostin, L. O., Lazzarini, Z., Neslund, V. S., & Osterholm, M. T. (1996). The public health information infrastructure: a national review of the law on health information privacy. *JAMA, 275*(24), 1921-1927.

Green, L. A., Potworowski, G., Day, A., May-Gentile, R., Vibbert, D., Maki, B., & Kiesel, L. (2015). Sustaining "Meaningful Use" of Health Information Technology in Low-Resource Practices. *Annals of Family Medicine, 13*(1), 17-22. doi:10.1370/afm.1740

Guba, E. G. (1981). Criteria for assessing the trustworthiness of naturalistic inquiries. *ECTJ, 29*(2), 75.

Halamka, J. D., & Tripathi, M. (2017). The HITECH era in retrospect. *New England Journal of Medicine, 377*(10), 907-909.

Health Information Technology for Economic and

Clinical Health Act, 201, Pub. L. No. 111–5 § 13400 Definitions, 123 Stat. (2009 February 17, 2009).

HealthcareInfoSecurity.com. (2017). Assessing the ISMG Healthcare Security Summit. *Healthcare Information Security Podcast*.

HealthIT.gov. (2012). *Meaningful Use Tables for November 01, 2012*. Healthit.gov Retrieved from https://www.healthit.gov/sites/default/files/meaningfulusetablesseries1_110112.pdf

HealthIt.gov. (2018). Adoption of Electronic Health Record Systems among U.S. Non-Federal Acute Care Hospitals: 2008-2015.

Hegwer, L. R. (2017). Managing Cybersecurity Threats. *hfm (Healthcare Financial Management), 71*(2), 1-4.

Herold, R., & Beaver, K. (2004). *The practical guide to HIPAA privacy and security compliance*: CRC Press.

HHS.gov. (2013, July 26, 2013). Breach Notification Rule. Retrieved from https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

HHS.gov. (2017a). How OCR Enforces the HIPAA Privacy & Security Rules. Retrieved from https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/how-ocr-enforces-the-hipaa-privacy-and-security-rules/index.html

HHS.gov. (2017b, May 12, 2017). The Security Rule. Retrieved from https://www.hhs.gov/hipaa/for-professionals/security/index.html

HHS.gov. (2018a). Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information. Retrieved from https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

HHS.gov. (2018b). Enforcement Results by Year | HHS.gov.

HHS.gov. (2018c). Resolution Agreements and Civil Money Penalties. Retrieved from https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html

HIMSS. (2015). *2015 HIMSS CyberSecurity Survey: Executive Summary*. Retrieved from http://s3.amazonaws.com/rdcms-himss/files/production/public/FileDownloads/2015-cybersecurity-executive-summary.pdf

HIPAA History. (2017). *HIPAA Journal*.

Hoffman, K. E. (2015). NOT IF, BUT WHEN. *Medical Marketing and Media, 50*(12), 40-41.

Holtzman, D. (2017). OCR Says Desk Audits Rates Many HIPAA Efforts to be Inadequate or Worse.

House, T. W. (2013). Presidential Policy Directive -- Critical Infrastructure Security and Resilience.

Huberman, A., & Miles, M. (2002). *The Qualitative Researcher's Companion*. doi:10.4135/9781412986274

Initiative, N. J. T. F. T. (2011). Managing Information Security Risk: Organization, Mission, and Information System View. *NIST Special Publication*, 800-839.

Institute, P. (2016). State of Healthcare Cybersecurity Study.

Institute, P. (2017). *2017 State of Cybersecurity in Small & Medium-Sized Businesses*. Retrieved from

Johnson, D. W., & Koch, H. (2006, 04-07 Jan. 2006). *Computer Security Risks in the Internet Era: Are Small Business Owners Aware and Proactive?* Paper presented at the Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06).

Jones, S. S., Rudin, R. S., Perry, T., & Shekelle, P. G. (2014). Health information technology: An updated systematic review with a focus on meaningful use. *Annals of Internal Medicine, 160*(1), 48-54. doi:10.7326/M13-1531

Kane, C. (2017). *Policy Research Perspectives*. Retrieved from

Kaplan, A. (1964). The Conduct of Inquiry: Methodology for Behavioral Sciences. San Francesco: Chandler.

Kissel, R. (2013). NIST IR 7298 Revision 2: Glossary of Key Information Security Terms. *National Institute of Standards and Technology. May. Accessed July, 7*, 2013.

Kotz, D. (2011). *A threat taxonomy for mHealth privacy.* Paper presented at the Communication Systems and Networks (COMSNETS), 2011 Third International Conference on.

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

L. Strauss, A., & Corbin, J. (1998). *Basics of Qualitative Research : Techniques and Procedures for Developing Grounded Theory*: Sage Publications.

Lakshmi, S., & Mohideen, M. A. (2013). ISSUES IN RELIABILITYAND VALIDITY OF RESEARCH. *International Journal of Management Research and Reviews, 3*(4), 2752-2758.

Landry, J. P., Pardue, J. H., Johnsten, T., Campbell, M., & Patidar, P. (2011). *A Threat Tree for Health Information Security and Privacy.* Paper presented at the AMCIS.

Lempert, L. B. (2007). Asking Questions of the Data: Memo Writing in the Grounded. *The Sage handbook of grounded theory*, 245-264.

Locke, L. F., Spirduso, W. W., & Silverman, S. J. (2014). *Proposals that work*: Sage.

Luna, R., Rhine, E., Myhra, M., Sullivan, R., & Kruse, C. S. (2016). Cyber threats to health information systems: A systematic review. *Technology & Health Care, 24*(1), 1-9. doi:10.3233/THC-151102

Mandiant. (2016). M-Trends 2016.

Marshall, C., & Rossman, G. B. (2014). *Designing qualitative research*: Sage publications.

Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: how safe are we? *Bmj, 358*, j3179.

Maxwell, J. (1992). Understanding and validity in qualitative research. *Harvard educational review, 62*(3), 279-301.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. *The Academy of Management Review, 20*(3), 709-734. doi:10.2307/258792

McCallin, A. M. (2003). Designing a grounded theory study: Some practicalities. *Nursing in critical care, 8*(5), 203-208.

McGee, M. K. (2014). HIPAA Audits: Round 2 Details Revealed. Retrieved from https://www.healthcareinfosecurity.com/hipaa-audits-round-2-details-revealed-a-6747

Millman, R. (2016). Ransomware holds data hostage in two German hospitals.

Morgan, D. L. (1996). Focus groups. *Annual review of sociology, 22*(1), 129-152.

NIST, S. (2004). 800-37. *Guide for the Security Certification and Accreditation of Federal Information Systems*.

NIST, S. (2010). 800-37, Revision 1. *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, 16*.

NIST, S. (2012). 800-30 Revision 1. *Risk Management Guide for Information Technology Systems (September 2012): http://csrc. nist. gov/publications/nistpubs/800-30-rev1/sp800_30_r1. pdf.*

O'Brien, D., Budish, R., Faris, R., Gasser, U., & Lin, T. (2016). Privacy and Cybersecurity Research Briefing.

Otero, A. R., Otero, C. E., & Qureshi, A. (2010). A multi-criteria evaluation of information security controls using Boolean features. *International Journal of Network Security & Its Applications (IJNSA), 2*(4).

Paul Proctor, K. T., Earl Perkins, Khushbu Pratap. (2016). *Best Practices in Implementing the NIST Cybersecurity Framework*. Retrieved from Gartner: https://www.gartner.com/document/3188133?ref=solrAll&refval=191179207&qid=7521d247e4481716f90ac38d4af1fa70

Peltier, T. R. (2005). *Information security risk analysis*: CRC press.

Price, J. H., & Murnan, J. (2004). Research limitations and the necessity of reporting them. In: Taylor & Francis Group.

Rohn, E., Rohn, E., Sabari, G., Sabari, G., Leshem, G., & Leshem, G. (2016). Explaining small business InfoSec posture using social theories. *Information & Computer Security, 24*(5), 534-556.

Ross, R. (2013). NIST SP 800-53, Revision 4. *Security and Privacy Controls for Federal Information Systems and Organizations*.

Samy, G. N., Ahmad, R., & Ismail, Z. (2009, 18-20 Aug. 2009). *Threats to Health Information Security.* Paper presented at the Information Assurance and Security, 2009. IAS '09. Fifth International Conference on.

Saunders, M., Lewis, P., & Thornhill, A. (2009). Research methods for business students.

SBA. (2018). Size Standards Tool | The U.S. Small Business Administration | SBA.gov. Retrieved from https://www.sba.gov/tools/size-standards-tool?ms=nid4060

SC Code of Laws - Title 39 - Chapter 1 - General Provisions. (2018). Retrieved from https://www.scstatehouse.gov/code/t39c001.php

SCDHEC. (2019). Health Care Preparedness Staff Contacts – State and Local. Retrieved from https://www.scdhec.gov/health-professionals/emergency-preparedness/get-help-health-care-system-preparedness/health-care-0

Schatzman, L., & Strauss, A. L. (1973). *Field research: Strategies for a natural sociology*: Prentice Hall.

Schoew, J. (2018). LOSING THE CYBERSECURITY CULTURE WAR [Accenture consluting healthcare division]. Retrieved from https://www.accenture.com/us-en/blogs/blogs-losing-cybersecurity-culture-war

Section 160.103. Definitions, (2013).

Shekelle, P., Morton, S. C., & Keeler, E. B. (2006). Costs and benefits of health information technology.

Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. *Education for information, 22*(2), 63-75.

Sikolia, D., Biros, D., Mason, M., & Weiser, M. (2013). Trustworthiness of grounded theory methodology research in information systems.

Smith, K. G., Smith, K. A., Olian, J. D., Sims, H. P., O'Bannon, D. P., & Scully, J. A. (1994). Top Management Team Demography and Process: The Role of Social Integration and Communication. *Administrative Science Quarterly, 39*(3), 412-438. doi:10.2307/2393297

Smith, M. (2017). Cyber attacks cost U.S. enterprises $1.3 million on average in 2017 | CSO Online.

Smithson, J. (2000). Using and analysing focus groups: limitations and possibilities. *International journal of social research methodology, 3*(2), 103-119.

Strauss, A. L. (1987). *Qualitative analysis for social scientists*: Cambridge University Press.

Sultan, N. (2014). Making use of cloud computing for healthcare provision: Opportunities and challenges. *International Journal of Information Management, 34*(2), 177-184.

Symantec. (2017). Internet Security Threat Report.

Tarouco, L. M. R., Bertholdo, L. M., Granville, L. Z., Arbiza, L. M. R., Carbone, F., Marotta, M., & de Santanna, J. J. C. (2012). *Internet of Things in healthcare: Interoperatibility and security issues.* Paper presented at the Communications (ICC), 2012 IEEE International Conference on.

Van Ommen, B. (2014). IT Security in SMEs: Necessary or Irrelevant?

Verizon. (2018). *Protected Health Information Data Breach Report*. Retrieved from http://www.verizonenterprise.com/resources/protected_health_information_data_breach_report_en_xg.pdf

Whitman, M. E., & Mattord, H. J. (2011). *Principles of information security*: Cengage Learning.

APPENDIX A: DEFINITIONS

The following terms are used throughout this report. Their definitions are provided and sourced. Appropriate definitions have been selected from healthcare and cybersecurity literature and regulations to align to the research and literature contained within this document.

Breach

(A) IN GENERAL. The term 'breach' means the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

(B) EXCEPTIONS. The term 'breach' does not include—

(i) Any unintentional acquisition, access, or use of protected health information by an employee or individual acting under the authority of a covered entity or business associate if—

(1) Such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the covered entity or business associate; and

(2) Such information is not further acquired, accessed, used, or disclosed by any person;

(ii) Any inadvertent disclosure from an individual who is otherwise authorized to access protected health information at a facility operated by a covered entity or business associate to another similarly situated individual at same facility; and

(iii) Any such information received as a result of such disclosure is not further acquired, accessed, used, or disclosed without authorization by any person. ("HITECH Act," 2009)

Business Associate

Business associate: (1) Except as provided in paragraph (4) of this definition, business associate means, with respect to a covered entity, a person who: (i) On behalf of such covered entity or of an organized health care arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or (ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in §164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person. ("Section 160.103. Definitions," 2013)

Covered Entity

Covered entity means: (1) A health plan. (2) A health care clearinghouse. (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter. ("Section 160.103. Definitions," 2013)

Disclosure

The release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.("Section 160.103. Definitions," 2013)

Electronic Health Record

The term ‘‘electronic health record’’ means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff. ("HITECH Act," 2009)

Healthcare Operations

Health care operations means any of the following activities of the covered entity to the extent that the activities are related to covered functions: (1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment; (2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities; (3) Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of §164.514(g) are met, if applicable; (4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs; (5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and (6) Business management and general administrative activities of the entity, including, but not limited to: (i) Management activities relating to implementation of and compliance with the requirements of this subchapter; (ii) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer. (iii) Resolution of internal grievances; (iv) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and (v) Consistent with the applicable requirements of §164.514, creating deidentified health information or a limited data set, and fundraising for the benefit of the covered entity.("45 CFR § 164.501 - Definitions.," 2004)

Protected Health Information

Individually identifiable health information: (1) Except as provided in paragraph (2) of this definition, that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium. (2) Protected health information excludes individually identifiable health information: (i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) In records described at 20 U.S.C. 1232g(a)(4)(B)(iv); (iii) In employment records held by a covered entity in its role as employer; (iv) Regarding a person who has been deceased for more than 50 years. ("HITECH Act," 2009)

Individually identifiable health information

Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual. ("HITECH Act," 2009)

Security or Security Measures

All of the administrative, physical, and technical safeguards in an information system. ("§ 164.304 Definitions.," 2011)

Health care Provider

The term 'health care provider' includes a hospital, skilled nursing facility, nursing facility, home health entity or other long term care facility, health care clinic, community mental health center (as defined in section 1913(b)(1)), renal dialysis facility, blood center, ambulatory surgical center described in section 1833(i) of the Social Security Act, emergency medical services provider, Federally qualified health center, group practice, a pharmacist, a pharmacy, a laboratory, a physician (as defined in section 1861(r) of the Social Security Act), a practitioner (as described in section 1842(b)(18)(C) of the Social Security Act), a provider operated by, or under contract with, the Indian Health Service or by an Indian tribe (as defined in the Indian Self-Determination and Education Assistance Act), tribal organization, or urban Indian organization (as defined in section 4 of the Indian Health Care Improvement Act), a rural health clinic, a covered entity under section 340B, an ambulatory surgical center described in section 1833(i) of the Social Security Act, a therapist (as defined in section 1848(k)(3)(B)(iii) of the Social Security Act), and any other category of health care facility, entity, practitioner, or clinician determined appropriate by the Secretary.("HITECH Act," 2009)

Threat

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. (Kissel, 2013)

Information Security

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.(Kissel, 2013)

Incident

A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. (Kissel, 2013)

Vulnerability

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. (Kissel, 2013)

Cyber Attack

An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. (Kissel, 2013)

APPENDIX B: INTERVIEW PROTOCOL

This document provides guidance on the agenda used to facilitate interviews for research associated with South Carolina, Small Healthcare Provider Organization Cybersecurity Program Decision Processes. Structure of interview and nature of question is based on Charmaz 2006, “Constructing Grounded Theory” (Charmaz, 2006). The following preamble is spoken by the researcher to the participant prior to asking any questions.

Preamble

Each interview will begin with my preamble to introduce myself, establish purpose of the interview and affirm confidentiality. The preamble is:

> Thank you for your time and speaking with me. I am a doctoral candidate. I currently work at the Medical University of South Carolina, researching small business healthcare cybersecurity decision processes. I would like to talk in generalities to get an understanding of the types of security issues you may face. I do not want to know explicitly if your company has had a successful breach or experienced a successful cyber-attack.
>
> The information provided will remain strictly confidential and you will not be identified by your answers. You and your company’s name will not be disclosed in any way. Data will be compiled with no individual responses tied to your name or any identifying information about you. I would like to record this interview. All information disclosed during our conversation will be kept in a secure location. You may choose not to answer any question. Do you have any questions before we get started? Are you willing to participate?

I will begin recording this interview session now.

Ice Breaker Questions

1. Please tell me about yourself and how long you have worked at [company]
2. How did you come to be involved in information security at [company]
3. Please describe the organization structure at [company].
4. Please describe your cyber security related responsibilities at [company].

Information Security Program Questions

1. Describe the process and procedures related to cyber security at [company]
2. Describe the culture or attitude relative to security and privacy?
3. What is the overall approach for cyber risk management?
4. Describe how decisions related to cyber security are made? For example, HIPAA regulations come out or the decision to invest in some type of security related technology (cyber insurance, anti-virus software, etc).
5. Can you describe your beliefs toward healthcare cybersecurity regulation?
6. Can you describe your thoughts on cyber security as a responsibility at [company]?
7. When working with vendors (i.e. cloud solutions), how does cyber security factor into the discussion and evaluation?
8. Without detail of an actual experienced cyber related attack, How has any experienced cyber security related events such as a virus-infected computer, a stolen laptop with patient data, or faxing to a wrong number, affected change at [company]?
9. How has your information security budget been changing over the past couple of years?
10. Describe your primary concerns from a cyber security standpoint?
11. What do you see as the biggest cyber threats for companies like yours?

12. How do you identify which threats are most important and prioritize accordingly?
13. How effective are your security controls? How do you know this?
14. Describe how end user experience factors into cybersecurity decisions?
15. What factor is most important in driving cybersecurity investment: cost reduction, compliance obligations, perceived risk reduction, general process improvement, or something else? Please elaborate.
16. Are you involved with information security related budgeting decisions? When evaluating about information security spending decisions, describe the process for making those decisions, including if evidence or metrics used in making cyber investment decisions.
17. Describe your thoughts on the information you have and use in managing overall cyber risk and prioritizing accordingly?
18. Describe your thoughts on how cybersecurity is supported and decided here?
19. Can you describe how cybersecurity and the decisions made about cybersecurity have changed over time?
20. What outside organizations have helped you in making cybersecurity decisions?
    a. How did they get involved with your organization (sought out, vendor sales, post breach, insurance provider, conference)?

Ending Questions

1. What do you think are the most important ways to make cybersecurity decisions for small healthcare businesses?
2. Is there anything else you think I should know to understand how cybersecurity is managed and how decisions about it are made at your organization?

3. Is there anything that you might not have thought about before that occurred to you during this interview?
4. Is there anything you'd like to ask me?

Interview Probes to Clarify and Elicit More Information

1. Could you clarify what you meant about ____?
2. How does ____ relate to ___?
3. How often does ____happen?
4. Where?
5. When?
6. Who is involved?
7. Is that always the same situation or have you ever experienced it to be different?
8. Was that the unusual?
9. Was that exceptional?
10. That's something I haven't heard before, could you explain more about _______?
11. Do you know other people who may experience that from a different perspective?
12. How did you come to know this?
13. Please go on _________. I'd like to know more about that, please explain

APPENDIX C: IRB APPROVAL

APPROVAL:

This is to certify that the research proposal **Pro00079974** entitled:

South Carolina, Small Healthcare Provider Cybersecurity Program Decision Processing: A Grounded Theory Study

and submitted by: **Gerald Auger**

Department: **Medical University of South Carolina**

For consideration has been reviewed by **IRB-II - Medical University of South Carolina** and approved with respect to the study of human subjects as adequately protecting the rights and welfare of the individuals involved, employing adequately methods of securing informed consent from these individuals and not involving undue risk in the light of potential benefits to be derived therefrom. Additionally, the Institutional Review Board for Human Research (IRB) recommends approval of the investigator's request for Waiver of Signed Consent in accordance with 45 CFR 46.117(c)(1),(2) because the only record linking the subject and the research would be the consent document and the principal risk would be potential harm resulting from a breach of confidentiality and/or because the research presents no more than minimal risk and involves no procedures for which written consent is normally required outside of the research context.. No IRB member who has a conflicting interest was involved in the review or approval of this study, except to provide information as requested by the IRB.

Original Approval Date: **7/19/2018**

Approval Expiration: **7/18/2019**

Type: **Expedited**

Chairman, **IRB-II - Medical University of South Carolina**

Susan Sonne, PharmD*

Statement of Principal Investigator:

As previously signed and certified, I understand that approval of this research involving human subjects is contingent upon my agreement:

1. To report to the Institutional Review Board for Human Research (IRB) any adverse events or research related injuries which might occur in relation to the human research. I have read and will comply with IRB reporting requirements for adverse events.
2. To submit in writing for prior IRB approval any alterations to the plan of human research.
3. To submit timely continuing review reports of this research as requested by the IRB.
4. To maintain copies of all pertinent information related to the research activities in this project, including copies of informed consent agreements obtained from all participants.
5. To notify the IRB immediately upon the termination of this project, and/or the departure of the principal investigator from this Institution and the project.

***** ***Electronic Signature**: This document has been electronically signed by the IRB Chairman through the HSSC eIRB Submission System authorizing IRB approval for this study as described in this letter.*

APPENDIX D: CODING AND CATEGORIES

Table 5 - Coding inventory

Index	Name
1	Trust IT vendor with Security
2	Trust IT vendor with Security (NOT)
3	Reliant on Vendor
4	Reliant on Vendor (NOT)
5	above and beyond HIPAA
6	accepting and supportive of HIPAA
7	accepting certification as secure
8	Access controls
9	adopting EMR relative to compliance
10	adopting EMR relative to financial motivations
11	adopting technology slowly
12	assessing end user population as very careful
13	assessing paper records as low value asset
14	assuming no breach
15	availability as a security objective in practice
16	be as secure as possible
17	belief that security should be high quality
18	believes no security incidents
19	believing business is HIPAA compliant

Index	Name
20	breach of patient data is the impact
21	budget increased by cyber security
22	budget unaffected by cyber security
23	cautious about agreeing to requirements for cyber insurance
24	challenging to keep up with protecting as technology evolves
25	cloud solutions more secure because absensce of physical threats
26	collaborating with IT vendor on decisions
27	concern of HIPAA violation
28	concern of ownership of a breach
29	concerned with record retention and disposal
30	concerning about financial impacts
31	concerning about threats that can stop business
32	concerning about threats that damage reputation
33	confidence in production technology being secure
34	confidentiality as a security objective in practice

Index	Name
35	conflicting priorities at the business
36	constraining challenges of small business
37	controls are reactive in nature
38	coorelating restituion from contract breach as financial
39	cyber insurance certainly worth it from a cost benefit ratio
40	deferring and accepting of vendor security standards
41	discussing attempted breaches
42	dont take cyber security threats as serious until you've experienced it
43	educating end users
44	encrypting email
45	end user convenience is a factor in security decisions
46	end user convenience is not a factor in security decisions
47	enforcing security program
48	equating moving to EMR with information security needs
49	equating size of staff with necessity of control scope
50	erring on caution when complying with HIPAA

Index	Name
51	executing DR/BCP scenarios
52	factoring cost of cyber security decisions
53	factoring risk reduction in cyber security decisions
54	Fearing lack of control for external threats
55	functionality over securty
56	generational factors into secure use of technology
57	hackers as a threat
58	hardware as an asset
59	HIPAA scope seen as privacy
60	holding staff accountable for compliance
61	I wouldn’t really be looking at other metrics or data, it would just be is this the right time to go ahead and start working on this insurance policy.
62	identifies program security as appropriate
63	implementing improvements to security based on lessons learned
64	implementing security to comply with legislation

Index	Name
65	income to medical practices has gone down
66	insider threat
67	integrity as a security objective.
68	interacting with IT for break/fix mostly
69	IT and security vendor
70	IT budget explicit contains security
71	IT budget implicit contains security
72	key quote
73	knowing area of weakness but not addressing
74	lack of compliance oversight leads to responsbile person's interpretation of whats best practice
75	lack of security compliance due to change resistance
76	lack of security compliance due to understanding
77	low IT knowledge
78	maintaining current systems
79	medications and writing prescriptions as an asset
80	meh HIPAA
81	money well spent
82	needing to have basic awareness and education on regulations and good understanding of information sharing

Index	Name
83	not considering vendor security practices during selection
84	patient care is impact
85	patient quality of life is the impact
86	patient trust impact
87	patients information as an asset
88	practicing proactive security
89	previous incidents awareness have impacted workflows
90	protecting from environmental threats with business continuity
91	putting patients at risk
92	questioning the effectiveness of HIPAA due to lack of enforcement
93	receiving regular update reporting
94	reliant on experts
95	remote access security designed and implemented
96	reputation as an asset
97	review security
98	risk-based security program
99	security as a continuous process
100	security decision making requires competency
101	security decision making requires tech savvy person

Index	Name
102	security is taken seriously
103	security not a consideration for business until an issue (Reactive)
104	security staff information as an asset
105	security too hard to keep up to date and be an expert on
106	securty as a burden
107	seeing ransomware as a threat
108	seeing security and privacy as different concepts
109	seeing security as IT only
110	seeing size of practice as a benefit to low costing security (meh)
111	seeking complete security
112	seeking security expertise for program maturity
113	self aware of security knowledge gaps
114	self aware of security program maturity level
115	sensitive information destruction practice
116	small business has small footprint of patient information
117	staff have too much on their plate for security

Index	Name
118	staff information as an asset
119	staying engaged with security
120	strong passwords
121	technology needed to be efficient and competitive
122	texting PHI a concern
123	thinking of security as privacy
124	too small a business for more controls
125	too small a business to be a target
126	transferring perceived responsibility
127	trusting vendor
128	try to do what the best practices are
129	validating security controls work
130	vendor selection through trusted referral
131	verifying vendor security before selection
132	view on cyber security hasnt changed over time because havent seen anything (reactive)
133	we stay on the cutting edge of technology
134	wishing for compliance oversight
135	workforce security conscious
136	working directly with IT company

Table 6 - Category inventory

Index	Category
1	ASSETS
2	Confidence in Security Program
3	FINANCIAL RELATED
4	Healthcare Cyber Regulation
5	IMPACTS
6	Knowing but not Doing
7	Negative Security
8	OUTLIER CODES
9	Privacy as the full scope of Security
10	PROACTIVE SECURITY
11	REACTIVE SECURITY - Changing security from lessons learned
12	REACTIVE SECURITY - Seeing no reason to change current security
13	THREATS - External threats
14	THREATS - Internal threats
15	Vendor Trust - Blind Trust
16	Vendor Trust - Explicit Functionality, Assumed Security
17	Vendor Trust - Reliance

APPENDIX E: CALCULATING HHS AUDIT SCOPE

Table 7- Calculating HHS OCR phase 2 audit scope

765,117	Number of physicians in the United States as of November 2017(Colleges, 2017)
57.8%	57.8% of physicians work in practices with 10 or fewer physicians (Kane, 2017)
442,238	Total number of physicians in the United States that work in a practice with fewer than 10 physicians. Formula: (.578 * 765,115)
44,224	Assuming all practices with fewer than 10 physicians all have 10 physicians, therefore the maximum number of practices with 10 or fewer physicians (i.e. SHPOs). Formula: (442,238 / 10)
1	Fewest number of practices for all physicians that are in practices with more than 10 physicians.
350	Number of audited covered entities that were audited for Phase 2 audit protocol per interview with HHS OCR (McGee, 2014)
0.79%	The likelihood of being selected for an HHS OCR Phase 2 Audit Protocol. Formula: (350/(44,224 + 1))

APPENDIX F: DATA SUMMARY TABLE

Table 8 - Data summary crosswalk

Participant	Limited IT Knowledge	Risk-based program	Security seen as Privacy	Trust IT vendor with Security	Reliant on Vendor	Risk Analysis performed(s)	Confidence in Sec Program	Support for HIPAA	Strong support for being secure / compliant
3	no - think for us it is having someone who is a little bit more tech savvy, who knows more about computers than just logging on and logging into a system and using it; knowing the background, knowing how the basics of a computer system work, and how VPN and how your IP address can be vulnerable and how things can happen. You need someone who understand that to be able to make those decisions	yes- "It is part of the conversation with the IT provider when we go through our reports quarterly to look at risk, potential risk. Or if something was not catching spam or if it was seeing someone trying to infiltrate our system then we would change it. Our risk percentage would then go up and we would have to look at new options."	no- other assets "with cyber security it's always someone hacking into our EMR system to get patient information, hacking into my bank accounts"	yes- "So I work directly with our IT company who handles our cyber security as well"	yes- "I rely on my IT company to give me my metrics and my risk factor, and that is what will decide whether I'm going to change or upgrade to a different product or security. It's going to all depend on my risk factors."	yes- "It is part of the conversation with the IT provider when we go through our reports quarterly to look at risk, potential risk."	yes- " I mean, your security should be topnotch. You're handling patients' information which has not only their social security numbers but it has medications" "So as long as my risk stays at a low percentage—we're talking less than a 5% chance of being hacked into or someone getting into our system"	yes-"o I think it's very important not only HIPAA—I mean, HIPAA's also important"	yes-"So as long as my risk stays at a low percentage—we're talking less than a 5% chance of being hacked into or someone getting into our system—we tend to leave things the way they are. " "

Participant	Limited IT Knowledge	Risk-based program	Security seen as Privacy	Trust IT vendor with Security	Reliant on Vendor	Risk Analysis performed(s)	Confidence in Sec Program	Support for HIPAA	Strong support for being secure / compliant
5	yes- I kind of put that trust in there that they were going to follow through with whatever the standard for information technology and security and just trust that was there to start with, for me personally I don’t know the specifics and ins and outs that would be done on a technical level. So I wasn’t really interested in asking those questions to make comparisons, for me it was more about the product itself.	no-	yes- " I think we recognize that the patients information and security of that is obviously very important. So we take some steps to minimize potential, I guess, misuse of that information or accidently letting that information get out to the public."	yes- "Did they seem legitimate company, it wasn’t something a little bit shady and I had questions, so I kind of put that trust in there that they were going to follow through with whatever the standard for information technology and security and just trust that was there to start with, for me personally I don’t know the specifics and ins and outs that would be done on a technical level."	yes- " I’m sort of at the mercy how well or how poor they are going to do their job"	no- seems on cusp though "they do offer an additional cyber security policy which I’ve talked to them a little bit about recently but to get that done I’ve looked at the requirements which I need we have to make some concrete protocols and have a few more things written down"	yes- "I would say they(sec controls) are good, they have been effective and are currently effective the way we are using them but certainly need to be reviewed and improved upon."	yes- "I think HIPAA and everything that follows along with that, obviously it plays a very important role. I think for the most part everything seems to be done obvious with good intention"	yes- "Really one is it’s the right decisions to make assuming you believe personal health information should be private and protected well that’s the right decision"

Participant	Limited IT Knowledge	Risk-based program	Security seen as Privacy	Trust IT vendor with Security	Reliant on Vendor	Risk Analysis performed(s)	Confidence in Sec Program	Support for HIPAA	Strong support for being secure / compliant
6	yes- Well with me I'm the managing partner of course just working with our IT firm that handles our IT part of our business and it's mostly just working with them to ensure we are secure as we can be and that they're safeguarding all of our information, its not too technical what I do, I lean a good bit on our IT firm to make those decisions	no-	no- availability "The main we one we had this last time we do use the cloud for backup we also use backup hard drives too at two different locations or when hurricanes come in inclement weather and something maybe destroyed we have the capability of taking those to a secure place"	yes- IT vendor; "Again the IT firm handles that so I trust them" "it's just a working relationship with the IT firm having confidence in them that they are up-to-date on current practices and best practices. So we stay ahead of any kind of security risk"	yes- "the only thing you can do rely on the experts the people who who work in this field"	no-	yes- always been HIPAA compliant	yes-	yes- "we always have to be compliant no matter what" "we have the attitude we want to be as secure and as private as we can"

Participant	Limited IT Knowledge	Risk-based program	Security seen as Privacy	Trust IT vendor with Security	Reliant on Vendor	Risk Analysis performed(s)	Confidence in Sec Program	Support for HIPAA	Strong support for being secure / compliant
7	yes-" I rely a lot on my IT vendor I have a good relationship and trust him to be able to help me understand. My background is certainly not in IT"	no-	yes- "for me the cyber security part of it is so interconnected with protecting PHI and complying with HIPAA and all that stuff."	yes-"talking to my IT person, he doesn’t understand the billing part of it, or a lot of the HIPAA part of it, but he does understand the cyber security part"	yes-" I rely a lot on my IT vendor I have a good relationship and trust him to be able to help me understand. My background is certainly not in IT"	no- does do 'mini-risk assessments' when making decisions, but not really security risk analysis.	no- "cyber gets kicked to the side unfortunately" "I think your questions were pretty thorough but I guess just just like the perspective to you know at the end of the day it all kind of comes back to budgeting and the financial resources too. I’m lucky enough to work in a dermatology group that has been very successful but there’s not a whole lot of independent practices left particularly with certain specialties. Derm seems to be excluded from some of those threats they don’t have the resources to just function as they are much less worry about things like that if that makes sense like there are so many practices that go under because they have some sort of Medicare lawsuit or they just can’t pay their staff or they are not able to purchase an EHR and participate in that and they keep getting the reimbursement cut	no- "Okay I personally don’t have a problem with that I think I understand it and I understand why and I understand the risk but I think it goes back to what I was saying before about how it changes it involves so much it’s not just IT it’s I think IT in general information security and all that technology it touches so many different areas it’s hard to I guess keep up with it wrap my arms around it it’s not just it affects HIPAA it affects that , it affects my financials, it effects my patients, it affects the staff there’s just a lot of if that changes a lot and keeping up"	no- "I’ll tell you my doctors are more worried about malpractice suits then cyber security all day long you know that’s been ingrained in their brain from day one about making appropriate clinical decision and minimizing your risk there and avoiding a malpractice lawsuit from a patient or referring doctor or anything else they are worried about that kind of security and financial security not necessarily the cyber security and I just think it hasn’t been on the forefront of anybody’s brain for a long time in this industry"

Participant	Limited IT Knowledge	Risk-based program	Security seen as Privacy	Trust IT vendor with Security	Reliant on Vendor	Risk Analysis performed(s)	Confidence in Sec Program	Support for HIPAA	Strong support for being secure / compliant
							and I think they're so worried about all these other things that there is enough time or resources or room to worry about cyber security until all those other foundational things are stable. I think it kind it goes back to psychology class I took a while ago where are you know you don't have a roof over your head and food to eat you're not really worried about some of those other things until you are stable yeah want you get a roof over your head and you have enough to eat then you can worry about all these other things and I'm not saying that cyber security is smaller but in the grand scheme of things if you can't pay yourself and your staff that's a bigger problem then if information is getting compromised so I think it is kind have to work through that in order to and that health care is so tumultuous right now and changing		

Participant	Limited IT Knowledge	Risk-based program	Security seen as Privacy	Trust IT vendor with Security	Reliant on Vendor	Risk Analysis performed(s)	Confidence in Sec Program	Support for HIPAA	Strong support for being secure / compliant
							so much and it’s getting harder and harder to practice independently that they never get to a point to worry about cyber security they either collapse and fold their practice or they get bought out buy a big system that already has that stuff in place so they never get to the point where they can actively think about it I guess my role with the derm office I’m lucky to work in a place that is stable financially and doesn’t have they are starting to feel some issues with reimbursement but they are stable enough that I need to worry about are we going to make payroll next time or anything like that that I can start to think about those things. that’s the only other thing I’d say about that is that that’s the big reason why it’s not a priority is that there are a lot of other things I guess more financially related and regulatory related that they are already behind the		

Participant	Limited IT Knowledge	Risk-based program	Security seen as Privacy	Trust IT vendor with Security	Reliant on Vendor	Risk Analysis performed(s)	Confidence in Sec Program	Support for HIPAA	Strong support for being secure / compliant
							curve with technology and then they're always worried about these other things hey what's the new law that passes or a new regulation, or is everything else we have to worry about that cyber security gets kicked to the side unfortunately."		

Participant	**Limited IT Knowledge**	**Risk-based program**	**Security seen as Privacy**	**Trust IT vendor with Security**	**Reliant on Vendor**	**Risk Analysis performed(s)**	**Confidence in Sec Program**	**Support for HIPAA**	**Strong support for being secure / compliant**
8	yes - I'm 65 years old, or soon to be 65 within about three months. I'm not electronically very savvy. When I was in high school, people that were taking keyboarding weren't going to college, they were going into some other field. And computer labs in the colleges were just one or two courses. So it certainly would have probably slowed me down considerably in patient care trying to learn all that.	no-	yes- "I think it's something we talk about but we think more about clinical care than we do about security because it's pretty automatic. It's hard—one chart, one patient in a private room. And we're very—we are very careful. We don't mention any names of other people that we see. We're very careful about that." "I don't know if you call that security or not, but inability to access patient records I think that's a type of security problem" "~~Roper should have a better backup system to prevent loss of availability; i have paper records that are susceptible to fire and flood,	no- doesn't use vendor or EMR	no- doesn't use vendor or EMR	no-"I don't—guess what you could call—we have cyber security. We use strictly paper records and they are kept very confidential, very secure, locked in a set of record locks as well as behind a separate locked office door, as well as locked behind a general office door every day. "	yes- "I don't—guess what you could call—we have cyber security. We use strictly paper records and they are kept very confidential, very secure, locked in a set of record locks as well as behind a separate locked office door, as well as locked behind a general office door every day. " Interviewer: How effective do you think your security controls are? Interviewee: I think they're 100% effective.	no- "I think HIPAA has utility. It's minimal. It also has some drawbacks" "I don't think HIPAA's necessarily a bad thing"	no- "I don't think there's a whole lot of value for a thief or someone who's compiling information to break into three locks and carry out pounds and pounds of paper information. I don't think it's worth it to them! "

Participant	Limited IT Knowledge	Risk-based program	Security seen as Privacy	Trust IT vendor with Security	Reliant on Vendor	Risk Analysis performed(s)	Confidence in Sec Program	Support for HIPAA	Strong support for being secure / compliant
			but its in God's hands"						

Participant	Limited IT Knowledge	Risk-based program	Security seen as Privacy	Trust IT vendor with Security	Reliant on Vendor	Risk Analysis performed(s)	Confidence in Sec Program	Support for HIPAA	Strong support for being secure / compliant
9	yes- I’m not an IT professional!	yes- "Well, through those annual health or security assessments we identify certain elements that may/could use some attention, or new equipment, or, you know, say there are some inactive users that, you know, we haven’t deactivated. So we go through just a full assessment of all of our equipment and try and assess what is susceptible and shore that up. " "I generally rely on my IT guy here that I really trust. I usually ask him, if he suggests a particular mitigation strategy, to give me a couple of vendors and the pluses and minuses of both as well as the cost of each, and then we move forward based on that information"	no- "Well, you know, we have annual training—cyber security, HIPAA, OSHA, all of that—through our compliance program. We have forced password rules, you know, to update passwords. We’ve recently wanted employees to use phrases not, you know the typical passwords. So we’re instituting that. All of the employees are told not to share passwords. We have, you know, a handbook that lists all of those requirements for good stewardship of data, and new employees are oriented with those policies as well." "all cyber security, especially,	no- "I observe this gentleman every day in his interaction with the employees. You know, I think when he gives me updates or things that he identifies during his time here they generally have been right on. I keep up with, you know—every now and then I’ll read newsletters just enough to be dangerous and get scared with the cyber security and all of the breaches that are out there. And he always—if I ask him a question about them he can tell me what really occurred and why, you know, we need to be cognizant of it and if we are subject or susceptible to any of those attacks that have been successful. You know, it’s hard to put your finger on it, but sometimes you can just talk to somebody and just realize that they know what they’re doing."	yes- "I generally rely on my IT guy here that I really trust. I usually ask him, if he suggests a particular mitigation strategy, to give me a couple of vendors and the pluses and minuses of both as well as the cost of each, and then we move forward based on that information."	yes- "through those annual health or security assessments we identify certain elements that may/could use some attention, or new equipment, or, you know, say there are some inactive users that, you know, we haven’t deactivated. So we go through just a full assessment of all of our equipment and try and assess what is susceptible and shore that up. So, you know, we have those discussions with myself, my deputy—my administrative assistant—and the head of the IT security, and then we develop a timeframe to—you know, if something is obviously a red threat level we act on it immediately."	yes- "our mission states that, you know, we’re going to do everything we can to secure data."	yes- "it’s very important, obviously. The HIPAA rule has been around for quite some time and we drill, drill, drill how important it is to secure information and how privacy of our patients’ health conditions is crucial. "	The HIPAA rule has been around for quite some time and we drill, drill, drill how important it is to secure information and how privacy of our patients’ health conditions is crucial. And that’s not only in personal communications, which is kind of what we’ve drilled down and made sure that people understand, but it’s also in your technical communications and making our employees aware that, hey, you know, don’t walk away from your screen. You know, log off when you leave. You know, you wouldn’t want, if it was your information, up for people to casually see. You know, just trying to put yourself in the mindset of the patient, and just an overall culture of that. yes- "And, you know, we’ve had people that have

Participant	Limited IT Knowledge	Risk-based program	Security seen as Privacy	Trust IT vendor with Security	Reliant on Vendor	Risk Analysis performed(s)	Confidence in Sec Program	Support for HIPAA	Strong support for being secure / compliant
			you know, with healthcare many breaches occurring throughout the country with large hospital systems and, you know, ransomware and various things. We just want to do—we want to be ahead of the curve and try and make it as difficult for someone that might eye our organization as possible to affect us negatively. So, I mean, it’s a little bit of yes, the internal assessment certainly, but also, you know, it’s just looking at the landscape of cyber security in society and trying to beef it up as best we can for a small organization."						not taken that directive as serious as we would like and those people have been disciplined. We have very little tolerance for that type of behavior because, you know, if your patients can’t trust you with their sensitive information that’s a very big hurdle to overcome. So it’s just ingrained in our culture from the day that people are oriented how important it is to be good stewards of the data that we have."

Participant	Limited IT Knowledge	Risk-based program	Security seen as Privacy	Trust IT vendor with Security	Reliant on Vendor	Risk Analysis performed(s)	Confidence in Sec Program	Support for HIPAA	Strong support for being secure / compliant
10	no	yes- "So the way we do it is we kind of set up a system where we have different tasks involved and first you try and adjust your risks, which includes the vulnerability, the threats, and the risk itself. So you want to look at the scope of the analysis, your data collection. You identify any potential documents—documented potential threats and vulnerabilities. You want to assess the current security measures, determine the likelihood that the threat may occur, determine the level of the risk itself, finalize your documentation, and then plan to periodically review and update your risk assessment. " "for the cyber-related security	no- "So it’s my job to make sure that access to the IT is always safeguarded. So I’m the one that keeps control of the keys to the server room—because right now we have a server because we’ve been server-based for fourteen years but, as I mentioned, we’re going to cloud-based. We use an external IT company that monitors everything. I monitor the arm and disarm reports for the alarm system to make sure that no one’s coming in and going out. I monitor the employees by inactivating them, you know, the minute that they might leave our employ. I monitor difference uses. I keep	no- "if there’s new technologies out there then we’re going to fit them into our budget for business operations and make sure that you’re protecting everything that you need. And you really have to do a lot of evaluation. You have to reach out to different resources. Certainly your IT company should be able to provide you with a lot of that."	no- "if there’s new technologies out there then we’re going to fit them into our budget for business operations and make sure that you’re protecting everything that you need. And you really have to do a lot of evaluation. You have to reach out to different resources. Certainly your IT company should be able to provide you with a lot of that."	yes- "So the way we do it is we kind of set up a system where we have different tasks involved and first you try and adjust your risks, which includes the vulnerability, the threats, and the risk itself. So you want to look at the scope of the analysis, your data collection. You identify any potential documents—documented potential threats and vulnerabilities. You want to assess the current security measures, determine the likelihood that the threat may occur, determine the level of the risk itself, finalize your documentation, and then plan to periodically review and update your risk assessment. " " I also do the	yes- "I think the hacker’s probably our biggest threat. I mean, I know that our facility is secure and I’m not worried about that. A hurricane is a hurricane. They’re unpredictable and we certainly have protocols in place."	yes- "Nobody comes by from HIPAA. There are no HIPAA police. they’re far understaffed. And the reason why is because people don’t take cyber security threats as serious as they should until you’ve experienced it, and then once you’ve experienced it or you’ve really sat down to consider—do you know how many office managers that are out there that don’t know what a security risk analysis is? "	yes- "Nobody comes by from HIPAA. There are no HIPAA police. they’re far understaffed. And the reason why is because people don’t take cyber security threats as serious as they should until you’ve experienced it, and then once you’ve experienced it or you’ve really sat down to consider—do you know how many office managers that are out there that don’t know what a security risk analysis is? " "I went to a doctor’s office on a visit with a family member and I was, you know, appalled at how loosely things were operated" "For us cyber security was the Number 1 element because the functionality of the current EMR we use is certainly not the best. I mean, it’s more incumbent. It’s a little

Participant	Limited IT Knowledge	Risk-based program	Security seen as Privacy	Trust IT vendor with Security	Reliant on Vendor	Risk Analysis performed(s)	Confidence in Sec Program	Support for HIPAA	Strong support for being secure / compliant
		we do a security risk analysis every year. We evaluate the environment. We evaluate the demographics, what threats might be proposed. Like we live in the South, so there's a great threat of hurricanes and that kind of stuff. So we always have to go to an emergency preparedness plan in terms of our technology, because we rely solely on technology. "	control and lockdown on most of the external websites. I continuously communicate to staff regarding, you know, different types of spam and what we don't want them to open and if they think something's suspect how we want it handled. And we educate the staff annually on HIPAA regulations. "			security risk analysis for the IT system on an annual basis and do all the compliance for, you know, HIPAA and all EMR facilitation"			harder, and we know that there are other programs out there that are maybe more user friendly, but they don't provide the protection and privacy that the EMR we use does. So for us we are more concerned with protecting the integrity of the data than we are of end user use." "You go through a process of what is reasonable within your budget. And, you know, you do hear me refer to the budget because it can get expensive. But, you know, it's money well spent if you're following what's required of you. I mean, in our industry your data's got to be authenticated. You've got to know that what's being put in there is actually what happened. So we try and make sure that our risk analysis process

Participant	Limited IT Knowledge	Risk-based program	Security seen as Privacy	Trust IT vendor with Security	Reliant on Vendor	Risk Analysis performed(s)	Confidence in Sec Program	Support for HIPAA	Strong support for being secure / compliant
									is ongoing and that we're—you know, if there's new technologies out there then we're going to fit them into our budget for business operations and make sure that you're protecting everything that you need"

Participant	Limited IT Knowledge	Risk-based program	Security seen as Privacy	Trust IT vendor with Security	Reliant on Vendor	Risk Analysis performed(s)	Confidence in Sec Program	Support for HIPAA	Strong support for being secure / compliant
12	yes- I’m personally not trained in technology, so I would literally have to, you know, rely on others’ suggestions and then not just jump on it right away but do some research of my own before we just go ahead and move forward with something different for our office, for our practice here.	no-	yes- Well, when it comes to like for our business, yeah, I think it’s important that you keep everybody’s records safe, you know. Because you think about it. Not only the medical history is on there. You have people’s social security on there. You have, you know, addresses and phone numbers and—you know, definitely it’s for the safety of our patients, you know. and that in my eyes is the priority. It’s our first priority is to keep our patients’ information safe. it’s amazing to me because I’m really not very familiar with all the hyper, you know, technology	yes - No, I mean, just overall, you know, being in this field it’s what you hear, you know, and how to be, you know, on the lookout and protecting your patients and stuff like that. so, you know, we had to go with somebody, and then of course you hear about the [REDACTED] people. but, you know, other than that it’s not like we hear a lot about cyber security, you know. We just know personally that we have to be careful with our patients’ information, you know, so how we’re going to protect and now what is the best way to do it and who do we trust, who can we trust? And of course we, you know, met with [REDACTED] and we heard good things about them and we liked them and we’ve had this relationship with	yes- I’m personally not trained in technology, so I would literally have to, you know, rely on others’ suggestions and then not just jump on it right away but do some research of my own before we just go ahead and move forward with something different for our office, for our practice here. So that’s what I worry about. That’s my responsibility here in the office: to make sure that things run smoothly within the office. When it comes to technology and cyber security I have to—because I’m not familiar with it I have to rely on companies like [REDACTED]and [REDACTED] that they’re doing their job.	no- a MIPS based risk analysis on the EMR is performed by the EMR hosting provider for the org as a client. No risk analysis on the organization is performed.	yes - Now, if the computers are running slow or if we feel like somebody hacked, that’s when, you know, we start thinking about oh, shoot, something’s happening, you know, we need to get in touch with our IT department or, you know, cyber, you know, security and stuff like that. But we don’t really—it’s not something that we think about. Now, maybe because we’re confident that we are safe. Although you can never be too safe, I guess, you know.	no - I’m not saying it’s not effective. I mean, it’s effective. It’s been working out. I mean, from—again I’ve been here for a year. I mean, it works out. You know, it’s okay. you know, it’s what is there now. There’s always going to be adjustments. I think it’s been a great start of it, I guess, I don’t know.	yes-

Participant	Limited IT Knowledge	Risk-based program	Security seen as Privacy	Trust IT vendor with Security	Reliant on Vendor	Risk Analysis performed(s)	Confidence in Sec Program	Support for HIPAA	Strong support for being secure / compliant
			especially, as much as it has grown, that we have to be careful with, you know. So then of course, you know, you go around and you have to do—I talk to the staff here and make sure that they're at the same—we're all at the same level, you know, with confidentiality when it comes to, you know, Google searching to patient information to sharing information and everything else.	them now for a long time. So it kind of fell in like that. Right. Yeah, so anyway, so there's a lot of things. So that's—you know, when it comes to cyber security we rely on [REDACTED] and [REDACTED].					

Participant	Limited IT Knowledge	Risk-based program	Security seen as Privacy	Trust IT vendor with Security	Reliant on Vendor	Risk Analysis performed(s)	Confidence in Sec Program	Support for HIPAA	Strong support for being secure / compliant
14	yes - I defer a lot to them because I'm not an IT person, they are, and I rely on them to make sure that everything is secure.	no-	yes- I mean, we're not a corporation where we're hiding any, you know, secret plans as far as like what we've built or, you know, patented information or anything like that. our information that's very private to us is that of our patients.	yes- A lot of that comes over again from IT, you know. And we've been working with the same IT group for, gosh, almost ten years and go with their recommendations of what we need. You know, and then of course we look at costs and all of that and if it's over a certain threshold we go to our board of directors, you know, to sign off on that purchase.	yes- I defer a lot to our IT department. I mean, like I said, they monitor, they make sure that they check and run for viruses or breachments in our system, which we haven't had any. I defer a lot to them because I'm not an IT person, they are, and I rely on them to make sure that everything is secure.	no- Okay. So as a practice there what's the overall approach to cyber risk management? interviewee: The overall approach—I don't know exactly— Interviewer: How do you guys manage your cyber risk there? Interviewee: Cyber security—you know, we have downloaded onto our system, so that's checking on a regular daily basis.	yes- I think maybe after our conversation with you and you helping to educate me a little more I could better answer that question. But as it stands now I feel pretty secure.	no - Well, I don't have bad thoughts about regulations. I think it's important. I think it's necessary. You know, I don't want my information of my children's information, you know, out there for everyone to access, so I think it's important. I think like anything else I think you can go overboard with regulations and some of it be unnecessary and cost money and time that's unnecessary, but at the same time I think what we have in place right now that's required of us is sufficient. I'm sure there's room for improvement in places for that but it's important.	yes- Absolutely, yes. And we take it very seriously. We want to be able to make sure that, you know, their identity is kept confidential, they trust in us.... So it's important to me and my team that we keep everything in the strictest of confidence.