A DELPHI STUDY OF COUNTERMEASURES TO SECURITY THREATS IN NETWORKED MEDICAL DEVICES

by

Melinda Lyles

TIMOTHY SHIMEALL, Ph.D, Faculty Mentor and Chair

AHMAD MOSTAFA, Ph.D, Committee Member

VU TRAN, Ed.D, Committee Member

Todd Wilson, Ph.D, Dean, School of Business and Technology

A Dissertation Presented in Partial

Fulfillment

Of the Requirements for the Degree

Doctor of Information Technology

Capella University

March 2020

Abstract

The purpose of this qualitative Delphi study was to come to a consensus on measure to improve the security of medical devices using the theory of reasoned action (TRA). The researcher explored the underlying basic motivation of information technology (IT) experts' urges to perform an action and create a model for developing effective countermeasures for cyber threats to networked medical devices in the healthcare industry in the United States. The researcher conducted this study in reaction to the growing need for security countermeasures supporting the technology in the healthcare industry, which aligns with the risks related to networked medical devices. The study included 15 IT experts who validated relevant experiences with employing a schema to analyze security risks in networked medical devices. The researcher conducted semi-structured interviews in multiple rounds and reached data saturation in the third round. IT experts had experiences with different types of networked medical devices at different hospitals and therefore had varying experiences. This model can be used as the forefront of guidance in support of networked medical devices to ensure security threats and vulnerabilities are minimized. The findings for this research could provide users a tool for preventing a security breach through networked medical devices. IT leaders in the healthcare industry, including networked medical device manufacturers, could use the model to enhance procedures in order to ensure the security of the device from cyber threats and minimize risks related to its use, especially when connected to a network medical device. The findings from this study could provide a possible capability to give awareness to IT support and healthcare organizations within the United States that support networked medical devices. This study may also contribute to the automation of alerting the appropriate personnel as a way to reduce risk with networked medical devices and mitigate cyberattacks. In addition, the model may also be helpful to scholars who are

focusing on how to increase efficiency in terms of identifying areas of risk where more methods are needed.

Dedication

This research is dedicated to family and friends who each play a role in achieving my educational goals. This subject was dedicated to my father, as we have been through many trials and tribulations with his health leading up to having depended on technology to regulate his heart and keep him with us to enjoy him as long as we can. Thank you to my mother for always being my cheerleader encouraging me throughout my educational endeavors and never giving up on me even when I wanted to give up on myself. My son Matthew Ball for always asking me what my grades are and how school was each and every day; he always tells me how proud he is of me and I love you to infinity and beyond. I also dedicate this work to other family and friends, Dave my brother who listens to me when I get discouraged; Jennifer and Ajith Mathew's, Donte Blackwell, Misty Ball, and Wensdy and Ray Maldanado who have always supported my dreams and educational goals, no matter how wild and high they may be. Finally, a mentor of my career, friend, and United States Public Health Service brother, Craig Hodge, without you I would not be where I am today in my adult life, I thank you for all the support that cannot be measured in value.

Acknowledgments

I would like to acknowledge my mentor, Timothy Shimeall, Ph.D, for his all his support toward encouraging me throughout my journey turning all discouraging into encouraging moments. My committee members Ahmad Mostafa, Ph.D and Vu Tran, Ed.D who provided valuable input throughout this program. I would also like to acknowledge all cohorts who supported me through this journey and who provided constant encouragement and support to pursue my personal goals.

Table of Contents

List of Tables

List of Figures

CHAPTER 1. INTRODUCTION

Introduction

As technology continues to develop, more medical devices connect to networks for faster communication and to take advantage of the benefits of the Internet (Ransford et al., 2017; Williams & Woodward, 2015). Medical devices are an emerging concern by patients, physicians, and information technology personnel in the United States (Middaugh, 2016). With the growing sophistication of hackers' skills, cyber threats continue to evolve that affect networked medical devices (Ransford et al., 2017). Possible gaps in security could all attackers to harm and corrupt the care of a patient, impose identity theft of personal information, and expose other system vulnerabilities (Ransford et al., 2017).

The topic of this study was cybersecurity threats impacting networked medical devices. Previous research by scholars and practitioners in the field of cybersecurity provided further discussion and research on the topic of networked medical devices and connectivity with healthcare systems (Gantz, Philpott, & Windham, 2013; Ransford et al., 2017; Williams & Woodward, 2015). Identifying controls are essential to risk management when implementing a more secure posture for devices and systems (Lam & Wong, 2018). This researcher conducted a Delphi study with experts in determined the enhancement of defense mechanisms through a threat risk assessment. In this study, the results provided support for the development of a model to include effective countermeasures for cyber threats with networked medical devices based on experiences and perceptions of Information Technology (IT) experts. Thus, using enhanced attacks, such as spoofing identity, tampering with data, repudiation, Information disclosure, denial of service, elevation of privilege STRIDE threat model, and the Confidentiality, Integrity,

Availability (CIA) triad, were implemented as a guided policy to apply security governance in an healthcare organizations.

The purpose of Chapter 1 is to explain purpose of the supportive factors of the intended study. Security threats drew attention to networked medical devices that created a vulnerable state causing exposure and potential danger in information security within the healthcare industry. For preventing compromises to systems, patients, and networked medical devices, different threat models and security frameworks were evaluated that could be used as countermeasures to prevent compromises (Cerkovnik, 2015; Olendorf, 2015; Seale, 2017; Stine, Rice, Dunlap, & Pecarina, 2017). The problem of interest for this research is the vulnerabilities in networked medical devices and how the countermeasures could ensure the safety and security with the protection with patient care and exposed healthcare systems. The rest of the sections in Chapter 1 relate to the problem of interest justifying a need for this study. The different sections of Chapter 1 include the following: (a) background of the study, (b) the statement of the need for the study, (c) the purpose and significance of the study, (d) the research design, (e) the research question, (f) the assumptions and limitations of the study, and (g) definitions of terms used in the study.

Background

Dimensional Research (2016) surveyed 338 Information Technology (IT) and security professionals in different industries within the United States; 27% of the healthcare industry players did not use a security framework and 73% adopted a security framework. The Dimensional Research survey reported that 12% of organizations in the healthcare industry within the United States used the Cybersecurity Framework (CSF), which is a National Institute of Standards and Technology (NIST) framework for improving critical infrastructure for

cybersecurity. The CSF is a NIST (2018) framework that encompassed security controls that organizations can employ to form an information security program protecting users, infrastructure, and assets managed by the organization, which included those from the healthcare sector. With the increase in delivering remote healthcare, networked medical devices were implemented to support the management of patient care through an adaptive risk-based schema to assess the current state of the system (Rao, Carreon, Lysecky, & Rozenbilt, 2017).

Researchers conducted studies to evaluate the impact of security failure on networked medical devices (Assante & Lee, 2015; Schwartz et al., 2018). Assante and Lee discussed the kill chain control within cyber security based on an attacker's objectives. The researchers used the risk scoring system to define the assets that were being protected, with the scores indicating level of risk for devices that could pose a threat to patient safety. This allows defenders to focus on the most exposed devices among those critical to safety. Seale, McDonald, Glisson, Pardue, and Jacobs (2018) found healthcare environments were continuously attacked. The attacks revealed that manufacturers often only acted to preserve trust and accountability only in reaction to report attacks (Seale et al., 2018). According to the United States Food & Drug Administration (FDA) (U. S. Food & Drug Administration, 2019b), there were 2,282 known issues reported in the Manufacturer and User Facility Device Experience Database (MAUDE) in U. S. Food & Drug Administration 2017 related to networked medical devices that led to code causing problems that harmed the patient or reflected insufficient required care. The FDA would not accept the risk and is not required to approve all software updates (Schwartz et al., 2018). Therefore, when a failure impacts a patient with a networked medical device due to a malicious attack, unsecure code, or a faulty appliance, the healthcare provider is held responsible for those actions according to the regulations in place by FDA.

Threats in networked medical devices within healthcare organizations led to security breaches of sensitive data on the privacy of medical information (Das et al., 2018; McNally, Frey, & Crossan, 2017). In a survey conducted about the cybersecurity, Filkins and Wright (2017) discovered that the healthcare industry was among the top five industries that use data protection and is a common target of cyberattacks. Furthermore, the Ponemon Institute (2017) conducted a survey and discovered 67% of medical device manufacturers and 56% of healthcare organizations indicated a malicious attack on a medical device would likely occur within the next 12 months. According to the Ponemon Institute's survey, one-third of device makers and healthcare organizations are aware of potential effects to patients due to the lack of device security resulting in a decrease or increase in the medical treatment and impacted therapy that was being provided. As a result, 17% of device makers or manufacturers and 15% of the healthcare organizations took preventative measures against the attacks.

Medical devices that exposed patients to threats were managed through standard risk management processes that were reported by users and practitioners' reporting in the MAUVE which notifies manufacturers (Weininger, Jaffe, & Goldman, 2017). Risk exposed to organizational networks led to emerging issues following the expansion of the system between networked devices and clinical operations. With security risks to networked medical devices, safety measures can be readily penetrated, leaving devices and networks at a vulnerable state that could have led to unauthorized personnel managing the devices with malicious intent (William & Woodward, 2015). According to FDA, risk management should be assessed throughout the lifecycle of any device by manufacturers. Therefore, regulators should require manufacturers should be required to provide recurring updates more frequently instead of waiting for reports of defects in medical device used by patients for medical therapy. The U. S. Food & Drug

Administration (2018d) maintains a surveillance tool called the Manufacturer and User Facility Devices Experience (MAUDE) database that tracks issues associated with recalled devices and includes risk assessments. The database classified these issues according to the risk to the patient.

This study utilized a Delphi method to support the development of a model for effective countermeasures for cyber threats with networked medical devices based on experiences and IT experts' perceptions. Overall, researchers who studied the use of networked medical devices in healthcare highlighted the importance and use of a cybersecurity framework as a countermeasure to prevent attackers from exploiting patients and other networks (Cerkovnik, 2015; Seale, 2017). Cerkovnik created a proof of concept database that was not peer-reviewed that used the classification of medical devices, defined the vulnerabilities and threats, aligned a score based on risks examining medical devices that were reported to the FDA due to failures and potentially exposing various points of the network. Seale expanded on the database created by Cerknovnik to assess risk models to indicate cybersecurity vulnerabilities within network devices using real-world de-identified data.

In this study, the focus was on the importance of developing a model of cybersecurity based on experiences and perceptions of IT experts that work with networked medical devices. Frameworks were the basis of the schemas used in analyzing security risks in networked medical devices. For this study, more commonly, schema is a structured format or model used to organize data. A schema refers to "a network of subschemata, where each of which carries out its assigned task of evaluating its goodness of fit whenever activated" (Rumelhart, 2017, p. 33).

Business Technical Problem

In the United States, over 300,000 patients had embedded networked medical devices, and were at risk, with life-threatening situations, dependent on such devices (Ankarali, Abbasi, Demir, Serpedin, Qaraqe, & Arslan, 2014). The general problem is the vulnerability of networked medical devices to cyberattacks (Ankaraili et al., 2018; Pycroft & Aziz, 2018; Ransford et al., 2017). Approximately 94% of healthcare organizations were victims of cyberattacks on medical devices and the infrastructure to support these devices (William & Woodward, 2015).

The specific problem addressed in this study was the lack of basis for developing effective countermeasures for cyber threats to networked medical devices leading to high possibility of security breaches (Pycroft & Aziz, 2018; Ransford et al., 2017). Failures of networked medical devices could potentially result in fatal events (Pycroft & Aziz, 2018; Ransford et al., 2017). Ransford et al. found cases where patients with a network medical harmed when exposed to risk concerning security vulnerabilities. These devices may have been affected by cyberattacks, such as altering code, which electronically controls delivery of care (i.e., telehealth), battery failure, and migration problems (Pycroft & Aziz, 2018). Cybersecurity vulnerabilities are detrimental to the safe operation of networked medical devices, as they compromise the patient treatment and safety more than personally identifiable information. In this study, the researcher addressed risks related to the exposure of networked medical devices to cyberattacks and identified security controls to confidentiality, integrity, and availability. The security posture with networked medical devices are of concern due to the serious effects of exploiting vulnerabilities. The researcher used the CIA Triad as the security model that represented each attribute of security (i.e., confidentiality, integrity, and availability) that was

used to evaluate policy within organizational assessment (NIST, 2018). STRIDE is a threat model to indicate threats within categories such as spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privileges (ISACA, 2017). Together, STRIDE and CIA Triad are security models used to determine how to reduce and improve patient safety for population with networked medical devices. Therefore, these models were the basis for the researcher's exploration and assessment of the problem of the study and to help identify threats to networked medical devices.

Research Purpose

The purpose of this qualitative Delphi study was to support the development of a model for effective countermeasures to protect against cyber threats with networked medical devices based on the experiences and perceptions of IT experts in the healthcare industry in the United States. There was an increase in security risk factors in networked medical devices and a lack of risk assessment found in two nonpeer-reviewed study's (Cerkovnik, 2015; Seale, 2017). According to Jorm (2015), Delphi research is used when developing a model in order to find a solution to an issue or a problem. Therefore, the purpose of this study was aligned with Delphi research. The target population of this study was IT experts in the field of healthcare. Specifically, through a Delphi approach, the researcher collected data from 15 cybersecurity IT experts in the industry of healthcare who were working with networked medical devices. The researcher conducted interviews in multiple rounds, which according to Delphi research was the optimal number of times interviews are conducted to reach a desired consensus (Birko, Dove, & Özdemir, 2015; Ozier, 2012).

Research Question

For this Delphi study, the researcher created the following main research question to support the development of a model of effective countermeasures for cyber threats with networked medical devices based on the experiences and perceptions of IT experts in the healthcare industry in the United States:

What are the relevant expériences in employing a schema to analyze security risks in networked medical devices?

Rationale

Past research using peer-review or nonpeer-review study's related to identifying countermeasures used to protect networked medical devices focused on creating a database to support healthcare industry to monitor and evaluate vulnerabilities in these types of devices (Cerkovnik, 2015; Chow, Sanghani, & Morris, 2017; Seale, 2017). Multiple researchers discovered that measuring risks to medical devices proactively by placing compensating control could potentially to protect against exposure (Cerkovnik, 2015; Chow et al., 2017; Seale, 2017). Other researchers in a nonpeer-review study attempted to determine if threats to the network medical devices traced assets would decrease if vulnerabilities, software exposure, and other cyber threats were controlled (Cerkovnik, 2015; Seale, 2017).

Over the past several years, many articles were published on network medical devices, cyber threats exposing the patients, networks, and information (Ankarali et al., 2014; Hwang, Sokolov, Franklin, & Kesselheim, 2016). Many researchers had identified only by providing guidance that had addressed leaving responsibility and accountability vague (Khera, 2017; Olendorf, 2015). These researchers found problems with increased connectivity between networked medical devices and clinical medical system networks (MSNs) allowing for access by

unauthorized individuals with underlying malicious intents (Ankarali et al., 2014; Hwang et al., 2016; William & Woodward, 2015). Moreover, the researchers focused on network medical devices while evaluating scenarios with specific devices that would support the previously presented cybersecurity frameworks.

Mandating a mechanism for accountability to improve assessing lifecycle based on a monitoring structure for managing cyber threats reduces the risk to the patient and healthcare provider with security, malfunctioning, or malicious exposures (Ankarali et al., 2014). Ankarali et al. found that risk management should be addressed throughout the lifecycle of the device. While scholars acknowledge the security risks related to using network medical devices, there was a gap in the literature regarding the development of a model for effective countermeasures for cyber threats with networked medical devices. Therefore, there was a need for a study that aims to support the development of a model for effective countermeasures for cyber threats with networked medical devices based on experiences and perceptions of Information Technology (IT) experts in the healthcare industry in the United. This model can be helpful to practitioners in terms of avoiding gaps in protection from cyberattacks. Moreover, the model may also be helpful to scholars by means of increasing efficiency in terms of identifying areas of risk where more methods are needed.

Theoretical Framework

Healthcare organizations have been treating patients with medical devices to support quality of life. Manufacturers are responsible for providing the practitioner, user, and assisting healthcare organization with software updates, according to U. S. Food & Drug Administration (2019a). Olendorf (2015) indicated healthcare organizations managed the device affiliated with protecting patients' safety and the system it was connected to. The theory used for this study was

the theory of reasoned action (TRA). Dulany (1968) developed the TRA and Ajzen and Fishbein (1980) further developed the theory. The authors based the TRA on social psychological components of intended behaviors and explains that behavior results from an individual's intended behavior (Ajzen & Fishbein, 1980). Based on TRA, a person's behavioral intention was jointly determined by the person's attitude and the subjective norm concerning the behavior in question. Attitude refers to a person's mannerisms in relation to a behavior and the act of performing the behavior with limited regard to the overall performance (Ajzen & Fishbein, 1980). Subjective norm is based on the opinions of others and consists of a person's decision to perform or not to perform a specific behavior (Ajzen & Fishbein, 1980). The TRA provided a framework or basis for analyzing how a person responds to a particular situation (Ajzen & Fishbein, 1980). Therefore, in this study, the researcher used the elements of TRA as the basis for understanding IT experts' behavior, attitude, and perceived control with regard to intentions of how to implement cybersecurity and providing preventive measures with networked medical devices.

Significance

This study was significant to both researchers and practitioners. Specifically, the researcher made a contribution to academic research and to practice. The research design was a qualitative Delphi study. Therefore, the main academic contribution of this study was a model based on the perceptions and experiences of experts in the phenomenon of interest. Moreover, another contribution of the study to academic research was addressing the gap in literature about exploring effective countermeasures for cyber threats specific to the specific use of networked medical devices.

The findings were beneficial to practitioners who defend systems connecting to medical devices susceptible to cyber threats that led to malicious attacks (William & Woodward, 2015). In particular, those who led the forefront of guidance in support of medical devices were to ensure minimizing threats and vulnerabilities. With the findings for this research, the researcher provided a basis for IT experts to follow in terms of preventing a security breach when using networked medical devices. IT leaders in the field of healthcare, including networked medical device production, could use the model for this study to enhance procedures in order to ensure the security of the device from cyber threats and minimize risks related to its use, especially when connected to a network. Moreover, with the findings from this study, the researcher increased awareness of IT support and organizations within the United States that support medical devices. Others can also use the results of this research to assist in the automation of alerting the proper help to reduce risk to networked medical devices and mitigate cyberattacks.

Definition of Terms

CIA Triad. CIA Triad, according to NIST (2018), was a security model supported by Information Security (InfoSec) representing each attribute of security: confidentiality, integrity, and availability that is used to evaluate policy within organizational assessment.

Countermeasures. Seale (2017) described countermeasures as a mechanism in place to protect and alert by performing an analysis of confidentiality, integrity, or availability to avert encounters from potential attacks.

Information security. Information security, as defined by Federal Information Security Management Act (FISMA), encompassed integrity, confidentiality, and availability to protect systems maintaining information from unauthorized access, use, disclosure, disruption, modification, or destruction supporting.

Medical device. The U. S. Food & Drug Administration (n.d.) defined a medical device as a component intended to mitigate, prevent, or treat a patient's diseased or conditions attached to the body internally or externally.

Networked medical device. Networked medical devices are a set of medical devices that are connected to an IT network that a healthcare facility uses for storing and managing information and operating these devices remotely (Meng, Li, Xiang, & Choo, 2017).

Risk. Risk was defined in the Computer Security Resource Center (CSRC) glossary within the FIPS 200 by NIST as the likelihood of a threat occurring and the impact it has on the information system and the organizational (NIST, 2019).

Schema. Schema refers to a structured format or model used to organize data. A schema refers to "a network of subschemata," where each of which carries out its assigned task of evaluating its goodness of fit whenever activated" (Rumelhart, 2017, p. 33).

STRIDE model. The STRIDE threat model was developed by Microsoft employees Garg and Kohnfelder using a mnemonic for indicating security threats within categories such as spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privileges (Hernan, Lambert, Ostwald, & Shostack, 2014; Kohnfelder & Garg, 1999).

Theory of reasoned actions (TRA). A theory that aligns towards the attitude also refers to a person's mannerisms in relation to a behavior and the act of performing the behavior with limited regard to overall performance (Ajzen & Fishbein, 1980).

Telehealth. Telehealth refers to the distribution of services and information in the field of healthcare through electronic information and telecommunication technologies (Car, Tan, Huang, Sloot, & Franklin, 2017).

Threat. Threat was defined in the Computer Security Resource Center (CSRC) glossary within the FIPS 200 by NIST (n.d.) as any event with an information system that can potentially have an adverse impact to an organizations operation, assets, or individual as a means of unauthorized access, modification of information, or cause destruction.

*Vulnerabilit*y. Vulnerability was defined in the Computer Security Resource Center (CSRC) glossary within the FIPS 200 by NIST (n.d.) any weakness that could exploit an information system, internal controls, or breach the system security procedures by a source of threat.

Assumptions and Limitations

Assumptions

As with any study examining cybersecurity, this research was subject to assumptions and limitations. The researcher assumed that results from this study would build upon data from experts in the cybersecurity of networked medical devices. The first assumption for this researcher was that all medical devices connecting to a healthcare network could expose a patient and their records. Another assumption was that participants provided honest and complete answers when asked to give information about the topic of the study. The researcher also assumed that the researcher applied the methodology used when collecting and analyzing the data for measuring controls and assessing the integrity, confidentiality, and availability of the medical devices. The researcher also assumed that the continued development of medical devices will advance faster than technology could sustain and expectations for security will always remain an afterthought.

Limitations

The limitations of a research refer to the weaknesses in the design and nature of the study over which the researcher has no control. The first limitation of this study was that data would be collected only from IT experts in medical device industry with specialization in networked medical devices. Therefore, the researcher did not consider other participants for this study. The findings of the study cannot be directly generalizable to other settings, populations, and phenomenon. With the nature of Delphi research, the researcher was also limited to using multi-round data collection to reach and determine if a consensus exists among the participants (Dalkey & Helmer, 1963). The researcher conducted multiple rounds of data collection for this study. Another limitation was possible influences of researcher bias. The researcher has personal opinions, perceptions, and beliefs about the study, which may unnecessarily influence the findings of the study if left unaddressed. Therefore, the researcher acknowledged personal opinions, perceptions, and beliefs to increase personal awareness and cautiousness when making decisions and conclusions in alignment with these sources of personal biases.

Organization for Remainder of Study

In Chapter 1, the main discussion was about the topic of cybersecurity and risks involved in using networked medical devices. Based on the major discussion in Chapter 1, the general problem is the vulnerability of medical devices to cyberattacks. The specific problem addressed in the study was the lack of basis for developing effective countermeasures for cyber threats to networked medical devices leading to high possibility of security breaches. The purpose of this qualitative Delphi study was to support in a development for a model with effective countermeasures for cyber threats with networked medical devices based on experiences and perceptions of IT experts in the healthcare industry in the United States. The main research question was: What are the relevant experiences in employing a schema to analyze security risks

in medical devices? The researcher developed the discussion in Chapter 1 based on these key components of the study.

In answering the research question, Chapter 2 includes a literature review on security models, healthcare, and medical devices. The discussion in Chapter 2 built upon distinguishing the levels of risk between threats and vulnerabilities and defining the types of threats, both internally and externally, with the use of networked medical devices. Chapter 3 includes a summary of the methodology the researcher used to address the problem and research gap identified in Chapter 1 and Chapter 2. The researcher used a qualitative Delphi study. Chapter 4 includes the results from implementing the procedures discussed in Chapter 3. Chapter 5 includes the discussion of the conclusion, implications, and recommendations of the study.

CHAPTER 2. LITERATURE REVIEW

Introduction

Motivated by the increasing use of networked medical devices, multiple researchers conducted studies that have shown flaws in the security designed to protect these devices. (Cerkovnik, 2015; Jontz, 2015; Pardue, Purawat, & Landry, 2014; Seale, 2017). Several researchers explored risk, threats, and vulnerabilities of networked medical devices such as the study conducted by Pardue et al. A database-driven methodology was used to create a rational database to conduct a risk assessment identifying only assets, vulnerabilities, and security controls. The database performed capabilities such as queries showing value by executing and producing lists of threats to address and assess risks based on input (Pardue et al., 2014). Cerkovnik continued with a nonpeer-reviewed study make additional features to the proof-of-concept database-drive model previously created by Pardue et al. by applying a table within the database. This table was named tblDevice, which contributed to identifying information associated with networked medical device pertaining to certain attributes. These assisted in executing queries providing a tool for IT security experts to perform risk and vulnerability assessments. Seale continued upon Pardue et al.'s and Cerkovnik's work with the proof-of-concept database-driven model creating a case study using proposed frameworks consisting of security and risk. Using real-world data to build the case study captured threats with existing threat models and resourced information pertaining to vulnerabilities with networked medical devices, Pardue et al., Cerkovnik, and Seale continued to build a proof-of-concept rational database to assess risk, threats, and vulnerabilities with networked medical devices.

The researcher's discussion of literature review started with security breach exposures and security data breach. Next, the researcher explores cybersecurity frameworks, models, and

an analysis of networked medical devices. In this chapter, the researcher examines security control types and role in exposed networked medical devices relative to access control, audit and accountability, configuration management, identification and authentication, system and communications protection, and system and information integrity. Lastly, the comprehensive review includes an overall critique of existing research based on a database-driven proof-of-concept for risk assessment, vulnerability and risk management, and threat model database to assess networked device management. The researcher also employs an implementation of an automated mechanism for assessing risk using the CIA triad model incorporated with the STRIDE threat model supporting continuous diagnostics and mitigation for IT with alerting events and mitigating cyber-attacks.

Literature Search Strategy

The researcher used several databases to conduct the literature search including Google Scholar, ProQuest, SAGE Journals Online, ScienceDirect, ABI/INFORM Collection, AMC Digital Library, Summon, and on the Internet, United States government and organizational websites. Terms used to search in the databases were focused on networked *medical devices, cybersecurity, risk management frameworks, cyber threat models*. The researcher used the following words the key searches: (a) cybersecurity, (b) medical services, (c) security risk frameworks, (d) security threat, (e) security vulnerabilities, (f) security schema, and (g) security models. The researcher examined the full text articles and abstracts found when searching databases to determine if the sources were relevant to the study.

Conceptual Framework

The researcher used the theory of reasoned action (TRA) (Ajzen & Fishbein, 1980) as the conceptual framework to predict how individuals behaved given their pre-existing attitudes and

behavioral intentions. Ajzen and Fishbein's primary goal with the theory was to examine underlying basic motivation of an individual's urge in performing an action. With the TRA, Ajzen and Fishbein identified several factors that shape behavioral intentions and behaviors of individuals such as behavior, subjective norms, and perceived behavioral control. This researcher used the TRA to understand the perception of the participants and to build themes related to the elements of TRA and why participants choose to use the methods employed to protect networked medical devices.

Existing Theories

The existing body of knowledge in cybersecurity highlighted cyber-attacks on networked medical devices. This posed a greater risk than exposure of patient data as proved using the Hierarchical Cyber Incident Analytics (HCIA) technique as a technical approach that utilizes the technology threat avoidance theory (TTAT) to observe the phenomenon occurring with the risk to patient health (Young, Carpenter, & McLeod, 2016). Despite its limited use, TTAT transcended across other disciplines and applies to healthcare information systems, psychology, and risk analysis (Rho & Yu, 2011). The TTAT generally measures users who tried to avoid malicious threats to information technology and information systems. Developed by Liang and Xue (2009), as a theoretical framework, TTAT:

> Posits that users are motivated to avoid malicious IT when they perceive a threat and believe that the threat is avoidable by taking safeguarding measures; if users believe that the threat cannot be fully avoided by taking safeguarding measures, they would engage in emotion-focused coping. (p. 71).

The validity of the TTAT was based on the notion that user's behavior of avoidance and acceptance were different in the qualitative perspective, which acknowledges the inherent need for TTAT development (Liang & Xue, 2009; Rho & Yu, 2011). People sought to avoid negative stimuli and accept positive stimuli to varying information technologies in the IT environment

(Rho & Yu, 2011). Researchers had similar findings in a study of 486 computer users (Young et al., 2016). In Young et al.'s study, common predictors of avoidance motivation across different settings proved to safeguard cost, effectiveness, and self-efficacy. The researchers demonstrated that TTAT was a valid foundational framework designed to examine the behavior of users relative to malicious software (Young et al., 2016).

Several researchers used TTAT to understand security awareness and behaviors of individuals about security threats. Liang and Xue (2009) tested a model derived from TTAT and found that users' perceived threat, safeguard effectiveness, safeguard cost, and self-efficacy influence their threat avoidance behavior. Similar to Liang and Xue (2009), Arachchilage and Love (2014) used a theoretical model based on TTAT and revealed that user's self-efficacy influenced their phishing threat avoidance behavior. These researchers provided evidence that well-designed user education was needed to avoid security threats.

It is important to protect vulnerable code from being exploited to alter health care treatment. The theory of well-founded equivalence bi-simulation (WEB) refinement was utilized to verify code for correctness and can be employed in medical devices to facilitate patient treatment (Shuja, 2016). As a methodology, researchers used the WEB theory to bridge the gap between specifications and verification in the software life cycle process. Shuja examined the role of the WEB theory on two medical devices, insulin pumps and pacemakers. However, the technology within medical devices approved by the FDA is not deemed reliable and secure enough to distribute software while assuring patient safety (Shuja, 2016).

Researchers used the TTAT to explore how users try to avoid malicious threats to information technology and information systems while WEB would be used to determine how to protect vulnerable code in medical devices. Researchers used these two theories to explore

experiences of healthcare professionals with security threats in the medical devices. Frameworks for information systems provide precise definitions, steps, and standards that covered a range of essential functions of an information system; as it is related to risk management, the frameworks outlined the tasks that the system must be able to carry out in each of the steps. As Wilson and Rollman (2017) suggested, medical devices are a potentially dangerous security threat, and one of the means of improving assessment of risks and vulnerabilities were by widening the scope of risk assessment frameworks currently employed. This information could possibly assist with creating a model for developing effective countermeasures for cyber threats to wireless medical devices in the healthcare industry in the United States.

Security Breach Exposures

Network medical devices underwent radical technological advancements; however, this advancement increased healthcare networks, patients, and data exposure to security breaches. Multiple researchers found considerable risks associated with networked medical devices due to the lack of collaboration between manufacturers, providers, IT support, and patients, which contributed to weaknesses within the security of the systems (Patel, Al-Janabi, Alshourbaji, & Pedersen, 2015; Schwartz et al., 2018; Yuan, Fernando, & Klonoff, 2018). In fact, it has been reported that nearly 90% of healthcare organizations suffered a breach of their database (Gaukstern & Krishnan, 2018). Sametinger, Rozenblit, Lysecky, Ott, & Peter, (2015) discovered multiple challenges that could alter patient care when a medical device contained a flaw within the configuration, software, and communication protocols or when any threats impact the device. Patel et al. (2015) also discovered essential challenges that stem from the provision of healthcare by networked medical devices. As a result, networked medical devices imposed an increased risk leading to vulnerabilities (Patel et al., 2015). Additional findings proclaim that challenges

associated with networked medical devices affect decisions and mitigating factors linked to cybersecurity, patient safety, and hospital systems (Gee, 2017; Hagestad & Straumann, 2017; Sametinger et al., 2015). Hagestad and Straumann further posited that key stakeholders must work together to prevent harm to patients, systems, and medical devices by modernizing to the 21st century and putting security on the forefront. Similarly, Schwartz et al. (2018) noted that stakeholders across the healthcare sector must understand the need to cooperate in addressing medical device cybersecurity.

The integration of medical devices, networking, operating systems, and software compromise the safety of networked medical devices, especially wireless implanted medical devices. The most common vulnerabilities including challenges with device access to the Internet through internal networks, default administration passwords with hard coding, and web interfaces to infusion pumps within a hospital setting (Williams & McCauley, 2016; William & Woodward, 2015). Zavitsanou, Chakrabarty, Dassau, and Doyle (2016) also noted concerns about embedded control in wearable medical devices, especially in guaranteed safety in the presence of external disturbances and unexpected system failures.

Exposure of security breaches played a quintessential role in the current healthcare sector including healthcare systems and patient security. Hackers used compromised networked medical devices as a means to conduct other types of attacks that harmed healthcare organizations' networks (William & Woodward, 2015). Olendorf (2015) recognized that compromised devices could be harmful to patients and even fatal at times. Olendorf noted that infected medical devices were difficult to detect due to the limited access controls as well as the lack of standard detection and remediation in place today. Standard governance had an accountability issue regarding ownership of patient's privacy and risk. There was no delineated

line of responsibility with the devices, therefore, health care providers and users were not subject matter experts with regard to the specific device patients were using (Olendorf, 2015). The average person did not maintain this type of knowledge about technology regarding the maintenance and device security design. Providers and patients were provided a user guide and introductory session about their medical devices.

Implementing security precautions prevented a data breach; however, if the data were compromised, it might affect sensitive information and could lead to physical harm to patients. William and Woodward (2015) proclaimed that the threat to medical devices and subsequent concerns with patient safety was most significant when the devices connected via a wireless network. Research regarding security vulnerabilities in several other studies focused on studying implantable medical implants and its effect on healthcare systems and patient safety (Camara, Peris-Lopez, & Tapiador, 2015; Kramer et al., 2012; Kune, Backes, Clark, Kramer, Reynolds, Fu,… & Xu, 2013; Larson, 2017; Maisel & Kohno, 2010). In addition to standard security measures, Camara et al. indicated networked medical devices must also comply with the desired computing power, energy, and storage consideration or the device becomes comprised to the original intensions with providing proper medical requirements.

Researchers revealed privacy and security risks that compromise the implantable medical device and patient health. Adverse events were commonly associated with vulnerabilities in implantable medical devices. Researchers Camara et al. (2015), Kramer et al. (2012), Kune et al. (2013), and Maisel and Kohno (2010) denoted that the most significant concerns with adverse events were associated with patient safety. Exploited vulnerabilities in cardiac implanted devices, which was an example of wireless implanted medical devices, may lead to arrhythmia, bradycardia, heart failure, and tachycardia while adverse events of a drug delivery system such

as insulin pumps may contribute to injury, inappropriate dosage, inappropriate timing, and diminished pain relief (Camara et al., 2015). Decreased patient safety also arose since some of the data were utilized to inform treatment alternations (Larson, 2017). Another risk was the attempt to take control of the device by causing malfunctions related to electromagnetic interference (Ankarali, Demir, Arslan, & Gitlin, 2017; Larson, 2017).

Security Data Breach

Security data breaches inclusive of protected health information (PHI) and personal identifiable information (PII) appeared to have been increasingly prevalent in the healthcare industry. According to the Human Health Service's Office of Civil Rights (2013), a breach was characterized as any form of impermissible use or disclosure under the Privacy Rule that compromised the security or privacy of the protected health information. An impermissible use or disclosure of protected health information was presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there was a low probability that the protected health information was compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the protected health information involved, included the types of identifies and the likelihood of re-identification;
2. The unauthorized person who used the protected health information or to whom the disclosure was made;
3. Whether the protected health information was actually acquired or viewed; and
4. The extent to which the risk to the protected health information has been mitigated. (para. 2)

Entities and their associates covered under the Health Insurance Portability and Accountability Act (HIPAA) were required to notify individuals who were possibly affected by a breach (Center for Medicare & Medicaid Service, 2018; Office of Civil Rights, 2013).

Protected Health Information (PHI)

Disclosure of PHI was increasingly prevalent following a security data breach. According to the Centers for Medicare & Medicaid Services, the U.S. Department of Health & Human Services, and the Medical Learning Network, PHI included an individuals 'protected health information that can either be transmitted or held by a HIPAA covered entity (Center for Medicare & Medicaid Service, 2018). The Office of Civil Rights (2013) focused on unsecured PHI, which was characterized as "protected health information that has been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in guidance" (para. 5). PHI's were available in electronic, paper, and verbal forms and generally included private patient information such as "the individual's past present, or future physical or mental health or condition; The provision of health care to the individual; The past, present, or future payment for the provision of health care to the individual" (para. 5). Some of the most common identifiers included the patient's name, address, date of birth, and social security number (Center for Medicare & Medicaid Service, 2018). Swim (2012) extended the most common identifiers previously noted (Center for Medicare & Medicaid Service, 2018) and highlighted identifiers such as the patients' account numbers, device identifiers, email address, fax numbers, health insurance beneficiary numbers, medical record numbers, phone numbers, and serial numbers etched in the implantable medical device.

A security data breach of PHI involved the acquisition, access, utilization, and disclosure of unsecured personal identifying patient information, which significantly increased the risk of reputational, financial, and other harm to the individual affected. PHI-related breaches are measured in accordance with:

(1) An access to, or use or disclosure of unsecured PHI;

(2) A use, access, or disclosure that violates the Privacy Rule (i.e., Subpart E of 45 C.F.R. 164)

(3) A significant risk that such access, use or disclosure will cause financial, reputational, or other harm to the patient; and

(4) No exceptions that apply. (Johnson, 2019).

Patients were readily affected by a breach of unsecured PHI under provision 45 CFR SS 164.400-412 of the HIPAA Breach Notification Rule (Office for Civil Rights, 2013). HIPAA's breach notification, privacy, and security rules enhanced the protection of the security and privacy of an individuals 'health information. HIPAA's privacy rule established standards and guideline by which PHI could be used and disclosed nationally whereas the security rule was associated with ways in which to safeguard the HIPAA covered entity and its associates (U. S. Food & Drug Administration, 2017a). Covered entities included health care providers such as clinics, chiropractors, doctors, dentists, hospitals, nursing homes, psychologists, and pharmacies (Center for Medicare & Medicaid Service, 2018). The entity and its associates were required to employ these safeguards to protect the availability, confidentiality, and integrity of electronic PHI (U. S. Food & Drug Administration, 2017a). Klonoff and Price (2016) suggested the need for a privacy standard for medical devices that transmit PHI. Martínez-Pérez, De La Torre-Díez,

and López-Coronado (2015) also added that there should be a security standard for medical devices such as mobile health applications to ensured that safety of the patient.

Personal Identifying Information (PII)

In accordance with OMB Memorandum M-07-1616, personally identifiable information (PII) was defined as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked to a specific individual. Non-PII could become PII whenever additional information was made publicly available, in any medium and from any source, and when combined with other available information could be used to identify an individual (Speidel, 2018, para. 2).

The U.S. Department of Labor (2018) further extended the definition of PII proclaimed that it included direct and indirect information that permits another individual to ascertain an individual's identity such as date of birth, gender, geographic information, and race among many often identifiers (U.S. Department of Labor, 2018). Loss of PII contributed to significant harm such as fraudulent utilization of an individuals 'personal information and identity theft (U.S. Department of Labor, 2018). As a result, personal identifying information should be protected from misuse and loss (U.S. Department of Labor, 2018). NIST (2010b) supported the U.S. Department of Labor findings; however, they noted that in addition to its use, PII should be protected against inappropriate access and disclosure of personal information. Gordon, Fairhall, and Landman (2017) added that the attacks on PHI and PII were worrisome and could endanger patients.

Roles and Responsibilities for Medical Devices

Key stakeholders all have roles and responsibilities in addressing cybersecurity threats. Key stake holders, such as such as manufacturers and importers of the specific networked

medical devices, have significant roles and responsibilities as it pertains to medical devices, as well as the United States (U.S.) FDA, healthcare organizations, and affiliated healthcare providers, and patients (Webb, Dayal, & Lawyers, 2017). These stakeholders shared responsibility in addressing cybersecurity threats that can affect networked medical devices (Webb et al., 2017).

Medical Device Manufacturers and Importers

Manufacturers and importers of medical devices contributed to its widespread development, production, and distribution in the U.S. healthcare industry. The FDA posited that a manufacturer of medical devices was a distributor of medical equipment involved in the procedure of assembling biologically, chemically, or physically even if it entails secondary distribution as set forth in Title 21 of the Code of Federal Regulations (CFR) Part 807 ("Who Must Register, List and Pay the Fee," 2017). Manufacturers were therefore required to address any threats to cybersecurity that transpire during the medical device's lifecycle such as its design, development, production, deployment, distribution, and maintenance phase (U. S. Food & Drug Administration, 2016b). A postmarket recommendation established by the FDA denotes the postmarket management of such devices. Manufacturers of medical devices must be responsible for monitoring, identifying, and mitigating any cybersecurity exploits and vulnerabilities (U. S. Food & Drug Administration, 2016b; Webb et al., 2017). Vulnerabilities were a weakness or flaw within a system or design of a networked medical device or system that could expose threats exposing to patients, networks, and information (Ankarali et al., 2014; Hwang et al., 2016; Olendorf, 2015).

Researchers proclaimed that although manufacturers of medical devices shared similar roles and responsibilities to importers, reporting varies between both entities. According to the

U. S. Food & Drug Administration (2017b), an importer is characterized as a company or individual in the United States that was an owner, consignee, or recipient, even if not the initial owner, consignee, or recipient, of the foreign establishment's device that was imported into the United States. An importer does not include the consumer or patient who ultimately purchases, receives, or uses the device, unless the foreign establishment ships the device directly to the consumer or patient (CFR - Code of Federal Regulations Title 21, 2017, para. 27).

Manufacturers and importers of medical devices, mandatory reporters, were responsible for submitting reports of any product-related issues and adverse events to the FDA. According to the 21 Code of Federal Regulations (CFR) 806.1, the Federal Food, Drug, and Cosmetic Act required manufacturers and affiliated sponsors who were considered importers of devices to report all issues about possible corrupt, malfunctioning, removals or decommissioning within ten working days following initial action (U. S. Food & Drug Administration, 2018a). All actions required documentation and reported to the FDA based on regulation 21 CFR 803. Regulation 21 CFR 803 set forth within the Medical Device Reporting (MDR) mandated device user facilities, importers, and manufacturers to report problems with medical devices and adverse device-related events to the FDA (U. S. Food & Drug Administration, 2018b). Both manufacturers and importers must report to the FDA once they acquired knowledge and detailed information regarding a specific medical device associated with serious injury or contributed to an individuals 'death (U. S. Food & Drug Administration, 2018d; U. S. Food & Drug Administration, 2016a). Manufacturers were obligated to report immediately to FDA after becoming aware of device malfunctioning and the increased likelihood that the medical device might either cause or contribute to serious injury or death if the malfunction occurred again. In contrast, importers of medical devices must report to the manufacturer if the devices imported

malfunctioned of if they could possibly contribute to or cause serious injury or death upon recurring malfunctioning of the device (U. S. Food & Drug Administration, 2018b.)

Manufacturers had the responsibility to cybersecurity measures in networked medical devices. However, Lam and Wong (2018) found that manufacturers were not committed to cybersecurity risk management because they wanted lower cost and shorter product life cycles, which was not possible with the implementation of cybersecurity measures. Moreover, manufacturers also cited unequal power between manufacturers and distributors. Gee (2017) found manufacturers face challenges with networked medical devices experienced that correlate with advancing the development of medical devices with the latest technology by using sensors. However, this placed security as an afterthought during the design phase, as manufacturers were focused on treating the patient before protecting them (Hagestad & Straumann, 2017).

Since August of 1996, the Manufacturer and User Facility Device Experience (MAUDE) database provided a compilation of all the mandatory reports filed by importers and manufacturers of medical devices (U. S. Food & Drug Administration, 2018d; Webb et al., 2017). The FDA reported that mandatory reporters inclusive of manufacturers, importers, and device user facilities filed several thousand MDRs based on device-related malfunctions, serious injuries, and death (U. S. Food & Drug Administration, 2018b; U. S. Food & Drug Administration, 2019b).

Food and Drug Administration

In the United States, medical devices were regulated and approved for use by the FDA. The FDA was deemed responsible for enforcing laws to enhance the protection of public health. In 1976, findings reported a total of 731 deaths and 10,000 injuries caused by faulty medical devices led to the development and enactment of Medical Device Amendments (U. S. Food &

Drug Administration, 2018e). Under the Medical Device Amendments of 1976, new medical devices protected by safety and effective standards (U. S. Food & Drug Administration, 2018e). The FDA enhanced the provision of guidance for following Postmarket Medical Device requirements throughout the United States. FDA provided guidance and recognized the NIST Framework Core for the purpose of determining hazards and risks during the design phase ensuring protection can be eliminated prior to use by a practitioner and patient (Webb et al., 2017). Administrative laws, also known as the CFR, focus on mandates relative to the manufacturing and security of medical devices in parts 800 to 898. One of the essential regulatory requirements was that medical devices are in categories as Class 1, Class 2, or Class 3 based on its safety and clinical effectiveness. The U. S. Food & Drug Administration (2016b) later published a guidance document for medical devices encompassed cybersecurity as they were not enforced reporting requirements under 21 CFR part 806.

The U. S. Food & Drug Administration (2018d) maintains a surveillance tool called Manufacturer and User Facility Devices Experience (MAUDE) database categorizing issues contributing to risk assessments that track all recalls with the medical devices and classify according to the risk of the patient. Specific events with medical devices concerning malfunctions were required by U. S. Food & Drug Administration (2018d) to be tracked. Manufacturers, importers, and device user facilities were mandatory to report postmark the device. Voluntary requirements, only encouraged by the U. S. Food & Drug Administration (2018b), were the healthcare providers, and patients who use of the Medical Device Reporting (MDR). MedWatch is a tool used for social media to broadcast and report problems with medical devices (U. S. Food & Drug Administration, 2018c). Researchers found no existing database tracking malicious activity due to cyber events that could impact the equipment, patient safety,

and healthcare network devices that were connected (Alemzadeh, Iyer, Kalbarczyk, & Raman, 2013; Cerkovnik, 2015; Seale, 2017).

Healthcare Organizations, Healthcare Providers, and Patients

Voluntary reporter of medical devices also plays a quintessential role in ensuring safety and enhancing the effectiveness of medical devices. Voluntary reporters, such as consumers, healthcare professionals, patients, and caregivers, are also responsible for reporting medical device malfunctioning, issues relating to product quality, user errors, and therapeutic failures (U. S. Food & Drug Administration, 2018d). Major stakeholders inclusive of healthcare organizations and healthcare providers voluntarily report concerns of defective medical devices for the healthcare industry as well as patients concerning defective medical devices. The reports submitted to FDA's Safety Information and Adverse Event Reporting Program, MedWatch (U. S. Food & Drug Administration, 2018c). Information concerning adverse events caused by diminished quality, errors, failures, and malfunctioning is reported accordingly (U. S. Food & Drug Administration, 2018c). Zeitler et al. (2019) also emphasized the role of voluntary reporters in reporting adverse events involving medical devices and how it helps FDA in collecting information and notifying the organization and the public.

Cybersecurity Frameworks

Cybersecurity frameworks were a way for organizations to protect themselves regarding potential cyber-attacks. In compliance with various cybersecurity regulations, there are multiple frameworks within federal agencies, such as NIST's risk management and industry standards ISO 31000 Risk management (ISO, 2018), which were utilized to protect and defend against cyber-attacks. Since networked medical devices followed federally regulated guidelines in the United States, the U. S. Food & Drug Administration (2016a) published guidance for risk-based

frameworks designed to assess cybersecurity in medical devices. Kasparick, Schlichting, Golatowski, & Timmermann (2015) noted the need for standards ensured that networked medical devices were safe from cyber-attacks.

Cybersecurity was used to combat insider threats that adversely affect the healthcare industry. Insider threats may be malicious as well as unintentional in nature. Malicious insider threats involve the intentional utilization of a business partner, contractor, former or current employee information and authorization in a way that allows them to gain access to confidential information (HIMSS, 2017). This access may adversely affect the availability, confidentiality, and integrity of the healthcare organizations information systems. However, unintentional threats were not performed with an underlying malicious intent although the actions or inactions of the individual's activity causes harm or significantly increases the likelihood of future harm to the availability, confidentiality, and integrity of the organizations' information systems (HIMSS, 2017). Based on a survey conducted by HIMSS, approximately 85% of survey respondents conducted a risk assessment at minimum once annually (HIMSS, 2017). Of these respondents, 9% conducted daily risk assessments, 10% made risk assessments once a month, 8% performed quarterly risk assessments, and 51% conducted risk assessments annually (HIMSS, 2017). In a review of 31 peer-reviewed articles of cybersecurity in healthcare organizations, Kruse, Frederick, Jacobson, and Monticone (2017) found that healthcare industry lags behind in terms of security compared to other industries, which must be addressed because the healthcare industry is a prime target for medical information theft. Similarly, Coventry and Branley (2018) also asserted that electronic health records, healthcare infrastructure, and individual medical devices were targets of cyber-attacks. Due to the inherent weaknesses of security in healthcare

industry, it was the most targeted sectors worldwide with 81% of 233 healthcare organizations hacked in 2015 alone (Martin, Martin, Hankin, Darzi, & Kinross, 2017).

The Healthcare Information and Management Systems Society (HIMSS) in partnership with senior leadership within Healthcare and Public Health (HPH) organizations surveyed to examine the adoption of best practices concerning cybersecurity. Research findings revealed that approximately 86% of all respondents used a security framework within the organization. Additional results showed that roughly 95% of surveyed respondents leveraged the NIST Cybersecurity Framework by analyzing core functions to detect, identify, protect, respond, and recover. Another study was performed to provide additional insight into the purpose and utilization of cybersecurity frameworks within the U.S. healthcare sector. The report found substantial insight from experts in the U.S. healthcare organizations performed as a cybersecurity profession (HIMSS, 2017). Of 126 information security professionals who were either primarily responsible or partially responsible for the information security program within their respective health care organization throughout the United States, approximately 80% of survey respondents reported that their organization employed cybersecurity professionals (HIMSS, 2017). Findings demonstrate that about 78% of respondents identified a cybersecurity-staffing ratio, of which well over half (53%) reported a ratio equivalent to 1:500 or lower (HIMSS, 2017). Additional research findings revealed that approximately 75% of survey respondents reported that their healthcare organization had an insider threat management program (HIMSS, 2017). Based on these findings, 40% reported policies enforced while the other 35% noted informal threat management programs within their respective healthcare organizations (HIMSS, 2017). According to Kruse et al. (2017), time and funding should have been invested to ensure the

protection of healthcare technology as well as the confidentiality of patient information from unauthorized access.

National Institute of Standards and Technology (NIST) Framework

Methods for risk management and analysis developed the following concerns regarding the categorization and distribution of information surrounding security risks. Risk, a measure of the prospect of a threat occurrence and adverse impact associated with that event (NIST, 2012). In accordance to the NIST Special Publication 800-30: *Risk Management Guide for Information Technology Systems*, risks were identified and aligned with system security that determines the probability of occurrence, resulting in impact, and safeguards that could mitigate the effect. Risk factors and how such factors contribute to the depicted risk assessment. Olendorf (2015) found FDA identified potential risk to the safety and well-being of the public's health. By using monitoring techniques, manufacturers prevented exposures when threats were issued by NIST risk frameworks (NIST, 2010a; Smigielski, 2017).

The NIST (2010a) alongside the U.S. Department of Commerce noted three types of risk management within a three-tier hierarchy system. Tier 1 denoted the harm to the organizations' image or reputation or financial loss (NIST, 2012). Tier 2 was a representative of the incapacity to execute a business process successfully. Risk, a measured of the prospect of a threat occurrence and adverse impact associated with that event (NIST, 2012). Lastly, Tier 3 symbolized the resources expended in response to an incident to the organizations 'information system (NIST, 2012).

Cybersecurity was an amplification of the organization's risk management. In 2014, NIST's role updated by the Cybersecurity Enhancement Act of 2014 (U. S. Congress, 2014). NIST's new role incorporated the identification and development of cybersecurity risk

frameworks. Researchers indicated that NIST was responsible for identifying a cost-effective, flexible, performance-based, prioritized, and repeatable approach that included information security controls (NIST, 2013) and measures that may be voluntarily adopted by both critical infrastructure owners and operators (NIST, 2013). This approach aided in identifying, assessing, and managing cyber risks. Ponikowski et al. (2016) asserted that the importance of holistic risk management and how this would improve the NIST framework for cybersecurity.

International Organization for Standards (ISO)

Medical devices were required to adhere to international standards to ensure patient safety. Yuan et al. (2018) asserted the need to ensure standards for medical device cybersecurity. Since the advent of the Internet, medical devices and their malfunctioning played a critical role in continuous patient safety among patients who rely on such devices to improve their health outcomes (Anderson & Williams, 2018). Findings demonstrated deficiencies related to the standard and identifies cybersecurity components that identified. Designated areas of improvement included data backup, disaster recovery, emergency access, health data de-identification, physical locks on devices, third-party components in product lifecycle roadmap, transmission integrity as well as transmission confidentiality (Anderson & Williams, 2018). ISO 14971 focused on the risk management of single-manufacturer monolithic devices; however, the trends of building from reusable platforms posed as a risk challenge (Hatcliff, Vasserman, Carpenter, & Whillock, 2018). Anderson and Williams (2018) provided health delivery organizations that implemented ISO/ICE 80001 assurance regarding the degree of protection associated with the standard as well as the areas that required further improvement to increase cybersecurity and patient safety. Such outcomes influenced the development of international standards such as the Joint Working Group 7, the International Organizations for

Standardization, and TC215 Health Informatics as it is related to the utilization and assessment of ISO/IEC 80001 (Anderson & Williams, 2018). MacMahon, Mc Caffery, and Keenan (2015) explained the components of MedITNet framework and how this framework addressed the challenges faced by healthcare delivery organizations in terms of cybersecurity, which was also aligned with the requirements of ISO/IEC 80001.

Center for Internet Security

The Center for Internet Security (CIS) developed critical security controls that played a significant role in effective cyber defense against cyber-attacks. According to SANS, essential controls of security guided by two fundamental principles, "prevention is ideal, but detection is a must and offense informs defense" (SANS, 2018, para. 1). Organizations were responsible for defending their systems and networks from internal and external threats. Organizations were prepared to detect and prevent damaging activities following an attack within a compromised network (SANS, 2018). Organizations utilized critical controls to automate protection, and continuous monitoring of sensitive IT infrastructure to employ critical controls to protect the organizations 'critical assets, information, and infrastructure (SANS, 2018). As a result, critical controls minimized the number of compromised networks thus reducing recovery efforts needed and lower costs (SANS, 2018). Martin et al. (2017) noted that critical security controls were used to address cybersecurity measures for healthcare medical devices.

Analysis of Networked Medical Devices

Cyberattacks not only posed a threat to medical information of one patient but also to a lot of patients, especially if the attack occurred in networked medical devices. The FDA raised concerns about networked medical devices correlated with vulnerable off-the-shelf (OTS) software (HIMSS, 2005; U. S. Food & Drug Adminstration, 2018e). OTS software enabled

attackers to obtain unauthorized access to a medical device or its network (U. S. Food & Drug Administration, 2018e). Sametinger et al. (2015) warned the public about using OTS because while it powered the medical technology devices, it also could have been be subject to cyberattacks that could harm the patient. There was a need to address cybersecurity weaknesses to increase the overall safety and effectiveness of medical devices that connect to networks (U. S. Food & Drug Administration, 2018c).

There are numerous studies of this phenomenon due to increasing use of networked medical devices and its utilization within other healthcare systems. According to the Ponemon Institute (2017), approximately 44% of healthcare organizations that utilize network medical devices followed the FDA's guidance supporting security risks. Additional research findings revealed that only 17% of manufacturers made medical devices and about 15% of healthcare organizations implemented preventative measures to protect against attacks (Ponemon Institute, 2017). In support of advanced mechanisms to enhance the provision of patient care through interconnectivity and interoperability, as well as exposing cybersecurity risks, Schwartz et al. (2018) discovered that the FDA held public-facing workshops seeking to close the gaps between policy, science, and technology. Yuan et al.'s (2018) findings further complicated the results of Schwartz et al. Yuan et al. proclaimed that all recommended standards and guidance supported network medical devices were recommended that it may not comply to all products thereby leaving a gap with manufacturers testing and evaluating against the individual risk assessment process that potentially imposed a cyber-threat to the healthcare organization.

Several researchers noted that wireless medical devices can be subjected to cyberattacks. In fact, a pacemaker hack occurred in 2008 followed by an insulin pump hack 3 years later, in 2011 (Larson, 2017). In response to such hacks, minimum improvements were made to enhance

the level of protection provided to implanted insulin pumps from hackers who have the capability of administering large doses often legal (Jontz, 2015). In addition to attacks on implanted insulin pumps, cyber-attacks affected other implantable medical devices as well. Reports also proclaimed that cybersecurity breaches allotted hackers the opportunity to deliver deadly shocks to patients with pacemakers (Jontz, 2015). A new array of vulnerabilities discovered in 2013 with anesthesia devices, defibrillators, insulin pumps, laboratory equipment, patient monitors, surgical instruments, and ventilators (Larson, 2017). William and Woodward (2015) stated that this is a new form of hacktivism that could endanger the lives of many patients.

There was a need to ensure that networked medical devices were protected from cybersecurity attacks. To safeguard the management of healthcare technology, it was vital to design, build, and maintain a secure environment for networked medical devices (Busdicker & Upendera, 2017). In 2018, the Worldwide Health Industry predicted that by the year 2021, manufacturers of medical devices will be held liable for over 25 deaths (Shegewi, Mutaz, Dunbrack,& …Townsend, 2017). Results led to lawsuits totaling well over $100 million due to the lack of security causing vulnerabilities during cyber-attacks (Shegewi et al., 2017).

Networked medical devices created additional challenges when providing healthcare telemetrically. These challenges imposed a set of risks that increase the possibility of vulnerabilities that exposed the security and privacy of patients and health information systems (Patel et al., 2015). One study examined how prepared and unprepared manufacturers and healthcare organizations performed in defense against attacks on networked medical devices. Synopsys, who sponsored the research conducted by the Ponemon Institute (2017), discovered that roughly 31% of device manufacturers and 40% of healthcare organizations were aware of

the attacks. Medical device manufacturers (39%) reported a compromise by an attacker (Ponemon Institute, 2017). Research findings also revealed that approximately 38% of healthcare organizations found inappropriate patient telehealth delivered due to the lack of security with the medical devices (Ponemon Institute, 2017). Gaukstern and Krishnan (2018) also found that cybersecurity threats were targeting networked critical medical devices because of their vulnerabilities. Additionally, devices with inadequate software maintenance posed risks to network safety and patient safety and privacy (Ransford, Kune, Gookin, & DeOrio, 2016; Seale et al., 2018).

Industrial Control Systems Cyber Emergency Response Team

One way to address cybersecurity attacks was to create emergency response teams. The Industrial Control System-Cyber Emergency Response Team (ICS-CERT), in partnership and collaboration with law enforcement agencies, intelligence, and local, federal, state, and tribal governments, significantly decreased risks within all sectors (ICS-CERT, 2018). Hence, the primary organizations reported on safety and security of medical devices were the ICS-CERT and the U. S. Food & Drug Administration. ICS-CERT (2018) published numerous alerts and advisories warning about vulnerable devices, yet the. FDA had rarely, if ever, officially recalled a device as a result of its cyber vulnerabilities. An indicator that the FDA treated cyber vulnerabilities like other equipment flaws (ICS-CERT, 2018). He, Devine, and Zhuang (2018) stated that there was a need to use a decision-theoretic approach in cybersecurity information sharing among stakeholders to ensure that cyber vulnerabilities were not overlooked and being addressed seriously.

The proposed scoring system used for the cybersecurity frameworks by NIST could assist the FDA in categorizing medical devices based on their potential cybersecurity risks and outline

enhanced testing requirements for these devices. Stine et al. (2017) also suggested the use of a cyber-risk scoring system for medical devices ensured the safety of the patients. However, manufacturers of medical devices lacked independent testing facilities to conduct a proper postmarket test, premarket safety test, or destruction and survivability test provided proof of embedded cybersecurity defenses needed by networked medical devices (ICS-CERT, 2018; Lam & Wong, 2018; Pandey & Batra, 2013; U. S. Food & Drug Administration, 2013). Assante and Lee (2015) utilized attackers' objectives and examined the kill change control within cybersecurity. Three out of nine categories demonstrated the system components based on control, safety, sense, and views. A proposed risk scoring system for medical devices was employed to examine whether the device posed a threat to patient safety. Every medical device has a human-machine interface (HMI), which was used to control the device and its safety features thereby ensured both user and patient safety (ICS-CERT, 2018). Despite the ease and low operational cost associated with the risk scoring system, results yield consistent scores for medical devices based on their potential to impact patient health and wellbeing. This scoring system was designed to enable medical device vendors and healthcare providers evaluated the cyber risk of medical devices adequately.

Security Controls and Exposures

Access Control

Networked medical devices exposed multiple protocols to communicate through various radio frequencies beyond the scope of traditional tools. Capabilities provided a way to monitor and manage the network security in an attempt to safeguard detection and prevention mechanisms (Baranchuk, Refaat, Patton, Chung, Krishnan, Kutyifa, … & Lakkireddy, 2018; Mahler et al., 2018; Wu, Guizani, & Mohamed, 2017). Networked medical devices contained

potential risks with possibilities for reconfiguration. This reconfiguring aids in thwarting cybersecurity threats. In a study, Wu et al. (2017) found that attacks occur through the wireless connection between the medical device and the proxy device it communicated with to report therapy-related vitals. During an attack, the hacker leveraged the communications protocol on an implanted cardioverter defibrillator (ICD) to reverse-engineered the device, accessed the patient information, and activated an attack to control the therapy settings and battery (Wu et al., 2017). In addition to the examined implantable medical devices, another study focused on medical imaging devices (Mahler et al., 2018; Wu et al., 2017). Mahler et al. also discovered that medical imaging devices not updated with patches could expose the hospital infrastructure due to its connectivity with the device. By delivering false reports or electronic health records (EHRs) over the network may jeopardize the patient's health (Mahler et al., 2018).

Audit and Accountability

Healthcare organizations used supplier audits to assess the quality system of prospective suppliers before purchasing medical devices, which could also be important in cybersecurity of medical devices. During a supplier audit, IT risk management must acquire information that may affect the ability to integrate medical devices into the organization's network (Das et al., 2018; Rakitin, 2009). Manufacturers of medical devices and information technology network suppliers were recommended to work collaboratively with clinical engineering-information technology professionals to gain documentation of relevant safety cases and address safety issues that arise in the future (Das et al., 2018; Rakitin, 2009).

Configuration Management

In the configuration management process, a collection of hardware and software used was configured that could also affect cybersecurity of medical devices. Typical examples of

hardware and software components that may undergo configuration management included accessories, cables, computer hardware, database, documentation, network hardware components, and operating systems (Rakitin, 2009). Configuration management of networked medical devices involves two principal components, configuration identification, and change control. Configuration identification entailed the documentation of ways in which configuration items interconnect with one another (Rakitin, 2009). Configuration management then focused on change control and documentation of a new baseline by using the standard operating procedure with regard to how to approve, document, implement, initiative, and release changes (Rakitin, 2009). Planned changes included hardware or software updates or the implementation of additional modules.

Identification and Authentication

Before establishing a connection, the information system focused on identification and authentication. Since software continuously aged due to shifting threats, vigilance, updates, and maintenance was always needed. NIST's framework for cybersecurity control systems may apply to networked medical devices supporting the security posture. Sczyrba et al. (2017) also highlighted the role of NIST's framework in addressing challenges of new technology of medical devices. TrapX Labs (2016) examined vulnerable medical devices and notes that some devices have old operating software that no longer supported. Due to the long lifecycle of medical devices and the importance of security in developing devices, technology led to the evolution of engineering thereby generating support for providers caring for patients (Burns, Johnson, & Honeyman, 2016).

System and Communications Protection

Organizations developed a system and communications protection policy to address compliance, coordination among other entities, management commitment, purpose, roles and responsibilities, and scope. Procedures were also developed to implement the system and communications protection policy (Burns et al., 2016; NIST, n.d.; Webb et al., 2017). NIST highlighted transmission confidentiality and integrity, cryptographic management wireless link protection, mobile code, public access protections, and voice over Internet protocol (NIST, n.d).

System and Information Integrity

Cyber-attacks compromised system and information integrity. Cyber-attacks were common by both remotely or directly obtaining information and exploiting critical information such as code or personal identifying information. Devito and Johannes (2016) examined the security of Z-Waves on IoT's and the vulnerability attacks replayed. The researchers utilized FFT plots for GQRX and GNURadio; however, data were unusable (Devito & Johannes, 2016). FSK modulation was a success allowing for decoding of the signal. The Chairwoman of the U.S. Federal Trade Commission, Edith Ramirez, indicated that the threats to IoT include ubiquitous data collection, consumer data, and heightened security risk could potentially be unexpected for a patient (Devito & Johannes, 2016). In their study, Devito and Johannes also identified two factors that further compound risk. The risk compounded because consumers fail to recognize the value of privacy and security (Porup, 2016). Additional findings revealed that device manufacturers' poor implementation or exclusion of security features within products also contributes to a heightened risk of cyber-attacks (Noimanee, Noimanee, Krisanachinda, & Senavongse, 2016; William & Woodward, 2015).

Evaluating Risk Management Frameworks

Many researchers applied varying risk-based modeling simulations using different methodologies for mitigating the risk and determining how to employ mitigating factors to reduce risk (Alvarenga & Tanev, 2017; Rao et al., 2017; Seale et al., 2018; Stine et al., 2017). This study evaluated the opinions of IT experts' o who use risk management frameworks and effective countermeasures for cyber threats with networked medical devices. Exploring experiences with IT experts in the field and evaluating the relevant frameworks to support schema used to analyze security risks supporting networked medical devices.

Medical Device Privacy Consortium Framework

A risk assessment tool, the Medical Device Privacy Consortium Framework, benefits the stakeholders that obtain, control, and used the framework for medical therapy. A technology program at Carleton University performed a qualitative study that incorporated a value-sensitive design concerning risk probability (Rao et al., 2017). This risk probability design leveraged the MDPC framework (MDPC, 2014). Researchers in the study proposed that manufacturers maintain responsibility and actively communicate the device status details instead of utilizing the standard reporting method (Rao et al., 2017). The MDPC framework burdens manufacturers to identify the threat source and vulnerable state of the device, thereby reducing the exploitations for the asset and applying security controls to reduce the residual risk (MDPC, 2014; Rao et al., 2017). Rao et al. applied a risk-based framework that would continually manage and remediate security threats for medical devices. This type of model was developed as a middleware and embedded within medical devices to automate the remediate with security vulnerabilities (Rao et al., 2017).

MedDevRisk Framework

A proof-of-concept system collectively identified as MedDevRisk framework that leveraged existing research and the STRIDE model to identify risks with networked medical devices was developed (Seale et al., 2018). The features of MedDevRisk framework was a relational data model that captured medical device threats, assets, and vulnerabilities and a conventional risk assessment standard. This was used to address healthcare organizations 'need for proper threat assessment criteria (Seale et al., 2018, p. 3271). This framework ensured governance of the utilization of medical devices on the organizations' network. The MedDevRisk framework also enhanced the provision to integrate network device data and information with its corresponding security threat and remediation (Seale et al., 2018).

Threat Model Frameworks

Dimensional Research (2016) surveyed 338 Information Technology (IT) and security professionals in different industries in the United States; 27% of the healthcare industry players do not use a security framework; 73% adopted a security framework. The Dimensional Research survey reported that 12% of organizations in the healthcare industry in the United States use the Cybersecurity Framework (CSF), which is a National Institute of Standards and Technology (NIST) framework for improving critical infrastructure cybersecurity. CSF was a NIST (2018) framework that compassed security controls that organizations can employ to form an information security program protecting users, infrastructure, and assets managed by an organization, including those from the healthcare sector. With the increase in delivering remote healthcare, the use of medical devices was implemented to support the management of patient care through an adaptive risk-based scheme to assess the current state of the system (Rao et al., 2017).

Security threats were classified in accordance with different threat model frameworks. The STRIDE model, Open Web Application Security Project (OWASP), Common Weakness Enumeration (CWE), Threat-Vulnerability-Asset (TVA) model, and Confidentiality, Integrity, Availability (CIA) triad model assessed the risk and security of systems within the U.S. healthcare sector. Researchers conducted a number of studies regarding threat modeling in the healthcare sector. However, a gap in research literature existed due to the utilization of threat modeling methodologies such as STRIDE and CIA in medical devices particularly networked medical devices. Seale et al. (2018) examined the utilization/application of various threat assessment frameworks included a Common Vulnerability Scoring System, Common Vulnerabilities, and Exposures, and STRIDE within networked medical devices within a medical simulation lab.

STRIDE Model

The STRIDE model encompassed within Microsoft's Security Development Lifecycle (SDL) aided in defining the attack surface (Hernan, S., Lambert, Ostwald, & Shostack, 2014; Shostack, 2014). Microsoft's STRIDE model also aided in the identification of threats. The STRIDE threat model determined potential security threats and how to address such threats through threat identification, threat categorization, and threat documentation (Abomhara, Gerdes, & Køien, 2015; Seinfart & Reza, 2016). As a goal-based approach, the STRIDE model focused on threat identification and used system assets to ascertain an attackers' potential goals as well as how it can be achieved based on plausible points of attack (Seinfart & Reza, 2016).

In the STRIDE model, threats and attacks identify by six categories inclusive of denial of service, elevation of privilege, information disclosure, repudiation, spoofing, and tampering

(Abomhara et al., 2015; Seinfart & Reza, 2016; Shostack, 2014). According to Abomhara et al., the STRIDE model included the following categories:

- Spoofing: The attempt by an unauthorized user to gain access to a system.
- Tampering: The effective unauthorized modification or use of data.
- Repudiation: The user's denial that they performed unauthorized actions or transactions.
- Information Disclosure: The unwanted, potentially illegal, exposure of private data.
- Denial of service: The process of making an information system unavailable.
- Elevation of privilege: The act of assuming the identity of a privileged user if you are an unprivileged user who desires to gain privileged, or authorized access to an asset.

Some researchers stated that utilizing the STRIDE model was one of the most effective measures of reducing compromises to the information system (Abomhara et al., 2015; Olendorf, 2015). The STRIDE model classified the components of the information system into three separate categories of entities: assets, threat agents, and threats (Abomhara et al., 2015). How these entities were defined and how the STRIDE model projects them into organized tables would be further elucidated in the discussion of the CIA triad model.

Alhassan, Abba, Olaniyi, and Waziri (2016) provided more comprehensive delineations of the six categories within the STRIDE model (denial of service, elevation of privilege, information disclosure, repudiation, spoofing, and tampering). A denial of service attack occurs when an attacker seeks to make a machine, resource, or system within a network unavailable to others who have the intent of using it (Alhassan et al., 2016). Denial of service involves the temporary or indefinite interruption or suspension of a host and its related services that are connected to a network (Alhassan et al., 2016). In accordance with the elevation of privilege,

users find a manner in which to acquire access well beyond what their authorization (Alhassan et al., 2016). Such users tend to utilize the resources and services only allotted for users with more privileges. Information disclosure was correlated with the leaking of confidential information to a given user who does not have the authorization to access the data (Alhassan et al., 2016). In repudiation, a system user inclusive of legitimate as well as other users denies any accusations that they actively performed specific transactions as detected within the system (Alhassan et al., 2016). However, without proper logging of activities on auditing and systems, organizations were faced with the challenge of proving that a repudiation attack occurred (Alhassan et al., 2016). Regarding spoofing, a program or an individual could successfully impersonate any unsuspecting individual to acquire unauthorized access to information (Alhassan et al., 2016). This was achieved by using falsified information to obtain an illegitimate advantage. Lastly, a tampered attack occurs when an insider or outsider in the organization changes data in an effort to commit an attack (Alhassan et al., 2016). Privileged information was accessible to these individuals, so they tended to change the information for malicious purposes or to acquire access to data and information they were generally unable to view (Alhassan et al., 2016). The STRIDE model provided descriptive information and categorization and thereby ensured a comprehensive system-wide evaluation was performed (Abomhara et al., 2015; Seinfart & Reza, 2016).

Despite its benefits, the STRIDE model failed to provide an analysis of the significance of each attack. After threat classification, threats ranked in accordance with the level of risk they posed thereby differentiating threats with an increased risk of other threats with a relatively low risk (Seinfart & Reza, 2016). Stine et al. (2017) employed the STRIDE model to their study by using a questionnaire to generate the risk score of medical devices. One scenario in their study involved a total of three tests on medical devices (Stine et al., 2017). The risk scoring system

focused on application and utility within government and industry as a way in which to improve device security for healthcare organizations that must handle and maintain their security posture. Stine et al. indicated that this risk scoring system aids in supporting and better understanding the risk posture thus ensured to protect patient safety. Stine et al. also demonstrated that the risk to medical devices had an adverse impact on patient care. Although Stine et al. failed to categorize the types of attacks on medical devices, Seinfart and Reza (2016) posited that higher rating attacks occurred in the spoofing and tampering categories within the publish-and-subscribe architecture.

Alhassan et al. (2016) conducted a study on the threats inherent within electronic health systems. Countermeasures emphasized authorization and authentication purposes. In an effort to safeguard the availability, confidentiality, and integrity of health records, the researchers developed and proposed a threat model, which utilized the following two threat modeling tools: the STRIDE threat model and DREAD (Alhassan et al., 2016). In this study, the STRIDE model was used to identify possible threats that were then ranked based on the significant risk the threat poses to the system using scores from a threat risk rating model, DREAD (Alhassan et al., 2016). A combination of the STRIDE threat modeling and DREAD risk modeling resulted in a set of threats that were both identified and rated in order of decreasing risk to the electronic healthcare system (Alhassan et al., 2016). Proper identification and rating of threats are used to safeguard the convenience, trustworthiness, usability, and security of patient information. Moreover, the proper identification and rating of threats aid in identifying appropriate countermeasures that aim to minimize a prospective attacker's ability to misuse and exploit the electronic health system (Alhassan et al., 2016).

OWASP (Open Web Application Security Project)

As a not-for-profit organization, Open Web Application Security Project (OWASP, 2018) highlighted improvements in software security. OWASP provided information and knowledge about application security and software security to corporations, government-based entities, individuals, organizations, and universities. OWASP indicated that it aimed to "make software security visible" thereby enabling organizations and individuals to make well-informed decisions (para. 2).

National Vulnerability Database

Data regarding standard-related vulnerability management was contained within the U.S. government warehouse, the National Vulnerability Database (NVD) (National Vulnerability Database, n.d.; NIST, n.d.). Such data were represented based on the Security Content Automation Protocol, which facilitates compliance, security measurement, and vulnerability management (National Vulnerability Database, n.d.; NIST, n.d.). The NVD provided a list of Common Vulnerabilities and Exposures (CVE), as well as a Common Vulnerability Scoring System (CVSS) entries, and included a vulnerability summary for each exposure or vulnerability (Seale et al., 2018). The NVD listed vulnerabilities, impact metrics, misconfigurations, product names, security-based software flaws, and security checklist references (National Vulnerability Database, n.d.; NIST, n.d.; Zhang, Ou, & Caragea, 2015).

CVE. Seale et al. (2018) examined the role of CVE, a public dictionary developed by Mitre Corporation (2018), which encompassed a set of previously identified information security exposures and vulnerabilities. A list of cybersecurity vulnerability entries within the CVE contains a description, identification number, and a minimum of one public reference (NIST, 2018). A number of cybersecurity products and services available worldwide utilized CVE

entries (NIST, 2018). Seale et al. (2018) further proclaimed that CVE plays a quintessential role in determining identifiers of cybersecurity threats.

Common Vulnerability Scoring System (CVSS)

Cybersecurity vulnerabilities was modeled quantitatively using Common Vulnerability Scoring System (CVSS), which is a risk assessment framework responsible for "communicating the characteristics and impacts of IT vulnerabilities." Based on this risk assessment framework, impact scores were measured in accordance to three metric groups included base exposures, environmental exposures, and temporal exposures located in the /risk assessment of cybersecurity vulnerabilities (National Vulnerability Database: CVSS, n.d.; Seale et al., 2018). According to NIST (n.d.), CVSS also provided accurate, repeatable measurement in which users were able to see the vulnerability characteristics that produced the vulnerability score. Research literature posits that CVSS was commonly used to assess prioritization and severity of vulnerabilities and underlying vulnerability remediation activities (National Vulnerability Database: CVSS, n.d.).

Common Weakness Enumeration (CWE)

Common Weakness Enumeration (CWE) was developed to address problems associated with security weaknesses. A list of varying types of software weaknesses was created in an effort to "serve as a common language for describing software security weaknesses in architecture, design, or code. CWE serves as a standard measuring stick for software tools targeting these weaknesses there were manifestations aligned to unknown security requirements within networked medical devices. CWE was used as a common baseline of standard for weakness identification, mitigation, and prevention efforts (Overview – What is CWE, 2018, para. 1). Some of the most common software weaknesses included authentication errors, buffer

overflows, channel and path errors, code evaluation and injection, common special element manipulations, format strings, handle errors, insufficient verification of data, pathnames that were equivalent and traversal errors, randomness and predictability, resource management errors, and user interface errors (Overview – What is CWE, 2018).

The relevance of addressing all frameworks, models, and security tools was to show the value and capability of management and control to mitigate security risk for networked medical devices leading to harm. Preventive measures that were used to develop strategies for an organization reducing risk and assess the likelihood of an incident occurring. Analyzing controls eliminated the probability of exploitation.

TVA Model

The TVA model for risk assessment provided information regarding organizations ' information assets such as data, hardware, information, networking elements, people, procedures, and software, which were then placed against, perceived threats (Goodman, Straub, & Baskerville, 2008). Assets were defined as "information or data possessed and used by the organization as well as the systems that process, store, and transmit that information or data" (Goodman et al., 2008, p. 78). The assets and perceived threats were contained within a matrix and any suspected or known vulnerabilities are itemized. Threats such as an entity, object or person presented continuous danger and harm to an asset (Goodman et al., 2008). Identifying the assets, understanding the value of the assets to a given organization, and assessing assets affected by a compromise or the impact of a loss of assets can have on the organization (Goodman et al., 2008). Contrary to threats, vulnerabilities involved an action that typically occurs and yields potential harm (Goodman et al., 2008).

Confidentiality, Integrity, and Availability (CIA) Triad Model

Developed by Clark and Wilson in 1987, the confidentiality, integrity, and availability (CIA) model, provided guidance for information security policies within a given organization (Lefkovitz, Nadeau, Feldman, & Witte, 2017; Moghaddasi, Sajjadi, & Kamkarhaghighi, 2016). The Federal Information Security Management Act (FISMA) outlined the affiliation between information security and the CIA triad. Information security was the protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide support for the CIA triad (Moghaddasi et al., 2016; Rjaibi & Rabai, 2015). Confidentiality safeguards the restrictions of authorized users with access and disclosure to personal, private, and proprietary information (Moghaddasi et al., 2016). Integrity guards against modifications to information or destruction ensured information nonrepudiation, authenticity, and accuracy whereas availability ensured reliable access to all information in a timely manner (Moghaddasi et al., 2016).

Part of this study was to take the previous studies models, queries structures, and tables to use CIA-triad specific measurements for risk assessment. To show how it may be applied to impacted previous models first the projected categories of security vulnerabilities and threats as accomplished with STRIDE were evaluated in detail to provide context of how NIST RMF and the CIA triad were implemented. In application, the STRIDE and NIST RMFs project tables that classify assets, threat agents, and the identified threats. Abomhara et al. (2015) explained how these entities were projected, classified, and defined. The third type of entity, identified threats, was not represented as security threats in, which was unique from firm to firm, information system to information system, but they would be outlined in separate tables per identified threat.

Identification of threats (T), categorizes threats according to the following types: “authentication, authorization and access, privacy, as well as auditing and logging threats”

(Abomhara et al., 2015, p. 9). Adomhara et al. includes a description of the system or asset being assessed with the description. Adomhara et al. includes a description of the level of trust supporting threat agents depending on the description of the agent identified (TA and specific A-levels). The STRIDE model is represented in Adomhara et al. supporting the classification of profiling the threat related to identification of threats to a health organization.

The CIA triad was a risk assessment method that protects the identified assets with a structure of the following components, which could be likened to the components of hospital or healthcare facility security. The model was based on the following three foundational principles of security management that are defined as follows and represented in (Abomhara et al., 2015):

> *Confidentiality*: Maintaining the privacy of an asset; just as walls, solid doors, and window coverings provide security for the physical establishment of a medical facility, security controls and barriers prevent data breaches and the illegal or otherwise unauthorized access of patient data, software, device hardware, etc.
> *Integrity*: Maintaining the originality or the uniqueness of the asset's content. Just as alarm systems, security gates, and entry passes/key cards protect the facility's departments and laboratories and keep the hospitals' contents intact, security measures secure the content of the information system or the database that houses the electronic health records and other sensitive data.
> *Availability*: Maintaining the accessibility of the asset such that the contents of the asset are available to the people who need to use them in practice; for example, clinicians and other healthcare facility staff access areas of the hospital or treatment facility with key codes and key cards that keep unauthorized personnel out, and so security access controls such as login credentials and unique user IDs the track and monitor user activity can keep unauthorized personnel or the public from accessing sensitive, secured data.

As per the CIA triad requirements for predictive monitoring and security maintenance, there are three key activities, or functions that all evaluated devices should be able to perform. These functions included: monitoring, assessment and prioritization, notification, and finally, remediation which were a summarized according to Wilson and Rollman (2017). The definitions and requirements for efficacy of these functions, which indicates efficacy and security of the medical device, are categorized as follows:

> *Monitoring:* Active monitoring of security alerts from reliable external sources, customers, and any other external submitters. During this stage, the team actively monitors specific security notification email lists.
> *Assessment and prioritization:* Assessing, categorizing, and prioritizing the information system's vulnerabilities based on the identified level of severity, difficulty, and the potential of the threat agent to bypass the security measures to avoid the transmission of alerts; for this function, it is important to note that the level of difficulty refers to the precise degree to which any identified vulnerability can and might potentially be exploited, not to the level of difficulty it would take to fix the security issue.
> *Notification:* Notifying stakeholders of the information system—patients, clinicians, care providers, staff, insurance providers—and the submitter, also known as the threat agent, of the level of susceptibility or vulnerability of the system when the compromising action is identified and recognized by the security risk assessment which typically occurs when security controls have been violated or bypassed; notification should be performed within a short time frame, typically a 24-hour time period to remain ethical.
> *Remediation:* Implementation of the remediation action, either mitigating the security threat or reversing its damage, based on the unique classifications of susceptibility (Rao et al., 2017); the remedial action is performed within a short time frame, typically within a 24-hour time frame to prevent or mitigate damage. (Wilson & Rollman, 2017, p. 8)

Essentially, integrating the CIA triad model with the STRIDE model into the NIST RMF would mean a continuous assessment of the probability of security issues in addition to identifying the vulnerabilities of the information systems; in effect, assessing the likelihood of the security risk and projecting potential consequences if the appropriate security measures were not taken will provide a new model for measuring risk that maintains the firm continuity. In terms of medical devices, it would ensure that the device provider is proactively thinking about how to prevent the security threats rather than just mitigating them.

One of the best methods of representing this relationship between identifying security measures and projecting the probability of risk on a scale was to plot out a chart. Rather than categorizing the risk such as the STRIDE model does, this model would employ the use of a risk rating matrix. While there was little historical literature on risk management matrices, there was an influx of the topic in current study within the past 2 years.

Risk matrices were essential to the assessment of risk in qualitative data analysis. According to Baybutt (2017), when developing a risk rating matrix, the assigned subjective estimates of consequence severity and the probability, or likelihood values for an adverse event such as a data breach otherwise hazardous scenario to levels that correspond to predetermined values, or ranges of values of severity and probability for each consequence. For examples, consequences would be an impact on care facility personnel, patients, the equipment itself, etc. Some risk matrixes are simplified such as the example within Pasman's, (2016) article, which features a legend that assigns numerical value to the likelihood and consequence of each threat.

Despite the development of the CIA triad model, problems with availability were noted as more online facilities came into the market in the 1990s. A service deprivation attack by Morris Worm, an Internet worm, altered the perception of the Internet's reliability and security (Moghaddasi et al., 2016). Similar attacks focused on the availability and meaning associated with data security within a secured system (Moghaddasi et al., 2016). However, Rjaibi and Rabai (2015) suggested that a secure system was dependent on other basic security requirements inclusive of access control, identification, non-repudiation, and privacy.

Overall, studies about the use of medical devices in healthcare highlighted the importance and use of a cybersecurity framework as a countermeasure before exploiting patients and other networks (Cerkovnik, 2015; Seale, 2017). Cerkovnik created a proof of concept that was not peer-reviewed for using the classification, defined the vulnerabilities and threats, aligned a score based on risks in a database examining medical devices that were reported to the FDA due to failures potentially exposed various points of the network. Seale expanded on the database created by Cerknovnik to assess risk models to indicate cybersecurity vulnerabilities within network devices using real-world de-identified data. In this study, the focus was on the

importance of developing a model of cybersecurity based on experiences and perceptions of experts about two STRIDE threat model and the CIA triad guiding policy for implementing governance the use of networked medical devices.

Critique of Existing Research

Historical research risk assessments encompassed networked medical devices focused on leveraging a prototype database to apply countermeasures, which defended against weaknesses that exposed patient data, information, and networks connected to medical devices used for medical treatment purposes (Cerkovnik, 2015; Pardue et al., 2014; Seale, 2017). One of the models was a database-driven proof-of-concept for risk assessment. Pardue and his colleagues created a rational database using abstracts and categories for the design of the risk assessment process. Pardue et al. identified elements of the database model including threat, asset, vulnerability, and control and additional entities such as threat source, cause, and domain (Hoffman, Michelman, & Clements, 1978; Whitman, 2003). The risk assessment model database created by Pardue et al. was set up in a generic format to provide capabilities for any risk analysis to determine risk ranked based on appropriate security threats and the corresponding asset, controls, and vulnerability. Pardue et al. used Whitman's (2003) model and conducted studies using scenarios to leverage the TIA triad.

Cerkovnik (2015) created a use-case in support of a dissertation that was not peer-reviewed using Pardue et al. database-driven model with known data that was reported and published publicly within the FDA database. Cerkovnik expanded on Pardue et al.'s (2014) risk assessment database that had the potential to examine any asset leading to vulnerabilities. Cerkovnik specifically designed the database-driven model to focus on networked medical

devices. Cerkovnik added tblDevice to logically categorize devices in relation to its security attributes such as controls, countermeasures, threats, and vulnerabilities.

Seale (2017) made additional modifications that was not peer-reviewed to an existing relational database created by Pardue et al. (2014), which was later used to expand Cerkovnik's (2015) research which was not peer-reviewed, that resulted in the device management threat database model. Seale integrated modifications that focused on specific information regarding networked medical devices and called this portion of the database tblDevice and tblAsset. Seale used real-world data with the ability to perform cybersecurity risk assessment to create a use-case with medical devices. By creating queries in the SQL relational database, Seale generated the following threat model reports:

1. TVA model,
2. STRIDE threat model to categorize threat actions,
3. National Vulnerability Database (NVD) to summarize Vulnerability Summary for Common Vulnerabilities and Exposures (CVE) to identify vulnerabilities in cybersecurity,
4. Resource presenting the capability of reporting a mitigation ranking the severity of the risk based on controls.

By combining frameworks with threat models, Seale used this method to perform use-cases and identify the greater risk, largest impact, or greater exploits within networked medical devices that could lead to preventing future cyber-attacks. Seale focused on governing standards in the U.S. government published online as a resource for all additions to the relational database driven model.

Summary

In this literature review, the researcher evaluated historical risk frameworks and threat models used to determine weaknesses in network medical devices and how they could be leveraged to defend against thwarts to patients and healthcare systems. Chapter 3 includes a presentation of the gaps in the previous research that used threat modeling methodologies combining STRIDE and CIA in the proof-of-concept rational database that Pardue et a. created and Cerkovnik and Seale added for examined but not peer-reviewed (Cerkovnik, 2015; Pardue et al., 2014; Seale, 2017). The chapter also includes a description of how to address the alignment of this study with the appropriate model of effective countermeasures for cyber threats to networked medical devices in the healthcare industry in the United States.

CHAPTER 3. METHODOLOGY

Introduction

The specific problem that was addressed in this study was the lack of basis for developing effective countermeasures for cyber threats to networked medical devices leading to high possibility of security breaches (Pycroft & Aziz, 2018; Ransford et al., 2017). The purpose of this qualitative Delphi study was to support the development of a model with effective countermeasures for cyber threats with networked medical devices based on experiences and perceptions of Information Technology (IT) experts in the healthcare industry in the United States. The researcher used a qualitative Delphi design that addressed the alignment of this study to the required model of effective countermeasures for cyber threats to networked medical devices in the healthcare industry in the United States. The main phenomenon of interest for this study was the security of using networked medical devices in the United States.

The discussion in Chapter 3 focused on the specific methodology for this Delphi study. The researcher detailed the research methodology and design and discussed the basis for this study and the remaining portions of the chapter. However, before discussing the design and methodology, a restatement of the purpose and research questions are provided. A discussion of the credibility and dependability of the method for gathering information is shared. This is followed by a discussion of the data collection and data analysis. Finally, the researcher concludes this chapter with the discussion of ethical considerations.

Design and Methodology

The nature of this study was qualitative as the data collection employed sets of criteria that identified and categorized the results of pre-filtered data based on an objective and subjective level of risk, thus a qualitative approach was necessary. According to scholars, using a

qualitative methodology is effective and appropriate when exploring a phenomenon in-depth using data from relevant individuals (Lewis, 2015; Silverman, 2016). The phenomenon of interest for this study was the use of frameworks to address security supporting the use of networked medical devices in the United States. Moreover, the data of interest were experiences and perceptions of IT experts in the field of healthcare. The data were used to support a development for a model with effective countermeasures for cyber threats with networked medical devices based on experiences and perceptions of IT experts in the healthcare industry in the United States. Therefore, the qualitative methodology was appropriate to collect rich and thick data about the phenomenon in order to fulfill the purpose of the study.

A Delphi approach was the research design used for this study. This design is commonly used when there is a need to arrive at a consensus among experts in order to address a problem (Dalkey & Helmer, 1963). Using a Delphi method made it possible to simplify the complex problems (Dalkey & Helmer, 1963), such as cybersecurity of using networked medical devices in the United States. A qualitative Delphi method was the appropriate for this study in order to address the research question about the experiences in employing schemas to analyze security risks in medical devices. Specifically, the researcher used the Delphi method to support the development of a model with effective countermeasures for cyber threats with networked medical devices based on experiences and perceptions of IT experts in the healthcare industry in the United States.

Participants

Population

The target population of this study was IT experts in the field of healthcare. The IT professional was an expert in the field if he or she had been practicing the same career and IT

technical skillsets for at least 5 years. The skillsets included policies, settings, or the system management of medical devices. The population was chosen because these individuals were the ones in the center of the discussion of medical device information security. These individuals had the necessary IT career experience and depth of knowledge about the topic, which was essential to addressing the research question. Participant expertise was ensured through the eligibility criteria for recruitment. Therefore, the most appropriate individuals, IT experts in the field of medical devices, were recruited as participants.

Sample

The researcher used purposive sampling to recruit the participants in Positly.com. After identifying an initial set of participants, snowball sampling was used to recruit participants with the eligibility criteria (Griffith, Morris, & Thakar, 2016). Purposive sampling is a non-probability-sampling technique commonly used in qualitative data collection (Etikan, Musa, & Alkassim, 2016). Purposive sampling is a kind of participant recruitment process wherein specific groups of individuals are targeted based on a set of eligibility or inclusion criteria (Barratt, Ferris, & Lenton, 2014; Etikan Musa, & Alkassim, 2016). Through purposive sampling, the researcher collected information from people with relevant information that addressed the research question developed by the researcher. The eligibility criteria were used to filter potential participants in Positly.com. Participants were asked to send the invitation link to other individuals eligible for the study in order to gather more participants which reflected snowball sampling. This sampling technique was appropriate for this qualitative Delhi study.

When purposive sampling was implemented, the participants met a set of eligibility criteria. The eligibility criteria used for recruitment of IT experts included the following: (a) working as IT leaders in organizations using networked medical devices, (b) responsible and

accountable for the security of data involved with the use of networked medical devices, (c) has been in the cybersecurity field for at least five years, (d) and has professional experience ensuring cybersecurity in hospital that use networked medical devices. Only those who satisfied all the eligibility criteria were included in this study as participants.

Research on Delphi methods suggested that having a large sample size for a Delphi method study is time consuming and impractical because of the difficulty in achieving a consensus among the sample (Lyons et al., 2017; Ozier, 2012). The basis for identifying the sample size in qualitative studies was to the point of data saturation, which was the point in data collection and analysis that met the following criteria: (a) no more new information can be identified; (b) no new codes could be classified; (c) no new themes emerged (Fusch & Ness, 2015; Tran, Porcher, Falissard, & Ravaud, 2016). The usual sample size for Delphi studies is between 15 to 20 respondents in order to reach data saturation (Dalkey & Helmer, 1963). Moreover, for the first round of the Delphi method, the researcher knew if data saturation was reached. The researcher collected data from 15 IT experts for this Delphi study.

Participant Selection

The researcher used Positly.com, which was used to explore and identify IT experts who met the eligibility criteria, to facilitate the recruitment of participants. The researcher obtained IT experts who had active Positly.com accounts. The IT experts were from facilities using networked medical devices on patients. The IT experts were also asked to send the invitation link to other potential participants within their network. These experts were part of an interview process, which was the main data collection method for this study.

The researcher began recruiting participants by sending email invitations to the Positly.com accounts of IT experts working in facilities using networked medical devices on

patients. In the invitation email, the information about the purpose and significance of the study was provided to introduce the study to the potential participant. The researcher also included information about the scope of participation (e.g., multiple rounds of data collection) found in Appendix A. Those who agreed to participate used Positly.com, met the eligibility criteria, and had access to the digital informed consent form to sign. Only those who digitally signed the consent form had access to the qualifying questions found in Appendix B were considered as participants of the study and could receive monetary compensation ($50) for participation.

Protection of Participants

The researcher was responsible for protecting participants of the study (Wong & Hui, 2015). The researcher ensured that participants remained protected from possible risks and harm that may arise during data collection, analysis, and reporting of the study. The informed consent included information about important steps for protecting participants in the study. The contents of the consent form were important to ensure that participants were informed of their roles and rights as respondents to the study. All participants received a copy of the informed consent to gain information about the scope of participation, minimal risks, and other information (e.g., purpose of the study, confidentiality measures, and audio-taping procedures). Through this process, participants were protected against harm and risks during participation.

Setting

For this study, the researcher collected data from interviews with 15 IT experts in the field supporting healthcare and networked medical devices. Those who were disqualified either never showed for the interview, did not answer all the questions which provided gaps in experience and data, or disenrolled from the schedule on the calendar. Round One lasted roughly 30-60 minutes and the researcher asked the questions found in Appendix A. Round Two

captured all 15 participants, lasted roughly 30-60 minutes, and included reviewing the emerging themes Appendix B discovered in Round One. During Round Three, which included the group and lasted 30 minutes, the saturation of data has been reached. Data were analyzed using thematic analysis for each round of data collection until data saturation was reached.

Analysis of Research Questions

The problem of the study was about the vulnerability of medical devices to cyberattacks (Ankarali et al., 2014; Pycroft & Aziz, 2018; Ransford et al., 2017). Ninety-four percent of healthcare organizations have been victims of cyberattacks related to the use of medical devices and the infrastructure to support these devices (William & Woodward, 2015). The specific problem addressed in this study focused on the collecting data from IT expert's experiences with effective countermeasures aligned to cyber threats involving networked medical devices leading to high possibility of security breaches (Pycroft & Aziz, 2018; Ransford et al., 2017). Based on the problem, the research question was about how to develop effective countermeasures for cyber threats to protect networked medical devices. For this study, the researcher focused on exploring the lived experiences of IT experts in the field of medical devices to address the problem. This study had only one research question: What are the relevant experiences in employing a schema to analyze security risks in networked medical devices? This research question was aligned with the topic and problem therefore, the question was appropriate for this study. To answer the research question, the main source of data was semi-structured interviews in multiple rounds until saturation of data was reached. The researcher inquired about the experiences of IT experts to gain deeper understanding of the phenomenon and addressed the research questions of the study.

As part of the data preparation process, the researcher conducted a review of the interview guide. Conducting an instrument review was used to improve the validity and improve credibility of the study (Balkar, 2015; Leung, 2015; Lincoln & Guba, 1985). Three reviewers with at least five years of professional experience in cybersecurity, medical devices, and qualitative studies, evaluated the interview guide. Moreover, the reviewers who evaluated the data collection instrument were not participants in the study.

The instrument review was conducted such that the panel members were together via conference a call to discuss their comments about the data collection instrument. During the instrument review, the reviewers evaluated the interview guide questions that the researcher developed using the following criteria: (a) use of appropriate words, (b) development of appropriate structure of sentences, (c) and development of complete questions to address the research questions of the study comprehensively. The reviewers assessed the items together as a group and came up with a set of comments and feedback in relation to the criteria for the evaluation. The reviewers provided recommendations for possible changes that the researcher considered in order to improve the researcher-developed interview questions. The researcher made the necessary changes to the interview guide before conducting the remaining data collection for this study.

Credibility and Dependability

Credibility and dependability were achieved with the trustworthiness through the exploration of individuals experiences describing detail about a unique phenomenon. Achieving credibility was demonstrated with the understanding of the research method and dependability was demonstrated by applying and conducting data analysis over time and conditions (Cypress,

2017). The plausibility of findings was enhanced via the data collected throughout the duration of the study.

The researcher used purposive sampling to target IT experts and interviews to collect the data. Leveraging the responses of participants to the same research question observing the Theory of actions and the behaviors participants respond. Categorizing the probability and consequence in the data analysis with the aforementioned levels and categories will make the results appear generalized and limit the specificity which would make it difficult to apply these results to other types of security issues in non-medical information systems. Credibility was also supported through the iterative nature of the Delphi – participants were given multiple chances to clarify and correct results as the study progresses.

Data Collection

The procedures for data collection in this research was conducted using the Delphi method. Interviews were conducted in multiple rounds, until saturation was reached during data collection based on a review of Delphi research (Birko et al., 2015; Ozier, 2012). In the first round, participants answered open-ended questions. In the second round, the researcher provided the participants with a summary of the emerging themes from analysis of the first-round responses and requested revisions to these themes as guided by the participants' experience and attitudes. In the third round, participants were asked to provide example experiences that illustrated the emerging themes as revised by analysis of the second-round responses. Through the multiple rounds of questioning, participants arrived at a consensus. Based on these rounds of questioning, the researcher developed a final model that addressed the research question.

In the first phase of data collection, participants were selected who met the criteria for eligibility that undergone in an interview using the interview guide. Interviews were conducted

using a conference call. Each interview lasted for 30 to 60 minutes. All interviews were audio-recorded, as explained to the participant through the informed consent form. The questions in the interview were open-ended. The participants were asked to provide comprehensive answers to these questions. In some parts of the interview, the participants were asked follow-up questions to collect more information about the answers of the participants which gained better understanding of the information. The researcher processed the answers from the interviews. Specifically, the researcher provided an analysis of the answers of all the participants in the interview guide. The summary presented in the second round.

After the first round of data collection, the researcher presented the summary of the emerging themes from analysis to the participants. The purpose of the semi-structured interview in the second round of data collection allowed the participants to review possible issue in their answers to the initial interview and clarified the information through an explanation. The researcher provided a list of items in the second iteration of the Delphi method. Each item represented an emerging theme. Participants narrowed down the potential solution to the problem through additional input. The researcher also asked participants to rate the items from the first-round in order of precedence.

In the third round, the researcher asked participants to provide examples of experiences that illustrate the emerging themes as revised by analysis of the second-round responses. The purpose of the third round was to confirm the consensus between the participants. Because of time and resource constraints, the researcher was limited to three rounds. The consensus was reached after the third round when all the expert participants agreed on the themes that would be reported as the results of the study. However, the researcher noted that the final results were

based on consensus of participants. After conducting each data collection phase, the researcher wrote a transcript of the interviews and a soft copy of the answers to the online questionnaire.

Data Analysis

The data analysis for this study was accomplished after each round of questioning was completed. As is the case with the Delphi methodology, the researcher then used responses that constructed the reality of those participants to represent the reality of those within the real-life positions and roles (Dalkey & Helmer, 1963). With each level of questions, the researcher identified emerging themes that provided insight into the research questions. Then, the researcher formed additional questions that were needed to gather additional information until one arrived at a consensus (Lindstone, 1977). Overall, the researcher had three rounds of data collection. For each round of the data collection, the researcher conducted analysis. For the first round of data collection, the researcher analyzed the data using thematic analysis with the following steps: (a) data familiarization, (b) code development, (c) theme development, (d) theme revisions, (e) theme finalization, and (f) report generation (Terry, Hayfield, Clarke, & Braun, 2017). For the first step, the researcher read the data twice. The researcher highlighted important words and word segments that have a direct association to address one research question. During the first phase, the researcher considered the three elements of the theory of reasoned action (TRA) in order to understand the perceptions of participants. In the second step, the researcher coded the data. The researcher assigned a code to each highlighted phrase to identify how they related to the research question. The researcher based the codes on the concepts included in TRA. In the third step, the researcher grouped similar codes to form a theme that must relate between the research question. In the fourth step, the researcher eliminated negligible themes, combined smaller themes, or decomposed large themes, as needed. The themes were related to the three

elements of TRA. For the fifth step, the researcher developed a definition for each theme. However, the researcher did not perform generation until the analysis for the three rounds was completed.

To analyze the data from the second phase of data collection, the researcher graphed the frequency distribution of the ratings for the different themes. The researcher also searched for existing literature that supported the findings of the study from the themes and frequency distribution. Comments and opposing views that emerged in the second phase were also noted and carried over to the third round.

In the third round, the results were graphed. The frequency distribution of the ratings from the second round was also generated. The researcher also graphed the frequency of occurrence of the answers of participants about the experiences that illustrate the emerging themes as revised by analysis of the second-round responses. The researcher also gathered information from the existing researches to support the findings of the study. The difference in the findings was presented as a line graph of movement of opinion from second to third rounds. The detailed discussion of the findings presented in Chapter 4.

Instruments

The instrument review was conducted wherein the panel members joined on a conference call via dial-in due to geographical location to discuss their comments about the data collection instrument. Therefore, the chosen reviewers, who were in different geographical locations, agreed on a time to join a conference call to conduct the panel discussion.

The Role of the Researcher

As part of the data preparation process, the researcher conducted a review of the interview guide. Conducting an instrument review needed to be improve the validity and

improve credibility of the study (Leung, 2015; Balkar, 2015; Lincoln & Guba, 1985). The researcher asked multiple reviewers with at least 5 years of professional experience from each of the following fields to evaluate the interview guide: cybersecurity, medical devices, and qualitative studies. Moreover, the reviewers who evaluated the data collection instrument were not participants in the study.

Research Developed Guiding Interview Questions

During the instrument review, the reviewers evaluated the questions in the interview guide using the following criteria: (a) use of appropriate words, (b) development of appropriate structure of sentences, and (c) development of complete questions to address the research questions of the study comprehensively. The reviewers assessed the items together as a group and came up with a set of comments and feedback in relation demonstrating a verbal behavior (Dixon & Horton, 1968) to the criteria for the evaluation. The reviewers provided recommendations for possible changes that the researcher considered in order to improve the questions in the interview. The researcher made necessary changes to the interview guide before conducting any data collection for this study.

Ethical Considerations

Ethics are one of the important considerations in a study involving human participants. There are numerous ethical implications for a qualitative study for any kind, but especially one that involves medical data of any kind. While patient data itself was not being accessed, which is potentially an ethical and legal liability if not handled correctly, the data from the medical devices being evaluated could include patient-reported evidence of equipment failure (Hollis, 2016). When it comes to the results of the study and recommendations moving forward in the discussion, the importance of improving measurement of security control vulnerabilities and risk

assessment procedures was the utmost priority, as the goal of this research was to improve the current models (Ozair, Jamshed, Sharma, & Aggarwal, 2015). As it pertains to the analysis and discussion, the risk assessment matrix was designed to reduce, yet not eliminate uncertainty in risk assessments because they are merely part of the assessment (Peace, 2017).

An important measure for ensuring ethics for a research was informed consent. In the research informed consent, the researcher provided a digital informed consent to potential participants. The participants read the contents of the digital form to become aware of the rights and responsibilities associated with participating in the study. The participants who agreed to the contents of the study digitally signed and sent a digital approval to schedule interviews with the researcher through a calendar invite via email. Only those who digitally signed the consent form were considered as participants in this study.

Another ethical issue was confidentiality. The researcher ensured that the identity and other information from and about the participants of the study remained confidential. The researcher used pseudonyms to replace the real names of the participants. No identifiable information was collected from the participants. All data, such as notes, digital consent forms, questionnaires, protocols, and the like, collected during the study were stored in a secure location, which was a safe that is locked in the researcher's private office. Data will be kept for 5 years after completing the study. After 5 years, all data will be destroyed through burning.

Summary

The focus of the discussion in Chapter 3 was the methodology to support with creating a model for developing effective countermeasures for cyber threats to networked medical devices in the healthcare industry in the United States. Based on the discussion in Chapter 3, the researcher collected data from 15 IT experts in the field of healthcare using purposive sampling.

The participants confirmed the following eligibility criteria: (a) working as IT leaders in organizations using networked medical devices, (b) responsible and accountable for the security of data involved with the use of networked medical devices, (c) have been in the cybersecurity field for at least 5 years, and (d) have professional experience on ensuring cybersecurity in hospital devices. Data were collected through interviews and questionnaires in multiple rounds. In the first round, participants answered open-ended questions. In the second round, the researcher assessed the items summarized by the investigators based on the information provided in the first round. In the third round, participants assessed and made comments about the findings from the previous round. Data collected through thematic analysis for the first round and descriptive analysis for the second and third round. The discussion of the findings is presented in Chapter 4.

CHAPTER 4. RESULTS

Introduction

In the United States, over 300,000 patients had embedded networked medical devices, and approximately 2.5 million were at risk with life-threatening situations that were dependent on such devices (Ankarali et al., 2014). However, these medical devices were vulnerable to cyberattacks (Ankarali et al., 2014; Pycroft & Aziz, 2018; Ransford et al., 2017). Approximately 94% of healthcare organizations were victims of cyberattacks on medical devices and the infrastructure to support these devices (William & Woodward, 2015). Moreover, there was a lack of basis for developing effective countermeasures for cyber threats to networked medical devices leading to the high possibility of security breaches (Pycroft & Aziz, 2018; Ransford et al., 2017). Thus, the purpose of this qualitative Delphi study was to support in creating a model for developing effective countermeasures for cyber threats to networked medical devices in the healthcare industry in the United States. Given this purpose, the primary research question driving this study was: What are the relevant experiences in employing a schema to analyze security risks in networked medical devices?

Chapter 4 includes a discussion of the process of data collection and analysis. Subsequently, the chapter is structured by the major themes and the corollary subthemes. Finally, in the chapter summary, the researcher ties the themes together into a coordinated set of findings and concludes with a summary.

Data Collection Results

The procedures for data collection in this research were conducted using the Delphi method. Profiling participants were required to answer three significant prequalifying questions (see Appendix A) that helped eliminate those who were not considered IT experts experienced

with networked medical devices. Interviews were conducted in three rounds, which were a sufficient number for data collection based on a review of Delphi research to reach desired consensus (Birko et al., 2015). In the first round, participants answered open-ended questions developed by the researcher found in Appendix A. In the second round, the researcher provided the participants a summary of the emerging themes found in Appendix B from analysis of the first-round responses and requested revisions to these themes as guided by the participants' experience and attitudes. In the third round, participants provided examples of their experiences that illustrate the emerging themes as revised by analysis of the second-round responses and consensus to end with a data saturation.

Prior to participants being interviewed, the researcher used an online digital platform (see Appendix A) to seek IT experts with experience in employing a schema to analyze security risks in networked medical devices. There were three qualifying questions that if answered appropriately, allowed the participant to move forward to schedule an interview. The researcher created Table 1 to show all participants met the criteria of working within the United States as IT experts in the field of healthcare, having 5 years of relevant experiences in employing a schema to analyze security risks with networked medical devices, having skillsets with policies, settings, or the system management of medical devices, and employing schemas and frameworks as countermeasures to address security risks in medical devices.

Table 1 Participant years of experience.

Participant	Years' Experience
P1	10
P2	7
P3	15
P4	12
P5	20
P6	5
P7	8
P8	7
P9	6
P10	27
P11	7
P12	15
P13	15
P14	10
P15	8

In the first phase of data collection, the individuals who met the eligibility criteria for participants who interviewed with the researcher using the research develop interview guide (see Appendix A). Interviews between the researcher and selected individuals were conducted via conference call. All interviews were transcribed, as explained to the participant through the digital informed consent form. Each interview lasted between 30 to 60 minutes due to the experts explaining their experience with networked medical devices. The questions in the interview were semi-structured open-ended and the participants were asked to provide comprehensive answers to these questions.

After the first round of data collection, the researcher presented the summary of the emerging themes from the analysis to the participants. The purpose of the semi-structured interview in the second round of data collection was to allow participants to review possible issues in their answers to the initial interview and clarify the information through an explanation.

The researcher provided a list of themes in the second iteration of the Delphi method. Each item represented an emerging theme. Participants performed an analysis of emerging themes from the first-round responses and provided revisions to these themes based on the participants' experience and attitudes through additional input.

In the third round, the researcher asked participants to provide example experiences that illustrated the emerging themes as revised by analysis of the second-round responses. The purpose of the third round was to confirm completeness and consensus in the responses from the participants. Because of time resource constraints, the researcher limited the rounds to three to attain saturation and further collection of data was unnecessary. After conducting each data collection phase, the researcher wrote a transcript of the interviews and a soft copy of the answers to the interview guide and emerging themes.

Data Analysis and Results

The data analysis for this study was complete after each round of questioning. As is the case with the Delphi methodology, the researcher then used responses to construct the reality of those participants to represent the reality of those within the real-life positions and roles (Dalkey & Helmer, 1963). With each level of questions, the analysis took responses and identified emerging themes to provide insight on the research questions. Then, the researcher formed additional questions (see Appendix A) that required additional information for completeness and saturation of data (Lindstone, 1977).

Overall, the researcher completed three rounds of data collection and conducted an analysis after each round. For the first round of data collection, the researcher analyzed the data using thematic analysis with the following steps: (a) data familiarization, (b) code development, (c) theme development, (d) theme revisions, (e) theme finalization, and (f) report generation

(Terru et al., 2017). During data familiarization, the researcher read the data twice as well as through the process of transcription that was manually completed. The researcher highlighted important words and phrases with a direct association to the research question from the transcriptions. During the first phase, the researcher also considered the three elements of the theory of reasoned action (TRA) which are the persons intentions in relation between their attitudes and behaviors during actions in order to understand the perceptions of participants.

For the second step, the researcher coded the data manually with a T, R, or A. The researcher assigned a code to each highlighted phrase to identify how they related to the research question. The researcher ensured to base the elements on the concepts included in TRA. In the third step, the researcher grouped similar elements to form a theme that related to the research question. In the fourth step, the researcher eliminated elements and themes by combining smaller themes, or decomposed large themes, as needed manually. For the fifth step, the researcher developed a definition for each theme.

To analyze the data from the second phase of data collection, the researcher analyzed the frequency distribution of the ratings for the different themes. The researcher also searched for existing literature that supported the findings of the study from the themes and frequency distribution. Within the second round, all the participants agreed with the topics aligned to the cyber threats. Within the second theme, all participants commented on the subthemes due to not every place having a budget for automated tools or the ability to track every asset. In the third major theme, all participants agreed to the subthemes, with some comments on the wording, as well as ideas that eliminated. All participants agreed with the major and subthemes in the fourth major theme. Comments and opposing views that emerge in the second phase were noted and carried over to the third round.

Within the third round of interviews, data were analyzed by thematic analysis, aligning answers about participants' experiences within the revised themes and subthemes.

Results

The sample size of participants who qualified for this study is represented in Figure 1 created by the researcher. The sample included 15 IT experts who participated as represented with a P and number as shown in Table 1 in this study. The participants had relevant experiences in employing a schema to analyze security risks in networked medical devices. Purposive sampling was the technique used in this qualitative data collection as used by other researchers (Etikan, Musa, & Alkassim, 2016). Purposive sampling was used through Positly.com to recruitment specific IT experts targeted based on a set of eligibility or inclusion criteria (Barratt, Ferris, & Lenton, 2014; Etikan Musa, & Alkassim, 2016; Gignac, & Szodorai, 2016). Through purposive sampling, the researcher collected information from people with relevant information that addressed the research questions of the study; 15 out of P15 participants qualified for the study. Figure 1 shows 38% participants qualified while 62% were disqualified for not meeting the participation criteria.

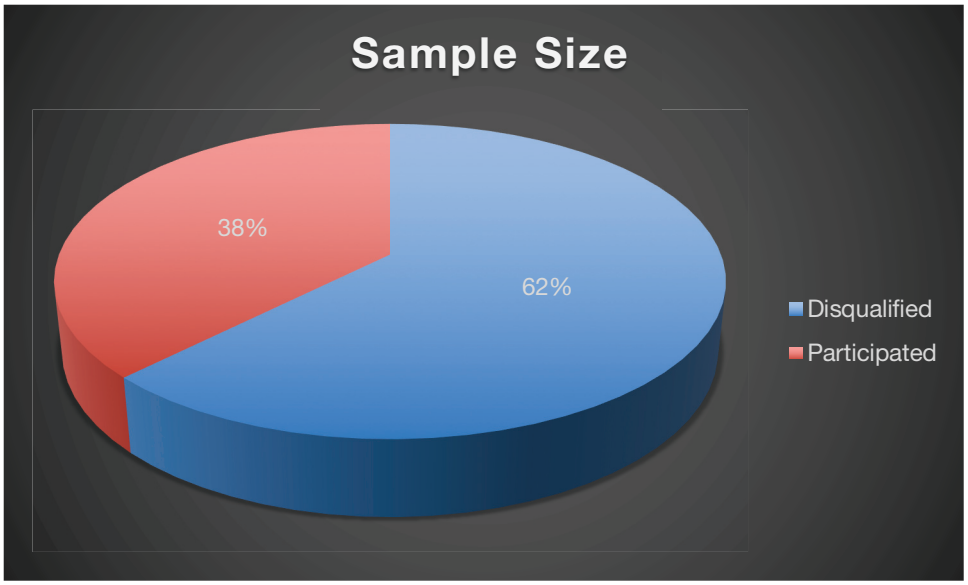

Figure 1. Sample size quota.

Major theme 1: Cybersecurity threats encountered. As seen in Figure 3, the first theme included six subthemes within parameters that focused on IT experts' experience with how the threats discover in networked medical devices. These subthemes placed within the order that discover to be more frequent from higher to least answered. Participants identified these threats from a personal perspective with configuration management, wireless and Bluetooth connections, Internet of Things, Data breaches, insider threat, and asset management as cybersecurity threats in networked medical devices.

Subtheme 1a: Configuration management. Configuration management refers to change control and documentation of a new baseline by using the standard operating procedure on how to approve, document, implement, initiative, and release changes. Planned changes include hardware or software updates or the implementation of additional modules, and may include changes to accessories, cables, computer hardware, database, documentation, network hardware components, and operating systems. In the first round, six participants listed configuration

management as a cybersecurity threat: P3, P7, P10, P13, P14, and P15. All participants agreed to this threat in the second and third rounds of interviews.

Subtheme 1b: Wireless and Bluetooth connection. Wireless and Bluetooth connection was the second most frequently discussed potential for cybersecurity threats. Participants described the ways in which attacks occur through the wireless connection between the medical device and the proxy device it communicates with it. Five participants in the first round of interviews, and all in subsequent interviews, agreed to this subtheme as a threat. As P6 explained:

> Networked medical devices have the same wireless protocols as other IoT devices like Bluetooth and Wi-Fi. When I think about cyber threats, I think about the medical devices that ingest data and provide information to providers over the air to other networks.

This threat was similarly described by P8:

> A smart device is an electronic device, generally connected to other devices or networks via different wireless protocols such as Bluetooth, Wi-Fi, etc. To improve technology, medical devices and smart homes, being able to control things from your smart device makes life more efficient. Consequently, medical devices/data connected to the smart devices, the same vulnerabilities that exist in smart devices exist with medical devices.

Subtheme 1c: Internet of things. The third cybersecurity threat decided upon by the participants in three rounds of interviews was the internet of things (IoT). Such a threat marked by the Internet connectivity of devices. This threat, particularly regarding medical devices, involves ubiquitous data collection, consumer data, and heightened security risk that could potentially be unexpected for a patient.

Subtheme 1d: Data breaches. Data security breaches were agreed upon as a potent cybersecurity threat to medical devices. As P5 explained, “Cyber threats seem to be an easy target with patient data and provide information to providers over the air to other networks.” The participant added, “The threats are with the compromise the health of the patient through the data

concerning their treatment." P11 described the threat as, "intrusion with medical devices impeding data breaches or leakage," and P9 stated "data loss" was a cybersecurity threat.

Subtheme 1e: Insider threat. Insider threats were agreed upon as a cybersecurity threat that could adversely affect the healthcare industry. While insider threats may be malicious or unintentional in nature, the participants in this study did not specify which they found to be more of cybersecurity risk. Unlike the previous subthemes, this threat was specifically about individuals, particularly those within or connected to the healthcare industry.

Subtheme 1f: Asset management. The final subtheme to emerge was asset management. Such a threat would include how hardware and software are managed, inventoried, tracked, and corrected on the network. If this is incorrectly complete and frequently, unauthorized devices could grant access to the network.

Major theme 2: How to address cybersecurity threats. The second theme, "How to Address Cybersecurity Threats," included four subthemes within parameters that focused on applying protective mechanisms that could help provide a defense for networked medical devices. IT experts who were participants identified how to address these cybersecurity threats from a personal perspective by controls assessment, automated technology, policy changes, and security awareness and training.

Subtheme 2a: Controls assessment. The most frequent response in the first round of interviews (10 out of 15 participants) and agreed to be all participants in the second and third round of interviews, controls assessment, as P2 explained, involves, "Independent and automated security controls assessment." P5 noted that internal and external audits could do this such an assessment:

> We are performing more internal and external audits for identifying vulnerabilities and potential security threats. Healthcare IT that monitors with security tools helps to identify

> the threats and risks and report them back to the manufacturer so we can try to incorporate and eliminate the treat when building these devices.

Two other participants (P6, P8) also specifically pointed to the use of both internal and external audits as a method of control assessment. P9 suggested "multi-Factor Authentication being required on all mobile devices," while P10, along with P15, described the need to "role access control." Also noted, two participants (P1 and P12) specifically said that any controls assessment should be "independent" from the organization. P13 noted the importance of such an assessment:

> By applying security controls to all our infrastructure that supports the networked medical devices as well as the medical devices we use, we see efforts of malicious attacks, but we prevent them with monitoring tools. Security controls also protects data from being exploited and changes in patient medical therapy from being changed and relayed to their devices, causing harm to the patient.

Subtheme 2b: Automated technology. The second method for addressing cybersecurity risks is the use of automated technology. As P6 said, "robust monitoring tools help to identify threats and risk" should be used. This sentiment was agreed upon by all the participants. P4 suggested "auditing and automated tools to monitor," and P12 suggested using "automated tools and allow for AI to report." P11 noted their firm already used such an approach: "We use AI and Big Data tools to enhance the administration of medical devices and patient care to protect and safeguard patient data." Likewise, P8 described the specific automated tools used to address cybersecurity threats: "With the tools in place we had in place, Armis sent us alerts that are built in our schemas to provide us alerts recognizing failures. Attacks are discovered by Splunk recognizing if something is knocking at our door that is unrecognizable."

Subtheme 2c: Policy changes. Four participants in the first round of interviews, and all in the subsequent rounds of interviews agreed that policy changes could be a useful way to prevent cyber-attacks. These policy changes would vary but might include a system and communications protection policy to address compliance, coordination among other entities,

management commitment, purpose, roles and responsibilities, and scope. Overall, this subtheme pointed to the need for the implementation of a comprehensive security governance policy in organizations, and the willingness to change and alter policies if they are subverting cybersecurity efforts.

Subtheme 2d: Security awareness and training. The final measure agreed upon by all participants was security awareness and training. As P2 described, such a method would require "security awareness for patient and providers [and] training for cybersecurity section of the hospital focused on tools we use." This method, then, is a two-step process: awareness, which may include patients, providers, and any third-party users, as well as training, particularly for those involved in the security of both the hospital and the device. Security awareness may include such measures as a perceived threat, safeguard effectiveness, safeguard cost, and self-efficacy.

Major theme 3: Medical devices and cyberthreats. The third theme (Figure 3), "Medical Devices and Cyberthreats," included six subthemes within parameters that focused on what the IT expert who was participants identified when analyzed issues that they faced with networked medical devices. The first subtheme "Security Measures" included four items that, if implemented or applied, would be the top four considerations to protect networked medical devices at the first level of defense. The second subtheme, "Cybersecurity Failures Experienced," included the three most prevalent items found to be the most experienced with the IT experts. The third subtheme, "Addressing Cybersecurity Failures," included the three items that were most prevalent found in failures with networked medical devices. The fourth subtheme, "Reasons for Failure," included the three items that were found to be the most reasons found by IT experts within networked medical devices. The fifth subtheme, "Prevention of Failures,"

included only one item that all IT experts reported, as active monitoring networked medical devices would actively prevent cyber threats with networked medical devices. The sixth subtheme, "Analytical Tools for Security Risk," included four items that IT experts used when performing analytical risks when actively monitoring networked medical devices.

Subtheme 3a: Security measures. Within this subtheme of security measures specific to medical devices, participants agreed on four items that, if implemented or applied, would be the top four considerations to protect networked medical devices at the first level of defense. The first was Physical, Operational, Management, Technical controls assessment (five in the first round of interviews, agreed on by all in Rounds 2 and 3). Such measures (or countermeasures) are used within an organization's information system to protect the integrity, confidentiality, and availability of the system and its information. However, given that each organization must determine its own appropriate set of security controls, the participants did not give specific parameters to this assessment.

The second security measure was policy, originally cited by four participants, and subsequently agreed to by all participants. These participants advocated for a Security Technical Implementation Guide (STIG), which would offer a way to standardize security protocols in all areas of cybersecurity. As P3 noted, it is essential to "establish a policy to set STIGs creating a baseline." P10 concurred, noting that this policy is only where an organization should *begin* rather than an end: "STIGs as a floor, not the ceiling."

The third security measured encryption. P3, as well as P10 and P15, described this as "Full disk, OS and app encryption set at BIOS level." Finally, participants described countermeasures that included blocks and controls. As P3 described this:

> No admin[sic] privilege of any user; removed access to all browsers; import via USB blocked, only export USB for certain role-based functions, Blue tooth off, set all clinical

> clients to only access single IP with client-server. No store local (increase back up cycle to limit data loss), et al.

P7 agreed, also adding countermeasures that included, "increased configuration controls or adding compensating controls to limit all non-mission functionality or access." P15 added, "Eliminate privileges, eliminate browser access, block all external ports such as USB and HDMI, only export role basked control."

Subtheme 3b: Cybersecurity failures experienced. This subtheme included three items that were found to be the most experienced cybersecurity failures to have occurred with the IT experts: malicious attacks, Denial of Service (DoS) attacks, and mechanism failure. P7 described one instance of a cyber-attack, saying, "Found malicious software post transient between vendors." The same incident described by P10, as well as P15, who added that "notifications of intrusions [were] alerted on Splunk." P13 noted that they experienced "Malicious attacks with exploiting vulnerabilities through software patches." Furthermore, P14 added having experienced, "malicious attacks like causing the battery to die through the exploitation of the software."

Denial of Service (DoS) attacks also cited by two different participants. P2 noted, "Common IoT aligned to DoS and human errors when messing with settings causing malfunctions to the devices." P3 also explained a potential threat (but ultimately failed attack): "Have had attempted intrusions (SQL, DOS) for Enterprise level EHR, but not when networked clients were operational. Addressed enterprise intrusions by terminating public facing access to servers, no data loss or compromise."

Mechanism failure was the third most cited instance of cybersecurity threats to medical devices. P10 stated, "We experienced communication failures as you see in the news with battery malfunctions and cyber threats. This was another vendor as we bought out the product to correct

the deficiency on the product." P11 said, "A security failure occurred on an insulin pump." Moreover, P8 related the problem to Bluetooth connectivity as well, saying, "When the medical devices are picking up multiple Bluetooth devices it could become even more vulnerable and potentially become inoperable."

Subtheme 3c: Addressing cybersecurity failures. In this subtheme, IT experts described three measures that are directed when failures occur with networked medical devices occur. The first is a lockdown and monitoring of devices. As P3 noted, when an attack occurred, they locked down the device by "terminating public facing access to servers," which allowed for "no data loss or compromise." P2 also cited, "lock down the device and monitor for changes." Likewise, P11 explained, "With tracking patterns of historical failures, monitoring the behaviors, we were able to contain the data and notify the patient there was an alert on the device."

The second measure is to report failure. P4 succinctly noted, "if a failure occurs, report it through the FDA website." P5 also discussed the importance of reporting, particularly to and through the FDA: "When we learn of a cyber threat or malfunction, we follow protocol with FDA and correct and run tests for the reported vulnerability to the device." P14 added that reporting should also occur to the vendor, saying, "Splunk provides alerts, we have an incident management plan, and a part of that is to report it to the vendor and FDA."

Finally, experts suggested the use of automated tools to help preempt any cyber-attacks that may happen in the future. As P13 suggested, "Implementing automated tools such as Armis and AI with Crowdstrike and IBM tools at a previous place of work." P6 added:

> Armis covers the comprehensive networked medical device as it has asset discovery, device type, location, software, vulnerabilities, services used, connection history for forensics, and passive monitoring, which does not disrupt devices. With our continuous monitoring in place, we stay alert for the hospital.

The specifics of these automated tools are a part of the discussion in more detail in subsequent subthemes.

Subtheme 3d: Reasons for failure. Within this subtheme, IT experts listed the three most experienced reasons for failure within networked medical devices. The first is device management. There can be multiple ways in which such devices fail. P4 noted that a "malfunction occurred with a battery." For P11, "failure occurred in public with Bluetooth." P5 also noted, "management of the device may not be properly handled throughout the lifecycle of the device. If a patch is not applied to a device due to lack of maintenance, a weak mistake can cause damage to the patient therapy being provided." P6 added, "if the medical devices are not managed properly and have open ports and are in public, a weak mistake can cause much damage by connecting to an unsecured network like our home WiFi." Furthermore, P8 recalled a device was "connected to multiple unsecured networks," noting that "the device was not properly managed."

Experts also pointed out problems with monitoring. Three participants specifically noted that reasons for failure are frequently due to "lack of continuous monitoring." P13 expanded on this problem, explaining, "Lack of automated tools to monitor. It is impossible to monitor over 100 assets, let along with the EHR network. Segmenting off the networked medical devices from the network seemed to set every device and monitoring easier."

Finally, participants also agreed that no matter the preventions and precautions are taken, there will always be some threat to cybersecurity. As P3 said, "External threats occur regardless of ITSEC measures." Likewise, P30 said, "Mission risk cannot be avoided," and P10 added that "One can never prevent attacks, only provide a defense in depth." Risk of threat echoed the

sentiment of P15, who said, “Threats will always exist regardless of what countermeasures are in place.”

Subtheme 3e: Prevention of failures. There was only one agreed-upon course of action to help prevent failures: active monitoring. P3 described this as “Prevent attacks is using a form of CSF and provide a defense in depth with monitoring capabilities.” Furthermore, P15 said prevention could be aided by, “Continuous monitoring with automated tools to provide a defense in depth.” For P6, this specific automated tool is Armis: “Allowing all networked medical devices to be monitored by Armis, at least in our environment, I feel that way.”

Subtheme 3f: Analytical tools for security risk. Experts agreed on three automated tools as an important measure against cybersecurity failures. These three were Splunk (8 people in round one, all agreed in subsequent rounds), APP Scan (4 people originally, all agreed in subsequent rounds), and NESSUX (4 people originally, all agreed in subsequent rounds). However, unlike any other subtheme, participants wanted to also be evident in giving other types of software they use. P6 said, “We use Armis that has asset discovery, device type, location, software, vulnerabilities, services used, connection history for forensics and passive monitoring which does not disrupt devices.” And P8 explained:

> We use Armis and Crowdstrike as well as Splunk. We apply and overlap some features to define the managed and unmanaged devices. If we allow for unmanaged devices to overextend our asset management list, we will lose control and lose manageable devices that our patients are currently using.

P9 also noted that some of these automated tools were contingent on a budget of an organization: “We use Airwatch and Checkpoint as well, but due to the budget not everyone has an appropriate cyber budget to support and reduce threats.”

Tools to analyze security risk. In addition to the automated tools these experts suggested, they also agreed that three other measures should be taken, the first of which is continuous

monitoring. Cited by five experts in the first round and agreed on by all in the subsequent two rounds, this measure included what P6 described as "monitoring of security controls," and P2 said, "Revolving vulnerabilities published for patching, which [means] monitoring software, asset management, online or not online as in networked active." The second of these tools was the protection of privacy and patient data in order to analyze security risk. This includes, as P4 said, "Privacy, PII, PHI, and patient safety." P4 added this protection should include, "Patient safety and the impact to telehealth therapy, data, PII, [and] PHI." Others included confidentiality (P8), and safety of the user (P11), with measures that protect what P6 called "impacts to telehealth therapy." The third tool for analyzing risk was limiting access. P3 noted this should include "Limit[ing] roles access and configuration to only mission-essential [since] user experience is minimal consideration for operational tools."

Major theme 4: Schemas and medical devices. The fourth theme, "Schemas and Medical Devices," includes three subthemes concerning IT experts who were participants experienced when analyzing risks for networked medical devices. The first subtheme, "Successful Schemas," included three items that were used by IT experts based on the priority of methods used. The second subtheme "Differences between Schemas," included two items that focused on what priorities to defend and monitor. The third subtheme, "Failures with Schemas," included three items that IT experts indicated were problematic or did not work.

Subtheme 4a: Successful Schemas. Within this subtheme, experts explained the three best methods used within successful schemas, which included security controls monitoring, updating patch versions, and having accurate and up-to-date manufacturer data. Cited by six participants in the first round of interviews, and agreed to by all experts in the second and third rounds of interviews, security controls monitoring includes "Implement[ing] security controls

such as NIST, [and] using CSF" (P3), "network monitoring" (P4), and "monitoring the device for network conductivity, patching, and configuration changes," (P13). Within the second method, experts (five in round one, all in rounds two and three) cited the need to have updated patch versions. As P2 explained, this involves, "Tracking the device lifecycle and network conductivity to include published patching version aligns to a successful schema." Likewise, P3 noted this should include "align[ing] all monitoring of devices to include updates from the vendor, on and off-line from the network." Finally, manufacturer data cited as a critical element to successful schemas. As P11 said, a thriving schema is one that is "set up to track the lifecycle of a medical device such as the manufacturer data, registration." Similarly, P15 agreed that successful schemas must include "manufacturing or vendor information pertaining to device, software, bios, or any other malfunctions or updates."

Within this first subtheme of successful schemas, experts also listed what they believe to be the most important characteristics for a successful schema. Participants agreed on three crucial elements: real-time monitoring, manual, and mitigating risk. As P4 explained within the first characteristic, "monitoring in real-time with schema has the ability to alert and resolve problems faster than manually. It is better to set up the schema to collect all and have unknowns than collect nothing." P13 also said, "With the types of schema employed, we continually monitor all networked medical devices in real-time." P11 also cited the importance of expediated information with real-time monitoring, saying, "the ability to provide monitoring the performance of healthcare information in real-time provides accuracy to pinpoint when and why the networked medical device impacted based on the types of initiatives the schema was built for." In terms of manual versus automated schemas, participants agreed that manual schemas were more successful. P3 noted, "Manual implementation verse automated schemas are more

successful and faster providing accurate real-time data." P7 concurred, adding that manual implementation, along with "continuous monitoring allows for anomaly detection to identify and prioritize the threats." The final crucial characteristic of a successful schema is its ability to mitigate risk. As P6 explained:

> A successful schema depends on the ability to mitigate risk. One cannot completely rid the technology of vulnerabilities, but implementing appropriate countermeasures, monitoring tools, and awareness of vulnerabilities provides more efficacy to organizations. Armis schema provides an agentless IoT security platform that lets enterprises see and control any device or network. The solution integrates with existing IT infrastructure and gives businesses visibility into and management over devices, whether on or off the corporate network.

P5 agreed, noting, "Schema is used to mitigate risk. Working as a team to deliver probability as well as security weakness with appropriate countermeasures and monitoring tools may provide more effectiveness with the device for trust with the provider and patient." In the final round of interviews, participants also added commentary on these three crucial characteristics, which pointed to the notion that more schemas are always better than fewer, particularly when they overlap. As P8 said, "We try to manage our footprint of devices by employing schemas with overlapping security technologies." P9 also noted, "We saw a lot of similarities which helped us affectively reduce the attack footprint to our mobile devices." Finally, P11 explained:

> Using appropriate schema is challenging as there are many types of technologies out there for networked medical devices, and there is no one appropriate schema. Nevertheless, we have found if apply all within the schema, eliminating objects that are being used on some but not applied to others are blank. Better to apply everything than apply less and wonder.

Subtheme 4b: Differences between Schemas. Within this subtheme, experts cited two items that focused on what priorities to defend and monitor: Protected Health Information (PHI) over Personally Identifiable Information (PII), and the differences between medical devices. Within the first difference, the expert noted that schemas supporting PHI were more critical than

those for PII. As P14 explained, “Monitoring patient health is most important, so we try not to use the following variables to the component traceability with device, location, as they are targets for fraud and scammers.” P3 also said, “Finding relational information supporting medical therapies to medical conditions treated we must compare to infrastructure IoT schemas that support without breaking the therapy or use of the medical device.” Within the second difference, the participants discussed the ways in which schemas were dependent on specific medical devices. As P4 explained, “All schema does not work for every medical device. All technology is different. Not every device maintains data and holds medical treatment. Some ingest and deliver data for monitoring purposes. Not all have Bluetooth or Wi-Fi capabilities.” P1 added to this, saying:

> Finding the right schema depends upon the device. Not every device has the same technology. Some provide therapy without retaining data. Some ingest data. If we are monitoring technology i.e., Bluetooth or patch or any type of network conductivity, we may use different tools. For all devices we do monitor when they are applied for therapy use and returned.

P5 noted that the difference in medical devices is very much dependent on different regulatory frameworks:

> Implementing standards that are mandated regulatory frameworks like PCI, HIPAA, or NIST and expanding frameworks after building the medical device can be tricky. As long as these controls do not break the therapy treatment, the device was intended for, using these frameworks can be useful but do not always work.

Subtheme 4c: Failures with schemas. This final subtheme included two ways in which schemas failed, as well as two primary characteristics of failed schemas. Within the first category, experts agreed that compromise of data and/or device, as well as the use of technology itself, has led to failed schemas. For P3, a failed schema involves “anything that compromises data or impacts the patient therapy.” As P13 noted, this could include, “Location of the devices, [which] can lead to data breach of PII and PHI.” However, more generally, experts in this study

agreed that any schema – as a technology – can be prone to failure. P4 noted, "Tools too can fail and can lead to false-positive analysis. Lessons learned are reviewing the schema often due to the constant evolution of growing cyber activities and attacks." P8 agreed, adding:

> Automated schema is another form of technology, and no technology is reliable. Monitoring tools must be updated to capture and analyze threats effectively. In order to prevent ineffective analysis, one must review the schema often due to the more sophisticated cyber activities and attacks.

P6 also said:

> When manually analyzing networked medical devices, it takes a greater amount of time, causing an effective response time to catch the error or the cause of the problem. Automated schema built into the technology relieves human error if the human sets up the appropriate objects, tables, and views correctly. Now depending on technology can help effectively capture and analyze threats faster, pinpointing the error a lot faster. The flaw is the technology must be set up for this to occur within the environment.

The second part of this subtheme includes two significant characteristics of failed schemas that the experts in this study have experienced: differences between technologies and misalignment with the vision of the organization. As P4 noted, when discussing the challenges of differences between technologies, there are often "challenges with different schemas meeting the requirements for monitoring technology that evolves." P11 also noted, "Different schemas made it challenging at times when it came to extract the data to be analyzed by engineers." Furthermore, P13 explained, "Some schemas are challenging because not all devices provide the same type of technology, so monitoring the basics is easy. Monitoring different types of technology becomes the challenge." This sentiment was echoed by P14, who said, "not all devices provide the same type of information for its technology." Likewise, P15 said, "All technology does not have the same type of access, store and forward data, or can provide the same standard set of controls to monitor for every networked medical device as it can break the device."

Experts also agreed that misalignment with the vision of the organization was another characteristic of a failed schema. P3 noted:

> Understanding the roles of different schema pose the only challenge and if they align with what the organization is monitoring based on the relationships of the devices. If automation is set up to conduct AI, the prioritization of threats will allow for a faster determination of the threat related to unrealistic or realistic events.

P8 also added that a challenge was, "Ensuring the schemas meet the mission and vision of the organization. Identifying the information, the organization wanted to capture helped us determine the most relevant schema for the medical devices and assess cybersecurity concerns." Similarly, P6 described the difficult process of finding a schema that aligned with the mission of the hospital:

> Finding the right schema to meet the mission of our hospital and the networked medical devices aligned to the supporting patient therapy due to the extensive devices that were supported. We looked out our specialty for our hospital, heart, diabetes, and brains. The challenge also was reviewing the different issues to the technology that already exist. Assessing how can we monitor in a holistic manner as if this was a regular network. Also, the hospital network as well, so we can eliminate risk to the entire enterprise. We had to identify the information for the hospital first. Then capture relevant helped us determine the most relevant schema for the medical devices and assess cybersecurity concerns.

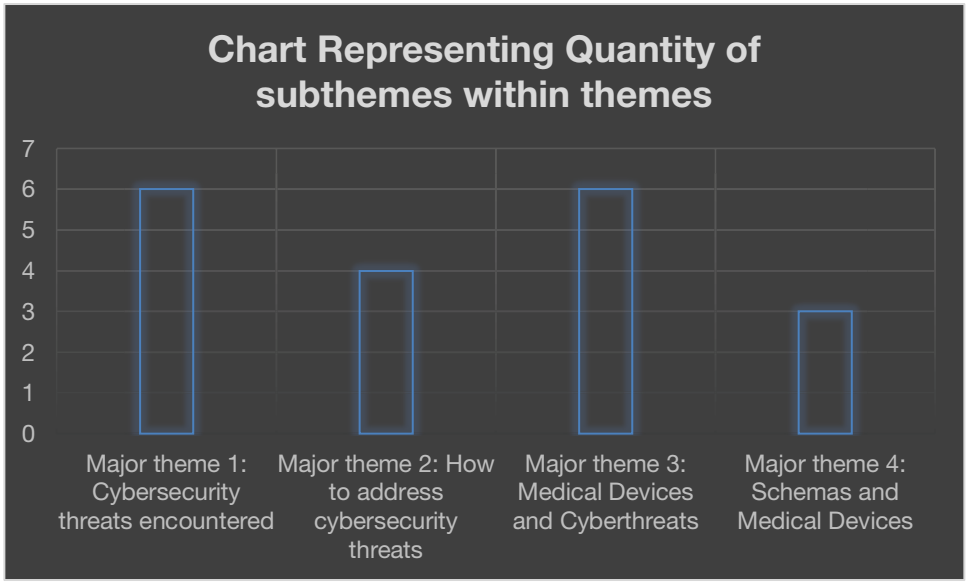

Figure 2. Chart representing quantity of subthemes within themes.

Summary

As seen in Figure 2, the first theme included six subthemes within parameters that focused on IT experts' experience with how the threats were discovered in networked medical devices. These subthemes were organized from most to least frequently occurring. Participants identified these threats from a personal perspective with configuration management, wireless and Bluetooth connections, Internet of Things, data breaches, insider threat, and asset management as cybersecurity threats in networked medical devices.

The second theme, How to Address Cybersecurity Threats, included four subthemes within parameters that focused on applying protective mechanisms that could help provide a defense for networked medical devices. IT experts identified how to address these cybersecurity threats from a personal perspective by controls assessment, automated technology, policy changes, and security awareness and training.

The third theme, Medical Devices and Cyberthreats, included six subthemes within parameters that focused on what the IT experts identified when analyzing issues that they faced with networked medical devices. The first subtheme "Security Measures" included four items that, if were implemented or applied, would be the top four considerations to protect networked medical devices at the first level of defense. The second subtheme, "Cybersecurity Failures Experienced," included three items that were found to be the most experienced with the IT experts. The third subtheme, "Addressing Cybersecurity Failures," included three most prevalent items found in failures with networked medical devices. The fourth subtheme, "Reasons for Failure," included three items that were found to be the most reasons found by IT experts within networked medical devices. The fifth subtheme, "Prevention of Failures," included only one item that all IT experts reported as active monitoring networked medical devices would actively

prevent cyber threats with networked medical devices. The sixth subtheme, “Analytical Tools for Security Risk,” included four items that were used by IT experts for performing analytical risks when actively monitoring networked medical devices.

Finally, the fourth theme, Schemas and Medical Devices, included three subthemes concerning IT experts who were participants experienced when analyzing risks for networked medical devices. The first subtheme, “Successful Schemas” included three items that were used by IT experts based on the priority of methods used. The second subtheme, “Differences between Schemas,” included two items that focused on what priorities to defend and monitor. The third subtheme, “Failure with Schemas” included three items that were found by IT experts that did not work or found problems within the schemas.

CHAPTER 5. DISCUSSION, IMPLICATIONS, RECOMMENDATIONS

Introduction

The healthcare industry was among the top five industries that use data protection and common targets of cyberattacks (Filkins & Wright, 2017). Medical devices that expose patients to threats managed through standardizing risk management processes (Weininger et al., 2017). These were risks to organizational networks leading to emerging issues followed the expansion of the system between networked devices and clinical operations. With security risks to networked devices, the safety measures readily penetrated, leaving devices and networks in a vulnerable state that could lead to unauthorized personnel managing the devices with malicious intent (William & Woodward, 2015). Thus, the specific problem that was addressed in this study was the lack of basis for developing effective countermeasures for cyber threats to networked medical devices leading to a high possibility of security breaches (Pycroft & Aziz, 2018; Ransford et al., 2017). Failures of networked medical devices could potentially result in fatal events (Pycroft & Aziz, 2018; Ransford et al., 2017). Given this problem, the purpose of this qualitative Delphi study was to support a development for a model with effective countermeasures for cyber threats with networked medical devices based on experiences and perceptions of IT experts in the healthcare industry in the United States. For this Delphi study, the main research question was: What are the relevant experiences in employing a schema to analyze security risks in networked medical devices?

The remainder of Chapter 5 includes an evaluation of the studies research question, a discussion of the fulfillment of the research purpose, the contribution of the findings of this study to the business technical problem, as well as recommendations for future research, based on the results of this study. The chapter concludes with a summary.

Evaluation of Research Questions

The primary research question for this study was: What are the relevant experiences in employing a schema to analyze security risks in networked medical devices? This research question aligned with the topic and problem; therefore, the question was appropriate for this study. To answer the research question, the primary source of data was semi-structured interviews in multiple rounds until saturation of data reached. The researcher inquired about the experiences of IT experts to gain a deeper understanding of the phenomenon and address research questions of the study. Such a research question allowed for an in-depth exploration of a sample with specific and precise knowledge about cybersecurity in medical devices. Indeed, the experts in this study were all working as IT leaders in organizations using networked medical devices, had been in the cybersecurity field for at least 5 years, and were responsible and accountable for the security of data involved with the use of networked medical devices, specifically in hospitals that use networked medical devices. However, given the nature of the research question, the risks and the networked medical devices were not monolithic. That is, IT experts may have had experiences with different types of medical devices at different hospitals and therefore had varying experiences.

Moreover, other limitations occurred because of the configuration of the research question. This research question was narrowly focused from a technical perspective rather than usability, insofar as it was limited only to IT experts. In this way, the research question did not address the issues of clinicians and/or patients, both of whom are somewhat uneducated about the methods for evaluating security risks with their medical devices. Moreover, because the patient perspective was not considered in this study, there was no discussion of patient safety, and given the lack of clinicians, there was no discussion of the procurement of these devices.

Both of these elements could be useful elements of cybersecurity but is not within this study research question.

In addition, the researcher did not seek to understand the ways in which manufacturers have (or have not) developed security problems and troubleshooting methods to address cybersecurity concerns, which may be an essential proactive development in protecting security devices and assessing vulnerabilities. While the research question did allow for IT experts' experiences *with* manufacturers – indeed, the consensus in this study found that manufacturer data is crucial in the protection process – there was a lack of research as to the dialectic *between* IT experts and the manufacturer.

Fulfillment of Research Purpose

The purpose of this qualitative Delphi study was to create a model for developing effective countermeasures for cyber threats to networked medical devices in the healthcare industry in the United States. Based on these rounds of questioning, the researcher developed the final model seen in Figure 3.

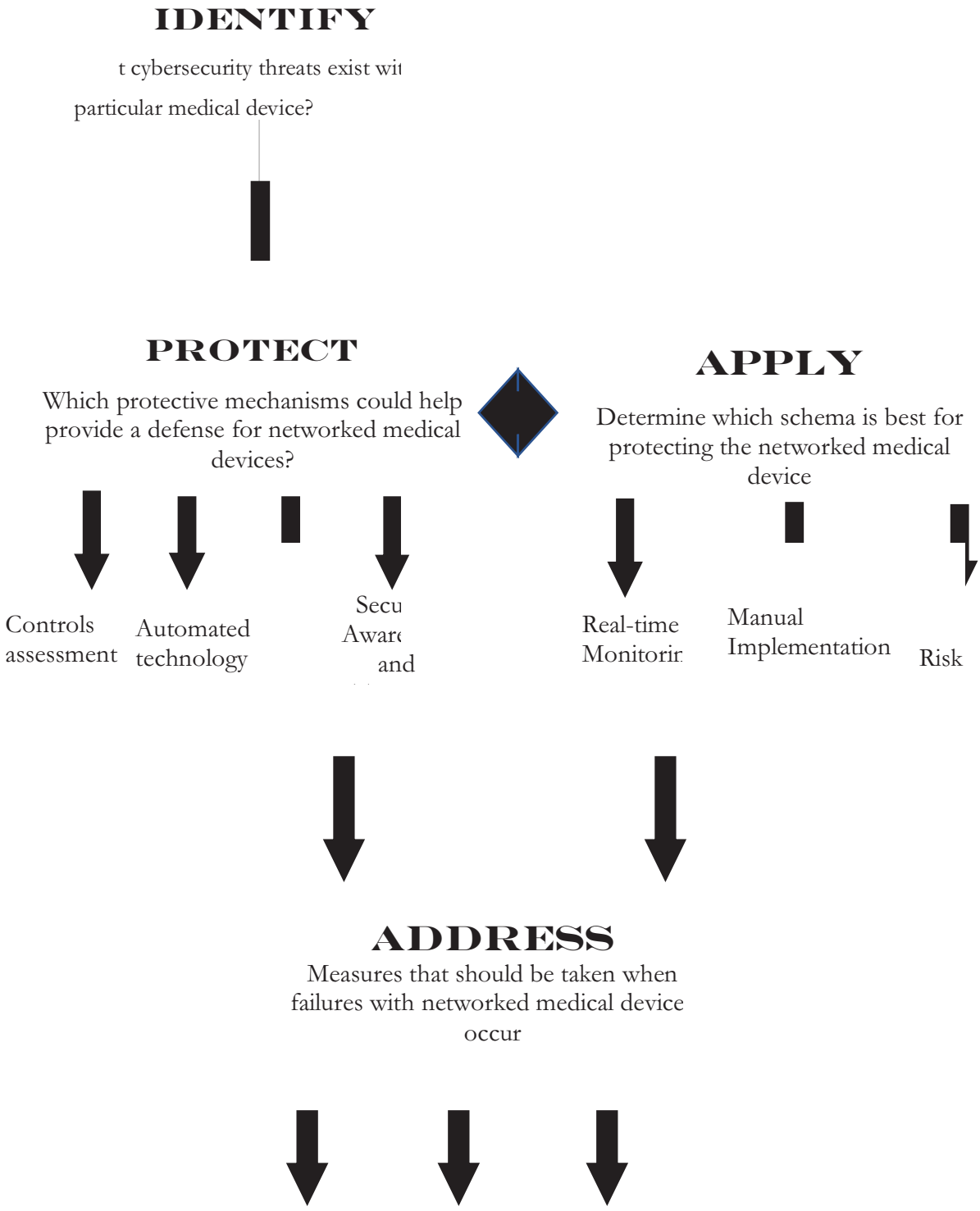

Figure 3. Model to support the development for effective countermeasures for cyber threats to networked medical devices in the healthcare industry in the United States.

The first phase of this model is identification. In this phase, IT experts determine what networked medical devices pose specific threats. Such a determination will be grounded in the medical device itself, its function, and connectivity, as well as vulnerabilities that emerge from those characteristics. According to the results of this study, such an assessment would include: Configuration management, wireless and Bluetooth connection, the Internet of Things (IoT), data breaches, insider threats, asset management, malicious attacks, Denial of Service (DoS) attacks, and mechanism failure.

The second phase occurs at nearly the same time – both are protective and specific measures and applications of schemas to facilitate the protection of networked medical devices. More specifically, protection mechanisms should include control assessments, automated technology, policy changes, and security awareness and training. With these mechanisms in mind, a specific schema is chosen, which also includes what the experts in this panel determined, are the three most important characteristics: real-time monitoring, manual implementation, and mitigating risk. In addition, the use of schemas would include three methods: control monitoring, updating patch versions, and having accurate and up-to-date manufacturer data.

If and when there is a cybersecurity failure, the final phase is to address the failure. According to the experts in this study, this includes locking down the device, reporting the failure to and through the proper channels, and running automated tools to discover the source of the failure. This model can then be repeated over again, starting by identifying the failures.

Contribution to Business Technical Problem

The extant literature has made clear the myriad of challenges that stem from the provision of healthcare by networked medical devices. In the United States, over 300,000 patients have embedded networked medical devices, and approximately 2.5 million are at risk with life-

threatening situations that are dependent on such devices (Ankarali et al., 2014). Moreover, approximately 94% of healthcare organizations were victims of cyberattacks on medical devices and the infrastructure to support these devices (William & Woodward, 2015). These devices may be affected by cyberattacks, such as altering of code delivering therapy of care via electronic healthcare delivery (i.e., telehealth), battery failure, and migration problems (Pycroft & Aziz, 2018). Cybersecurity vulnerabilities are detrimental to the safe operation of networked medical devices as it compromises the treatment of patient safety more than personally identifiable information. Additional researchers found challenges associated with networked medical devices affect decisions and mitigating factors linked to cybersecurity, patient safety, and hospital systems (Gee, 2017; Hagestad & Straumann, 2017; Sametinger et al., 2015). Thus, it is clear that networked medical devices impose increased risks leading to vulnerabilities (Patel et al., 2015).

Addressing these risks related to the exposure of networked medical devices to cyberattacks is how this study addressed this critical problem. By identifying what types of cybersecurity attacks most often occur with medical devices and having IT experts within this field come to a consensus on the best methods and measures to prevent, address, and redress these attacks, this study will help in improving patient safety for a population with networked medical devices by providing defense mechanisms identified by IT experts.

Using a model such as the one created by the results of this study, and mandating its implementation as a mechanism for accountability to improve assessing lifecycle based on a monitoring structure for managing cyber threats can help reduce the risk to the patient and healthcare provider with security, malfunctioning, or malicious exposures. This model can be helpful to practitioners in terms of avoiding gaps in protection from cyberattacks. The findings will be beneficial to practitioners who defend systems connecting to medical devices susceptible

to cyber threats leading to malicious attacks (William & Woodward, 2017). In particular, those who lead the forefront of guidance in support of medical devices are to ensure minimizing threats and vulnerabilities. The findings for this research could provide a basis that medical device users could follow in terms of preventing a security breach when using networked medical devices. IT leaders in the field of healthcare, including networked medical device production, could use the model for this study to enhance procedures in order to ensure the security of the device from cyber threats and minimize risks related to its use, especially when connected to a network.

Moreover, the findings from this study could provide a possible capability to give awareness to IT support and organizations within the United States that support medical devices. The present study may also be used to assist in the automation of alerting the proper help to reduce risk to networked medical devices and mitigate cyberattacks. In addition, the model may also be helpful to scholars employing increasing efficiency in terms of identifying areas of risk where more methods are needed.

Recommendations for Further Research

Further studies can expand upon the results of this research. While this study examined the issue of cybersecurity and medical devices through the lens of IT experts, future projects may explore how patients use these devices, and how such behaviors impact issues of security. Such research may also examine the public perceptions of cyber healthcare risks associated with the use of medical devices and if such perceptions alter the use of devices and/or individual health outcomes. Such research would integrate the multiple stakeholders involved in the cybersecurity of medical devices.

Another critical unit of study may be the hospitals from which these devices come. How do hospitals create IT policy based on cybersecurity risk? In what ways do the organizational elements of the hospital dictate how they manage cybersecurity risks? Because hospitals often have siloed IT units, such research – particularly done in a cross-comparative manner – could allow for an understanding of the obstacles and challenges in creating a universal cybersecurity policy.

Moreover, given the model the researcher created using the results of this study, further research is needed to gauge how such a model is successful in helping prevent cybersecurity attacks on medical devices. Utilizing a case study methodology, future research can examine how this model aids specific hospitals, or specific types of medical devices, from cyberattacks. Results from such studies could help expand and/or alter the model arrived at in this study.

Finally, participants of this study noted that schemas were often dependent on the current state and federal regulations of privacy. Future research is needed to explore how regulations vary state-by-state, as well as state-to-federal, and the implications of these variances for cybersecurity of medical devices.

Conclusions

As technology continues to develop, more medical devices have also connected to networks for faster communication and to take advantage of the benefits of the Internet (Ransford et al., 2017; William & Woodward, 2015). Medical devices are an emerging concern in the United States (Middaugh, 2016). With the growing sophistication of hackers' skills, cyber threats continue to evolve within the field of medical devices (Ransford et al., 2017). The specific problem addressed in this study was the lack of basis for developing effective countermeasures for cyber threats to networked medical devices leading to a high possibility of

security breaches (Pycroft & Aziz, 2018; Ransford et al., 2017). Therefore, the purpose of this qualitative Delphi study was to create a model for developing effective countermeasures for cyber threats to networked medical devices in the healthcare industry in the United States. The procedures for data collection in this research were conducted using the Delphi method, with interviews of IT experts within the field of medical devices conducted in multiple rounds.

The results of this study found four major themes, all of which reflected IT experts' experience with the threats discovered in networked medical devices, how to address cybersecurity threats, specific cyber threats to medical devices, and how to analyze and address medical device cybersecurity risks and failures. From these results, the researcher developed a model for of effective countermeasures for cyber threats to networked medical devices in the healthcare industry in the United States. Addressing these risks related to the exposure of networked medical devices to cyberattacks is how this study addressed this critical problem. By identifying what types of cybersecurity attacks occur most often with networked medical devices, and having IT experts within this field come to a consensus on the best methods and measures to prevent, address, and redress these attacks, this study will help improve patient safety for a population with medical devices.

REFERENCES

Abomhara, M., Gerdes, M., & Køien, G. M. (2015). *A STRIDE-based threat model for telehealth systems.* Proceedings of the 12th Norwegian Information Security Conference (NISC), 82-96. https://ojs.bibsys.no/index.php/NISK/issue/view/NISK2019

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior*. Englewood Cliffs, NJ: Prentice-Hall.

Alemzadeh, H., Iyer, R., Kalbarczyk, Z., & Raman, J. (2013). Analysis of safety-critical computer failures in medical devices. *IEEE Security & Privacy, 11*(4), 14-26. doi:10.1109/msp.2013.49

Alhassan, J. K., Abba, E., Olaniyi, O. M., & Waziri, V. O. (2016, November). *Threat modeling of electronic health systems and mitigating countermeasures*. International Conference on Information and Communication Technology and its Application. Minna, Nigeria: Federal University of Technology. https://www.researchgate.net/profile/Olaniyi_Olayemi_Mikail/publication/311238739_Threat_Modeling_of_Electronic_Health_Systems_and_Mitigating_Countermeasures/links/5840187508ae61f75dce2d55.pdf

Alvarenga, A., & Tanev, G. (2017). A Cybersecurity Risk Assessment Framework that Integrates Value-Sensitive Design. *Technology Innovation Management Review*, *7*(4), 32-43. doi:10.22215/timreview/1069

Anderson, S., & Williams, T. (2018). Cybersecurity and medical devices: Are the ISO/IEC 80001-2-2 technical controls up to the challenge? *Computer Standards & Interfaces, 56*, 134-143. doi:10.1016/j.csi.2017.10.001

Ankarali, Z. E., Abbasi, Q., Demir, A., Serpedin, E., Qaraqe, K., & Arslan, H. (2014). A Comparative Review on the Wireless Implantable Medical Devices Privacy and Security. *Proceedings of the 4th International Conference on Wireless Mobile Communication and Healthcare - "Transforming Healthcare through Innovations in Mobile and Wireless Technologies*". doi:10.4108/icst.mobihealth.2014.257411

Ankarali, Z. E., Demir, A. F., Arslan, H., & Gitlin, R. D. (2017). Physical layer security for wireless implantable medical devices: US Patent 9,749,086. https://patents.google.com/patent/US9749086B1/en

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304-312. doi:10.1016/j.chb.2014.05.046

Assante, M. J., & Lee, R. M. (2015). *The industrial control system cyber kill chain*. SANS Institute InfoSec Reading Room, 1. https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297

Balkar, B. (2015). Defining an empowering school culture (ESC): Teacher perceptions. *Issues in Educational Research*, *25*, 205-214. www.iier.org.au/

Baranchuk, A., Refaat, M. M., Patton, K. K., Chung, M. K., Krishnan, K., Kutyifa, V., … & Lakkireddy, D. R. (2018). Cybersecurity for Cardiac Implantable Electronic Devices: *Journal of the American College of Cardiology, 71, 1284-1288*. doi:10.1016/j.jacc.2018.01.023

Barratt, M. J., Ferris, J. A., & Lenton, S. (2014). Hidden Populations, Online Purposive Sampling, and External Validity. *Field Methods*, *27*(1), 3-21. doi:10.1177/1525822X14526838

Baybutt, P. (2017). Guidelines for designing risk matrices. *Process Safety Progress*, *37*(1), 49-55. doi:10.1002/prs.11905

Birko, S., Dove, E. S., & Özdemir, V. (2015). Evaluation of Nine Consensus Indices in Delphi Foresight Research and Their Dependency on Delphi Survey Characteristics: A Simulation Study and Debate on Delphi Design and Interpretation. *PloS One*, 10*:* e0135162. doi:10.1371/journal.pone.0135162

Burns, A. J., Johnson, M. E., & Honeyman, P. (2016). A brief chronology of medical device security. Communications of the ACM, 59(10), 66-72. Doi: 10.1145/2890488

Busdicker, M., & Upendra, P. (2017). The Role of Healthcare Technology Management in Facilitating Medical Device Cybersecurity. *Biomedical Instrumentation & Technology, 51(s6),* 19-25. doi:10.2345/0899-8205-51.s6.19

Camara, C., Peris-Lopez, P., & Tapiador, J. E. (2015). Security and privacy issues in implantable medical devices: A comprehensive survey. *Journal of Biomedical Informatics, 55*, 272-289. doi:10.1016/j.jbi.2015.04.007

Car, J., Tan, W. S., Huang, Z., Sloot, P., & Franklin, B. D. (2017). eHealth in the future of medications management: personalisation, monitoring and adherence. *BMC Medicine*, *15*. doi:10.1186/s12916-017-0838-0

Center for Medicare & Medicaid Service, (2018). HIPAA basics for providers: Privacy, security, and breach notification rules. *Centers for Medicare & Medicaid Services, U.S. Department of Health & Human Services, Medical Learning Network*. U. S. Department

of Health & Human Services, Center for Medicare & Medicaid Service, Medical Learning Network..https://www.cms.gov/Outreach-and-Education/ Medicare-Learning-Network-MLN/MLNProducts/Downloads/HIPAA Privacyand Security.pdf

Cerkovnik, J. (2015). *Managing vulnerabilities and risk in networked medical devices*. ProQuest Dissertations & These Global. University of South Alabama. (Publication No. 1604546)

Chow, E. Y., Sanghani, S. P., & Morris, M. M. (2017). Wireless MEMS-based implantable medical devices for cardiology. In *Wireless MEMS Networks and Applications*, 77-100. doi:10.1016/B978-0-08-100449-4.00004-X

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, *113*, 48–52. doi:10.1016/j.maturitas.2018.04.008

Cypress, B. S. (2017). Rigor or Reliability and Validity in Qualitative Research. *Dimensions of Critical Care Nursing*, *36*, 253-263. doi:10.1097/DCC.0000000000000253

Dalkey, N., & Helmer, O. (1963). An Experimental Application of the DELPHI Method to the Use of Experts. *Management Science*, *9*, 458-467. doi:10.1287/mnsc.9.3.458

Das, A. K., Wazid, M., Kumar, N., Khan, M. K., Choo, K. -K. R., & Park, Y. (2018). Design of Secure and Lightweight Authentication Protocol for Wearable Devices Environment. *IEEE Journal of Biomedical and Health Informatics, 22*, 1310-1322. doi:10.1109/JBHI.2017.2753464

Devito, M., & Johannes, J. (2016). A security assessment of Z-Wave devices and replay attack vulnerability. [1]: North Bethesda, MD: The SANS Institute. https://www.sans.org/reading-room/whitepapers/internet/paper/37242

Dimensional Research. (2016). *Trends in security framework adoption: A survey of IT and security professionals.* static.tenable.com/marketing/tenable-csf-report.pdf

Dixon, T., & Horton, D. (1968). *Verbal Behavior and General Behavior Theory*, 340-387. Englewood Cliffs, NJ: Prentice-Hall.

Dulany, D. E. (1968). *Awareness, rules, and propositional control: A confrontation with SR behavior theory*, 203-203. Englewood, Cliffs, NJ: Prentice-Hall.

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of Convenience Sampling and Purposive Sampling. *American Journal of Theoretical and Applied Statistics*, *5*, 1-4. doi:10.11648/j.ajtas.20160501.11

Filkins, B., & Wright, B. (2017). Sensitive data at risk: The SANS 2017 Data Protection Survey. https://www.sans.org/reading-room/whitepapers/threats/sensitive-data-risk-2017-data-protection-survey-37950

Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Research*, *20*, 1408-1416. http://nsuworks.nova.edu/tqr/vol20/iss9/3

Gantz, S. D., Philpott, D. R., & Windham, D. (2013). Federal Information Security Fundamentals. *FISMA and the risk management framework,23-52.* doi:10.1016/b978-1-59-749641-4.00002-3

Gaukstern, E., & Krishnan, S. (2018). Cybersecurity threats targeting networked critical medical devices. American Society for Engineering Education, Illinois-Indiana Section. doi:10.5703/1288284316840

Gee, T. (2017). Our Work Must Catch Up to Technology. *Biomedical Instrumentation & Technology*, *51*, 200-202. doi:10.2345/0899-8205-51.3.200

Gignac, G. E., & Szodorai, E. T. (2016). Effect size guidelines for individual differences researchers. *Personality and Individual Differences*, *102*, 74-78. doi:10.1016/j.paid.2016.06.069

Goodman, S., Straub, D. W., & Baskerville, R. (2008). *Information Security: Policy, Processes, and Practices.* New York: Routledge. doi:10.4324/9781315288697

Griffith, D. A., Morris, E. S., & Thakar, V. (2016). Spatial Autocorrelation and Qualitative Sampling: The Case of Snowball Type Sampling Designs. *Annals of The American Association of Geographers, 106*, 773-787. doi:10.1080/24694452.2016.1164580

Hagestad, B., & Straumann, A. (2017). Commentary: Collaborating to achieve a mutual cybersecurity advantage. *Biomedical Instrumentation & Technology*, *51*(1), 34-39. doi:10.2345/0899-8205-51.1.34

Hatcliff, J., Vasserman, E. Y., Carpenter, T., & Whillock, R. (2018). Challenges of distributed risk management for medical application platforms. 2018 IEEE Symposium on Product Compliance Engineering (ISPCE). doi:10.1109/ispce.2018.8379270

He, M., Devine, L., & Zhuang, J. (2018). Perspectives on cybersecurity information sharing among multiple stakeholders using a decision-theoretic approach. *Risk Analysis*, *38*, 215-225. doi:/10.1111/risa.12878

Hernan, S., Lambert, S., Ostwald, T., & Shostack, A. (2014). Undercover Security Design Flaws Using the STRIDE Approach. *MSDN Magazine. Microsoft Corporation*. The STRIDE threat model. November 2006 http://msdn.microsoft.com/msdnmag/issues/06/11/threatmodeling/default.aspx

HIMSS (2017*). HIMSS cybersecurity survey*. HIMSS North America. http://www.himss.org/sites/himssorg/files/2017-HIMSS-Cybersecurity-Survey-Final-Report.pdf

HIMSS (2005). *Guidance for industry: Cybersecurity for networked medical devices containing off-the-shelf (OTS) software*. HIMSS North America. http://www.himss.org/ guidance-industry-cybersecurity-networked-medical-devices-containing-shelf-ots-software

Hoffman, L. J., Michelman, E., & Clements, D. P. (1978). SECURATE-security evaluation and analysis using fuzzy metrics. *AFIPS National Computer Conference Proceedings, 47*, 531-540.

Hollis, K. F. (2016). To share or not to share: ethical acquisition and use of medical data. *AMIA Summits on Translational Science Proceedings*, *2016*, 420–427.

Hwang, T. J., Sokolov, E., Franklin, J. M., & Kesselheim, A. S. (2016). Comparison of rates of safety issues and reporting of trial outcomes for medical devices approved in the European Union and United States: cohort study. *British Medical Journal,* i3323. doi:10.1136/bmj.i3323

ICS-CERT (2018). *Indiana cybersecurity*. U. S. Department Homeland Security, ICS-CERT. https://www.in/gov/cybersecurity/ 2536.htm

ISO (2018). *Risk management – principles and guidelines*. ISO 31000:2018(en). International Organization for Standardization. https://www.iso.org/obp/ui/#iso:std:iso: 31000:ed-2:v1:en

ISACA (2017). Security assurance in the SDLC for the internet of things. *ISACA Journal, 3*. : https://www.isaca.org/Journal/archives/2017/Volume-3/Documents/ Security-Assurance-in-the-SDLC-for-the-Internet-of-Things_joa_Eng_0517.pdf

Johnson, S. (2019). *Safeguarding Against Data Breaches*. University of Tennessee Health Center, Applied Research Projects, 66. doi:10.21007/chp.hiim.0061

Jontz, S. (2015). Networked medical devices deliver benefits, drawbacks. *AFCEA*. https://www.afcea.org/content/?q=Article-networked-medical-devices-deliver-benefits-drawbacks

Jorm, A. F. (2015). Using the Delphi expert consensus method in mental health research. *Australian & New Zealand Journal of Psychiatry*, *49*, 887-897. doi:10.1177/000486741560089

Kasparick, M., Schlichting, S., Golatowski, F., & Timmermann, D. (2015). Medical DPWS: New IEEE 11073 standard for safe and interoperable medical device communication. 2015 IEEE Conference on Standards for Communications and Networking (CSCN). doi:10.1109/cscn.2015.7390446

Khera, M. (2017). Think Like a Hacker. *Journal of Diabetes Science and Technology, 11*, 207-212. doi:10.1177/1932296816677576

Klonoff, D. C., & Price, W. N. (2016). The Need for a Privacy Standard for Medical Devices That Transmit Protected Health Information Used in the Precision Medicine Initiative for Diabetes and Other Diseases. Journal of Diabetes Science and Technology, 11, 220-223. Doi:10.1177/1932296816680006

Kohnfelder, L., & Garg, P. (1999). The threats to our products. *Microsoft Interface*, Microsoft Corporation, 33.

Kramer, D. B., Baker, M., Ransford, B., Molina-Markham, A., Stewart, Q., Fu, K., & Reynolds, M. R. (2012). Security and Privacy Qualities of Medical Devices: An Analysis of FDA Postmarket Surveillance. *PLoS One, 7*, e40200. doi:10.1371/journal.pone.0040200

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. doi:10.3233/thc-161263

Kune, D. F., Backes, J., Clark, S. S., Kramer, D., Reynolds, M., Fu, K., ... & Xu, W. (2013). Ghost talk: Mitigating EMI Signal Injection Attacks against Analog Sensors. *2013 IEEE Symposium on Security and Privacy*. doi:10.1109/sp.2013.20

Lam, M. L. L., & Wong, K. W. (2018). Embracing Cybersecurity Risk Management in the Industry of Medical Devices. *Analyzing the Impacts of Industry 4.0 in Modern Business Environments,* 177-197. doi:10.4018/978-1-5225-3468-6.ch010

Larson, J. (2017). *Medical device security considerations – case study*. Joint Commission. https://www.jointcommission.org/assets/1/6/sbx2-w3-medical-device-security-considerations-case-study.pdf

Lefkovitz, N., Nadeau, E., Feldman, L., & Witte, G. (2017). *Building the bridge between privacy and cybersecurity for federal systems*. U.S. Department of Commerce National Institute of Standards and Technology, Information Technology Laboratory, Applied Cybersecurity Division. https://csrc.nist.gov/publications/detail/itl-bulletin/2017/04/building-bridge-b/w-privacy--cybersecurity-for-federal-systems/final

Leung, L. (2015). Validity, reliability, and generalizability in qualitative research. *Journal of Family Medicine and Primary Care*, *4*, 324-327. doi:10.4103/2249-4863.161306

Lewis, S. (2015). Qualitative inquiry and research design: Choosing among five approaches. *Health Promotion Practice*, *16*, 473-475. doi:10.1177/1524839915580941

Liang, H., & Xue, Y. (2009). Avoidance of Information Technology Threats: A Theoretical Perspective. *MIS Quarterly, 33*, 71-71. doi:10.2307/20650279

Lincoln, Y. S., & Guba, E. G. (1985). Establishing trustworthiness. *Naturalistic inquiry*, *289*, 331.

Linstone, H. A. (1977). Confessions of a Forecaster. Futures research: New directions, 11, 44.

Lyons, K. D., Radomski, M. V., Alfano, C. M., Finkelstein, M., Sleight, A. G., Marshall, T. F., ... & Fu, J. B. (2017). Delphi study to determine rehabilitation research priorities for older adults with cancer. *Archives of physical medicine and rehabilitation*, *98*, 904-914. doi:10.1016/j.apmr.2016.11.015

MacMahon, S. T., Mc Caffery, F., & Keenan, F. (2015). Development and validation of the MedITNet assessment framework: improving risk management of medical IT networks. Proceedings of the 2015 International Conference on Software and System Process - ICSSP 2015. doi:10.1145/2785592.2785599

Mahler, T., Nissim, N., Shalom, E., Goldenberg, I., Hassman, G., Makori, A., . . . Shahar, Y. (2018). Know your enemy: Characteristics of cyberattacks on medical imaging devices. *Computer Science: Cryptography and Security, 1*.

Maisel, W. H., & Kohno, T. (2010). Improving the security and privacy of implantable medical devices. *New England Journal of Medicine, 362*, 1164-1166.

Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: how safe are we? *BMJ*. doi:10.1136/bmj.j3179

Martínez-Pérez, B., De La Torre-Díez, I., & López-Coronado, M. (2015). Privacy and Security in Mobile Health Apps: A Review and Recommendations. *Journal of Medical Systems*, *39*. doi:10.1007/s10916-014-0181-3

McNally, G., Frey, R., & Crossan, M. (2017). Nurse manager and student nurse perceptions of the use of personal smartphones or tablets and the adjunct applications, as an educational

tool in clinical settings. *Nurse Education in Practice*, *23*, 1-7. doi:10.1016/j.nepr.2016.12.004

MDPC. (2014). *Security risk assessment framework for medical devices*. Medical Device Privacy Consortium. http://deviceprivacy.org/activities/mdpc-white-paper-september-2014

Meng, W., Li, W., Xiang, Y., & Choo, K. R. (2017). A bayesian inference-based detection mechanism to defend medical smartphone networks against insider attacks. *Journal of Network and Computer Applications*, *78*, 162-169. doi:10.1016/j.jnca.2016.11.012

Middaugh, D. J. (2016). Do security flaws put your patients' health at risk? *Medsurg Nursing, 25*(2), 131-132.

Mitre Corporation. (2018). *Overview - What is CWE? CWE*. https://cwe.mitre.org/about/index.html

Moghaddasi, H., Sajjadi, S., & Kamkarhaghighi, M. (2016). Reasons in support of data security and data security management as two independent concepts: A new model. *The Open Medical Informatics Journal, 10*, 4-10. doi:10.2174/1874431101610010004

NIST (n.d.). *National vulnerability database: CVSS vulnerability metrics.* U. S. Department of Commerce, National Institute of Standards and Technology. https://nvd.nist.gov/vuln-metrics/cvss

NIST (2010a). *Guide for applying the risk management framework to federal information systems a security life cycle approach*. U. S. Department of Commerce, National Institute of Standards and Technology. (NIST SP 800-37r1.) doi:10.6028/NIST.SP.800-37r1

NIST (2010b). *Guide to protecting the confidentiality of personally identifiable information (PII).* (NIST Special Publication 800-122). U. S. Department of Commerce, National Institute of Standards and Technology. doi:10.6028/nist.sp.800-122

NIST (2012). Guide for conducting risk assessments. U. S. Department of Commerce, National Institute of Standards and Technology. Doi:10.60.6028/nist.sp.800-30r1

NIST (2019). Glossary of Key Information Security Terms. U. S. Department of Commerce, National Institute of Standards and Technology. (NISTIR 7298 Rev 3). doi:10.6028/NIST.IR.7298r3

NIST (2013). *Security and Privacy Controls for Federal Information Systems and Organizations.* (NIST Special Publication 800-53 Rev.4). U. S. Department of Commerce, National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

NIST (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. U. S. Department of Commerce, National Institute of Standards and Technology. doi:10.6028/nist.cswp.04162018

Noimanee, S., Noimanee, K., Krisanachinda, S., & Senavongse, W. (2016). Study of cybercrime and security in medical devices. *2016 9th Biomedical Engineering International Conference (BMEiCON)*. doi:10.1109/bmeicon.2016.7859649

Office of Civil Rights (2013). *Breach Notification Rule*. U.S. Department of Health & Human Services, Office of Civil Rights. https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

Olendorf, K. N. (2015). *Cybersecurity of networked home medical devices* (Order No. 1587990). Available from ProQuest Dissertations & Theses Global. (1681637819). Utica College.

OWASP (2018). *Welcome to OWASP*. https://www.owasp.org/index.php/ Main_Page

Ozair, F. F., Jamshed, N., Sharma, A., & Aggarwal, P. (2015). Ethical issues in electronic health records: A general overview. *Perspectives in Clinical Research*, *6*, 73-76. doi:10.4103/2229-3485.153997

Ozier, W. (2012). The Delphi/modified Delphi technique: A consensus approach to information valuation. The Integrated Risk Management Group (TIRMG) http://ittoday.info/AIMS/DSM/85-10-10.pdf

Pandey, S. K., & Batra, M. (2013). Security Testing in Requirements Phase of SDLC. *International Journal of Computer Applications*, *68*(9), 31-35. doi:10.5120/11609-6985

Pardue, J. H., Purawat, S., & Landry, J. P. (2014). *A database-driven model for risk assessment: Research-in-progress*. Twentieth Americas Conference on Information Systems, Savannah. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1611&context=amcis2014

Pasman, H. J. (2016). Risk assessment: What can it do for you? It may be a matter of to be or not to be! *Journal of Applied Packaging Research*, 8-14.

Patel, A., Al-Janabi, S., Alshourbaji, I., & Pedersen, J. (2015). A novel methodology towards a trusted environment in mashup web applications. *Computers & Security, 49*, 107-122. doi:10.1016/j.cose.2014.10.009

Peace, C. (2017). The risk matrix: uncertain results? *Policy and Practice in Health and Safety*, *15*(2), 131-144. doi:10.1080/14773996.2017.1348571

Ponemon Institute. (2017). Medical device security: An industry under attack and unprepared to defend. https://www.synopsys.com/content/dam/synopsys/ sig-assets/reports/medical-device-security-ponemon-synopsys.pdf

Ponikowski, P., Voors, A. A., Anker, S. D., Bueno, H., Cleland, J. G. F., Coats, A. J. S., … van der Meer, P. (2016), 2016 ESC guidelines for the diagnosis and treatment of acute and chronic heart failure. *Eur J Heart Fail, 18*, 891-975. doi:10.1002/ejhf.592

Porup, J. M. (2016). "Internet of things" security is hilariously broken and getting worse. ARS Technica. http://arstechnica.com/security/2016/01/how-to-search-the-internet-of-things-for-photos-of-sleeping-babies

Pycroft, L., & Aziz, T. Z. (2018). Security of implantable medical devices with wireless connections: The dangers of cyber-attacks. Expert Review of Medical Devices, 15, 403-406. doi:10.1080/17434440.2018

Rakitin, S. R. (2009). Networked medical devices: essential collaboration for improved safety. Biomedical instrumentation & technology, 43(4), 332-338. https://www.swqual.com/images/Networked.pdf

Ransford, B., Kramer, D. B., Kune, D. F., Medeiros, J. A., Yan, C., Xu, W., & Fu, K. (2017). Cybersecurity and medical devices: A practical guide for cardiac electrophysiologists. *Pacing and Clinical Electrophysiology, 40*, 913-917. doi:10.1111/pace.13102

Ransford, B., Kune, F. D., Gookin, A., & DeOrio, A. (2016). Noninvasive postmarket security monitoring for medical devices. *Journal of Medical Devices*, *10*. doi:10.1115/1.4033285

Rao, A., Carreon, N., Lysecky, R., & Rozenbilt, J. (2017). Probabilistic threat detection for risk management in cyber-physical medical systems. *IEEE Software, 35*(1), 38-43. doi:10.1109/MS.2017.4541031

Rho, H., & Yu, I. (2011). *The impact of information technology threat avoidance factors on avoidance behaviour of user*. Dep. Bus. Manag. Sunc. Natl. Univ.

https://www.researchgate.net/publication/228769273_The_impact_of_information_technology_threat_avoidance_factors_on_avoidance_behavior_of_user

Rjaibi, N., & Rabai, L. B. A. (2015). Developing a novel holistic taxonomy of security requirements. *Procedia Computer Science, 62*, 213-220. doi:10.1016/j.procs.2015.08.442

Rumelhart, D. E. (2017). Schemata: The Building Blocks of Cognition. In *Theoretical Issues in Reading Comprehension,* 33-58. doi:10.4324/97813

Sametinger, J., Rozenblit, J., Lysecky, R., & Ott, P. (2015). Security challenges for medical devices. *Communications of the AMC, 58*(4), 74-82. doi:10.1145/2667218

SANS. (2018). *CIS critical security controls: Guidelines*. SANS Institute. https://www.sans.org/critical-security-controls/guidelines

Schwartz, S., Ross, A., Carmody, S., Chase, P., Coley, S. C., Connolly, J., & Zuk, M. (2018). The evolving state of medical device cybersecurity. *Biomedical Instrumentation & Technology, 52*(2), 103-111. doi:10.2345/0899-8205-52.2.103

Sczyrba, A., Hofmann, P., Belmann, P., Koslicki, D., Janssen, S., Dröge, J., ... & Bremges, A. (2017). Critical assessment of metagenome interpretation—a benchmark of metagenomics software. *Nature Methods*, *14*, 1063-1071.

Seale, K. A. (2017). *Integrating relational data frameworks into risk assessment of networked medical devices* (Order No. 10267720). Available from ProQuest Dissertations & Theses Global. (1893567916).

Seale, K., McDonald, J., Glisson, W., Pardue, H., & Jacobs, M. (2018). *MedDevRisk: Risk analysis methodology for networked medical devices*. Proceedings of the 51st Hawaii International Conference on System Sciences. doi:10.24251/hicss.2018.414

Seifert, D., & Reza, H. (2016). A security analysis of cyber-physical systems architecture for healthcare. Computers, 5(4), 27. doi:10.3390/computers5040027

Shegewi, Mutaz, & Dunbrack, A., L. …Townsend, M. (2017). IDC future scape: Worldwide health industry 2018 predictions.

Shostack, A. (2014). *Threat modeling: Designing for security*. Hoboken, NJ: John Wiley & Sons.

Shuja, S. (2016). *Formal verification techniques for safety critical medical device software control* (Order No. 10146387). Available from ProQuest Dissertations & Theses Global. (1829567904).

Silverman, D. (Ed.). (2016). *Qualitative research*. Thousand Oaks, CA: Sage.

Smigielski, R. (2017). Hardening infusion pump communication software for medical device cybersecurity. *Biomedical Instrumentation & Technology*, 51, 46-51. doi:10.2345/0899-8205-51.s6.46

Speidel, R. (2018). Rules and policies – protection PII – Privacy Act. *U.S. General Services Administration*. https://www.gsa.gov/reference/gsa-privacy-program/rules-and-policies - protecting-pii-privacy-act

Stine, I., Rice, M., Dunlap, S., & Pecarina, J. (2017). A cyber risk scoring system for medical devices. International Journal of Critical Infrastructure Protection, 19, 32-46. doi:10.2016/j.ijcip.2017.04.001

Swim, R. (2012). Keeping data secure: Protected health information and medical equipment. *Biomedical Instrumentation & Technology, 46,* 278-280. doi:10.2345/0899-46.4.278

Terry, G., Hayfield, N., Clarke, V. & Braun, V. (2017). Thematic analysis. In Willig, C., & Rogers, W. *The SAGE Handbook of qualitative research in psychology*(pp. 17-36). London: SAGE Publications Ltd doi: 10.4135/9781526405555

Tran, V. T., Porcher, R., Falissard, B., & Ravaud, P. (2016). Point of data saturation was assessed using resampling methods in a survey with open-ended questions. *Journal of Clinical Epidemiology*, *80*, 88-96. doi:10.1016/j.jclinepi.2016.07.014

TrapX Labs. (2016). *Anatomy of an attack: MEDJACK (medical device hijack).* http://deceive.trapx.com/rs/929-JEW-675/images/AOA_

U. S. Congress. (2014). Cybersecurity Enhancement Act of 2014. Public Law, 113-274. https://www.govinfo.gov/app/details/PLAW-113publ274/

U. S. Department of Labor. (2018). *Guidance on the protection of personal identifiable information*. https://www.dol.gov/general/ppii

U. S. Food & Drug Administration. (n.d.). *FDA basics - What is a medical device?* Center for Devices and Radiological Health. https://www.fda.gov/media/96118/download

U. S. Food & Drug Administration. (2013). *Content of premarket submissions for management of cybersecurity in medical devices - Draft guidance for industry and Food and Drug Administration staff*. Silver Spring, MD.

U. S. Food & Drug Administration. (2016a). *Medical device reporting for manufacturers*. https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidanceocuments/ucm359566.pdf

U. S. Food & Drug Administration. (2016b). *Postmarket management of cybersecurity in medical devices: Guidance for industry and food and drug administration staff*. U.S. Department of Health and Human Services, Food and Drug Administration Centers for

Devices and Radiological Health, Office of the Center Director, Center for Biologics Evaluation and Research. https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm482022.pdf

U. S. Food & Drug Administration. (2017a). CFR - Code of Federal Regulations Title 21. https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch. cfm?CFRPart=807

U. S. Food & Drug Administration. (2017b). *Who must register, list and pay the fee*? https://www.fda.gov/medical-devices/device-registration-and-listing/who-must-register-list-and-pay-fee

U. S. Food & Drug Administration. (2018a). Law enforced by FDA. https://www.fda.gov/RegulatoryInformation/LawsEnforcedbyFDA/default.htm

U. S. Food & Drug Administration. (2018b). Medical device reporting (MDR). https://www.fda.gov/MedicalDevices/Safety/ReportaProblem/default.htm

U. S. Food & Drug Administration. (2018c). MedWatch voluntary reporting form. https://www.accessdata.fda.gov/scripts/medwatch/index.cfm?action=reporting.home

U. S. Food & Drug Administration. (2018d). MAUDE - Manufacturer and user facility device experience. https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/ cfMAUDE/search.CFM

U. S. Food & Drug Administration. (2018e). *Information for healthcare organizations about FDA's guidance for industry: Cybersecurity for networked medical devices containing off-the-shelf (OTS) software.* https://www.fda.gov/RegulatoryInformation/Guidances/ucm070634.htm

U. S. Food & Drug Administration. (2019a). *FDA fact sheet*. https://www.fda.gov/downloads/medicaldevices/digitalhealth/ucm544684.pdf

U. S. Food and Drug Administration. (2019b). Manufacturer and User Facility Device Experience Database (MAUDE). Device data for problem codes. https://www.fda.gov/medical-devices/mandatory-reporting-requirements-manufacturers-importers-and-device-user-facilities/manufacturer-and-user-facility-device-experience-database-maude

Webb, T., Dayal, S., & Lawyers, C. U. (2017). *Building the wall: Addressing cybersecurity risks in medical devices in the U.S.A. and Australia*. Computer Law & Security Review, 33, 559-563. doi:10.1016/j.clsr.2017.05004

Weininger, S., Jaffe, M. B., & Goldman, J. M. (2017). The Need to Apply Medical Device Informatics in Developing Standards for Safe Interoperable Medical Systems. *Anesthesia and Analgesia*, *124*(1), 127-135. doi:10.1213/ane.0000000000001386

Whitman, M. (2003). Enemy at the gate: Threats to information security. *Communications of the ACM, 46*(8), 91-95. doi:10.1145/859670.8*59675*

Williams, P. H., & McCauley, V. (2016). Always connected: The security challenges of the healthcare internet of things. *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, Reston, VA, 2016, pp. 30-35. doi:10.1109/WF-IoT.2016.7845455

William, P. H., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem. *Medical Devices, 8*, 305-316. doi:10. 2147/MDER.S50048

Wilson, A., & Rollman, A. (2017). Cybersecurity for medical devices in a connected healthcare system. *Wind River*, Alameda, CA. 1-10.

Wong, K. K., & Hui, S. C. (2015). Ethical principles and standards for the conduct of biomedical research and publication. *Australasian Physical & Engineering Sciences in Medicine*, *38*, 377-380. doi:10.1007/s13246-015-0364-3

Wu, L., Du, X., Guizani, M., & Mohamed, A. (2017). Access Control Schemes for Implantable Medical Devices: A Survey. *IEEE Internet of Things Journal*, *4*, 1272-1283. doi:10.1109/jiot.2017.2708042

Young, D. K., Carpenter, D., & McLeod, A. (2016). Malware avoidance motivations and behaviors: A technology threat avoidance replication. *AIS Transactions on Replication Research, 2*, 1-17. doi:10.17705/1atrr.00015

Yuan, S., Fernando, A., & Klonoff, D. C. (2018). Standards for medical device cybersecurity in 2018. *Journal of Diabetes Science and Technology,* 193229681876363. doi:10.1177/1932296818763634

Zavitsanou, S., Chakrabarty, A., Dassau, E., & Doyle, F. (2016). Embedded Control in Wearable Medical Devices: Application to the Artificial Pancreas. Processes, 4(4), 35. doi:10.3390/pr4040035

Zeitler, E. P., Friedman, D. J., Loring, Z., Campbell, K. B., Goldstein, S. A., Wegermann, Z. K., … Piccini, J. P. (2019). Complications involving the subcutaneous implantable cardioverter-defibrillator: Lessons learned from MAUDE. *Heart Rhythm*. doi:10.1016/j.hrthm.2019.09.024

Zhang, S., Ou, X., & Caragea, D. (2015). Predicting Cyber Risks through National Vulnerability Database. *Information Security Journal: A Global Perspective*, *24*(4-6), 194-206. doi:10.1080/19393555.2015.1111961

APPENDIX A. RESEARCHER DEVELOPED INTERVIEW GUIDE

Demographic Characteristics

1. How old are you?
2. How long have you worked in facilities using networked medical devices?

Protocol (Round 1)

1. Please tell me about your experiences when analyzing security risks for networked medical devices.
2. What cyber threats have you considered with networked medical devices?
3. How did you address these cyber threats you consider?
4. What are the security measures have you implement when using these networked medical devices?
5. What actual cyber-attacks or cybersecurity failure did you experience with the use of the networked medical device, if any?
6. How did you address the attack or failure on the networked medical devices?
7. Why do you think the attack happened despite the security measures put in place?
8. How do you think you could have prevented the attacks or failures from happening?
9. What analytical tool do you use if any to analyze security risks for networked medical devices?
10. What are the characteristics that you consider important when analyzing security risks for networked medical devices?
11. What are the experiences regarding successful schemas when analyzing networked medical devices?

12. What are the experiences regarding the difference between schemas in analyzing the cybersecurity data for medical devices?

13. What are the experiences regarding the failure within a schema when analyzing medical devices?

14. Overall, how were the different schemas useful to you in assessing cybersecurity of using networked medical devices?

15. Overall, how were the different schemas challenging you in assessing cybersecurity of using networked medical devices?

APPENDIX B. EMERGING THEMES

These are the major themes, as well as the accompanying subthemes, that emerged from the first round of interviews. Interviews will be conducted for comments on each of these, adding any revisions recognized by the interviewer that are necessary, or any explanations of what should be emphasized within each theme/subtheme. Fifteen of the 47 panelists who were recruited through Positly.com completed the interviews. Out of the interviews, four themes and multiple subthemes are in support of the Round 2 interviews to be further addressed.

Major Theme 1. Cybersecurity Threats Encountered

The Theme 1, "Cybersecurity Threats Encountered" included 6 subthemes within parameters that focused on IT experts experience with how the threats were discovered in networked medical devices. These subthemes are placed within the order that were discovered to be more common from greater to least answered. Participants identified these threats from a personal perspective with configuration management, wireless and Bluetooth connections, Internet of Things, Data breaches, insider threat, and asset management as cybersecurity threats in networked medical devices.

Major theme 1: Cybersecurity threats encountered

- Subtheme 1a: Configuration Management
- Subtheme 1b: Wireless and Bluetooth Connection
- Subtheme 1c: Internet of Things
- Subtheme 1d: Data Breaches
- Subtheme 1e: Insider Threat
- Subtheme 1f: Asset Management

Major theme 1: Do you have any experience that you want to share? OR Do you agree with this theme or recommend changes, if so what are they?

Major Theme 2. How to Address Cybersecurity Threats

Major Theme 2, "How to Address Cybersecurity Threats" included four subthemes within parameters that focused on applying protective mechanisms that could help provide a defense for networked medical devices. IT experts who were participants identified how to address these cybersecurity threats from a personal perspective by controls assessment, automated technology, policy changes, and security awareness and training.

Major theme 2: How to address cybersecurity threats

Subtheme 2a: Controls assessment

Subtheme 2b: Automated technology

Subtheme 2c: Policy changes

Subtheme 2d: Security awareness and training

Major theme 2: Do you have any experience that you want to share? OR Do you agree with this theme or recommend changes, if so, what are they?

Major Theme 3, Medical Devices and Cyberthreats

Major Theme 3, "Medical Devices and Cyberthreats," included six subthemes within parameters that focused on what the IT expert who were participants identified when analyzed issues that they faced with networked medical devices. The first subtheme "Security Measures," included four items that if were implemented or applied would be the top four considerations to protect networked medical devices at a first level of defense. The second subtheme "Cybersecurity Failures Experienced," included three items that were found to be the most

experienced with the IT experts. The third subtheme “Addressing Cybersecurity Failures,” included three items that were most prevalent found in failures with networked medical devices. The fourth subtheme “Reasons for Failure,” included three items that were found to be the most reasons found by IT experts within networked medical devices. The fifth subtheme “Prevention of Failures,” included only one item that all IT experts reported as active monitoring networked medical devices would actively prevent cyber threats with networked medical devices. The sixth subtheme “Analytical Tools for Security Risk,” included four items that were used by IT experts for performing analytical risks when actively monitoring networked medical devices.

Major theme 3: Medical Devices and Cyberthreats

Subtheme 3a: Security measures

- Physical, Operational, Management, Technical controls assessment
- Policy
- Encryption
- Eliminations and Blocks

Subtheme 3b: Cybersecurity Failures Experienced

-Malicious attacks

-Denial of Service attacks

-Mechanism failure

Subtheme 3c: Addressing Cybersecurity Failures

-Lock down and monitoring of devices

-Report failure

-Automated tools

Subtheme 3d: Reasons for Failure

-Device management

-Issues of monitoring

-Threats always exist

Subtheme 3e: Prevention of Failures

-Active monitoring

Subtheme 3f: Analytical Tools for Security Risk

-Splunk

-APP Scan

-NESSUX

-Tools to analyze security risk

•Continuous monitoring

•Privacy and patient data

•Limiting access

Major theme 3: Do you have any experience that you want to share? OR Do you agree with this theme or recommend changes, if so, what are they?

Major Theme 4, Schemas and Medical Devices

Major theme4, "Schemas and Medical Devices" includes three subthemes concerning IT experts who were participants experienced when analyzing risks for networked medical devices. The first subtheme "Successful Schemas" included three items that were used by IT experts based on priority of methods used. The second subtheme "Differences between Schemas" included two items that focused on what priorities to defend and monitor. The third subtheme "Failures with Schemas" included three items that were found by IT experts that did not work or found problems within the schemas.

Major theme 4: Schemas and Medical Devices

Subtheme 4a: Successful Schemas

-Security controls monitoring

-Patch version

-Manufacturer data

-Characteristics for a successful schema

- Real time monitoring
- Manual vs. automated
- Mitigating risk

Subtheme 4b: Differences between Schemas

-PHI versus PII

-Dependent on medical device

Subtheme 4c: Failures with schemas

-Compromise of data and/or device

-Technology

-Characteristics of failed schemas

- Differences between technologies
- Misalignment with vision of organization

Major theme 4: Do you have any experience that you want to share? OR Do you agree with this theme or recommend changes, if so, what are they?