5-2023

Risk Assessment Framework for Evaluation of Cybersecurity Threats and Vulnerabilities in Medical Devices

Maureen S. Van Devender

RISK ASSESSMENT FRAMEWORK FOR EVALUATION OF CYBERSECURITY THREATS AND VULNERABILITIES IN MEDICAL DEVICES

A Dissertation

Submitted to the Graduate Faculty of the
University of South Alabama
in partial fulfillment of the
requirements for the degree of

Doctor of Philosophy

in

Computing

by
Maureen S. Van Devender
B. S., University of South Alabama, 1991
MBA, Spring Hill College, 2002
May 2023

ACKNOWLEDGEMENTS

I would like to express my love and gratitude to my husband, Odie for his undying support of me through this process. Thank you for being there for me to lean on in so many ways. I would also like to thank my parents for instilling in me the value of an education, and to my family and friends for all the prayers and encouragement along the way.

I would like to thank my chair, Dr. Todd McDonald for encouraging me to pursue this line of research. In addition, I would like to acknowledge and express my appreciation to my committee, Dr. Harold Pardue, Dr. Brad Glisson, Dr. Mike Jacobs, and Dr. Todd Andel.

Finally, I would like to thank the School of Computing leadership team, my colleagues, and my fellow doctoral students for their support and encouragement during my journey.

TABLE OF CONTENTS

Page

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AAMI	Association for the Advancement of Medical Instrumentation
ANSI	American National Standards Institute
ASHRM	American Society for Healthcare Risk Management
CAPEC	Common Attack Pattern Enumerations and Classifications
CAS	Casualty Actuarial Society
CIA	Confidentiality, Itegrity, Availabliity
CIS	Center for Inernet Security
CIS RAM	Center for Inernet Security Risk Assessment Methodology
CISA	Cybersecurity and Infrastructure Security Agency
COBIT	Control Objectives for Information and Related Technologies
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CPE	Common Platform Enumeration
CSF	HITRUST Common Security Framework
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
DHS	Department of Homeland Security
DOJ	Department of Justice

DRE	Direct Recorded Electronic
DVI	Digital Visual Interface
EDPAA	Electronic Data Process Auditors' Association
EHR	Electronic Health Records
EMI	Electromagnetic Interference
ERM	Enterprise Risk Management
EU	European Union
FAIR	Factor Analysis of Information Risk
FBI	Federal Bureau of Investigation
FD&C Act	Food, Drug, and Cosmetic Act
FDA	Food and Drug Administration
FDA Medsun	Food and Drug Administration Medical Product Safety Network
FIPS	Federal Information Processing Standards
FISMA	Federal Information Systems Modernization Act of 2014
FLASH	FBI Liaison Alert System
FRAP	Facilitated Risk Analysis Process
GDPR	General Data Protection Regulation
HB	Heuristics and Biases
HIMSS	Health Information and Management Systems Society, Inc.
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health
HITRUST	The HITRUST Alliance
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team

ICT	Information Communication Technology
IEEE	Institute of Electrical and Electronics Engineers
IG	Implementation Group
IMD	Implantable Medical Device
ISACA	Information Systems Audit and Control Association
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
IT	Information Technology
ITL	Information Technology Lab
ITP	Interoperable Telesurgery Protocol
JAR	Joint Analysis Reports (FBI & DHS)
JTA	Joint Technical Advisories (FBI & DHS)
LAN	Local Area Network
LEF	Loss Event Frequency
MAC	Media Access Control
MacOS	Apple Mac Operating System
MAPI	Manufacturers Alliance for Productivity and Innovation
MAUDE	Manufacturer and User Facility Device Experience
Max	Maximum
MCPS	Medical Device Cyber Physical Systems
MDR	Medical Device Reports

MDS2	Manufacturer Disclosure Statement for Medical Device Security
Min	Minimum
MITA	Medical Imaging & Technology Alliance
MITA	Medical Imaging and Technology Alliance
NDM	Naturalistic Decision Making
NEMA	National Electronical Manufacturers Association
NIAP	The National Information Assuance Partnership
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OSINT	Open-Source Intelligence Techniques
OVAL	Open Vulnerability and Assessment Language
OWASP	Open Worldwide Application Security Project
PACS	Picture Archiving and Communication System
PCI	Payment Card Industry Data Security Standard
PERT	Program Evaluation and Review Technique
PHI	Protected Health Informatin
PII	Personally Identifiable Information
PIN	FBI Private Industry Notificaiton
RJ45	Registered Jack 45
RMF	Risk Management Framework
RS-232	Recommended Standard 232
RTOS	Real Time Operating System
SCAP	Security Content Automation Protocol

SCIMD	Security Criteria for Integrated Medical Devices
SCRM	Supply Chain Risk Management
SDI	Serial Digital Interface
SDLC	System Development Lifecycle
SFP	Small Form-factor Pluggable
SLM	Single Loss Magnitude
STRIDE	Spoofing, Tamperinc, Repudiation, Information disclosure, Denial of service, and Elevation of privileges
SWOT	Strengths, Weaknesses, Opportunities , and Threats
TAC	Threat Actor Capability
TADMUS	Tactical Decision Making Under Stress
TEF	Threat Event Frequency
TRS	Tip-Ring-Sleeve jack
TTP	Tactics, Techniques, and Procedures
TVA	Threat, Vulnerability, Asset
TVA-C	Threat, Vulnerability, Asset, Control
UML	Unified Markup Language
USB	Universal Serial Bus
UTP	Unshielded Twisted Pair
VDBR	Verizon Data Breach Report
VGA	Video Graphics Array
VLAN	Virtual Local Area Network
WAN	Wide Area Network

XML	Extensible Markkup Language

ABSTRACT

Maureen S. Van Devender, PhD, University of South Alabama, May 2023. Risk Assessment Framework for Evaluation of Cybersecurity Threats and Vulnerabilities in Medical Devices. Chair of Committee: Jeffrey T. McDonald, Ph.D.

Medical devices are vulnerable to cybersecurity exploitation and, while they can provide improvements to clinical care, they can put healthcare organizations and their patients at risk of adverse impacts. Evidence has shown that the proliferation of devices on medical networks present cybersecurity challenges for healthcare organizations due to their lack of built-in cybersecurity controls and the inability for organizations to implement security controls on them. The negative impacts of cybersecurity exploitation in healthcare can include the loss of patient confidentiality, risk to patient safety, negative financial consequences for the organization, and loss of business reputation. Assessing the risk of vulnerabilities and threats to medical devices can inform healthcare organizations toward prioritization of resources to reduce risk most effectively.

In this research, we build upon a database-driven approach to risk assessment that is based on the elements of threat, vulnerability, asset, and control (TVA-C). We contribute a novel framework for the cybersecurity risk assessment of medical devices. Using a series of papers, we answer questions related to the risk assessment of networked medical devices. We first conducted a case study empirical analysis that determined the scope of security vulnerabilities in a typical computerized medical environment. We then

created a cybersecurity risk framework to identify threats and vulnerabilities to medical devices and produce a quantified risk assessment. These results supported actionable decision making at managerial and operational levels of a typical healthcare organization. Finally, we applied the framework using a data set of medical devices received from a partnering healthcare organization. We compare the assessment results of our framework to a commercial risk assessment vulnerability management system used to analyze the same assets. The study also compares our framework results to the NIST Common Vulnerability Scoring System (CVSS) scores related to identified vulnerabilities reported through the Common Vulnerability and Exposure (CVE) program.

As a result of these studies, we recognize several contributions to the area of healthcare cybersecurity. To begin with, we provide the first comprehensive vulnerability assessment of a robotic surgical environment, using a da Vinci surgical robot along with its supporting computing assets. This assessment supports the assertion that networked computer environments are at risk of being compromised in healthcare facilities. Next, our framework, known as MedDevRisk, provides a novel method for risk quantification. In addition, our assessment approach uniquely considers the assets that are of value to a medical organization, going beyond the medical device itself. Finally, our incorporation of risk scenarios into the framework represents a novel approach to medical device risk assessment, which was synthesized from other well-known standards. To our knowledge, our research is the first to apply a quantified assessment framework to the problem area of healthcare cybersecurity and medical networked devices. We would conclude that a reduction in the uncertainty about the riskiness of the cybersecurity status of medical devices can be achieved using this framework.

CHAPTER I

INTRODUCTION

In February 2018, The Council of Economic Advisers to the President of the United States (US) reported that malicious cyber activity cost the US economy an estimated $57 to $109 billion in 2016 [1]. The report places healthcare at approximately seven percent of the Gross Domestic Product, yet it experienced more than 15 percent of the reported cybersecurity breaches in 2016 [1]. This report, among others [2], [3], highlights the cybersecurity risk exposure present in the healthcare.

A proliferation of technology into the healthcare sector is being encouraged by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 which requires the implementation of Electronic Health Records (EHR) for all healthcare providers that participate in Medicare or Medicaid [4]. In addition, the number of computerized medical devices deployed in healthcare is growing, and medical devices are becoming increasingly interconnected in larger network environments. These factors increase the complexity of providing cybersecurity protection in healthcare. The Federal Bureau of Investigation (FBI) predicted that enticing exploitation opportunities would be created due to the mass deployment of medical technology as a result of the HITECH Act [5] . The FBI goes on to state that the healthcare industry is not prepared to protect

against basic cyber-attacks, much less more sophisticated Advanced Persistent Threats (APTs).

Exhibiting that the opportunity is recognized by criminals, the Ponemon Institute reports that criminal attacks in the healthcare industry increased 125 percent from 2010 to 2015 [6]. The press release also emphasizes that most healthcare organizations are not prepared to handle cyber threat environments [6]. The Ponemon Institute goes on to report in 2016 that healthcare data breaches continue to rise and become increasingly costly, estimating that the industry cost may be $6.2 billion annually [7]. Confirmation of the ill-preparedness of healthcare organizations to deal with cyber threats is visible in news that Hollywood Presbyterian Medical Center acquiesced to a ransom-wear attack [8]. Supporting the Ponemon claim, in a 2015 survey of executives at large U. S. healthcare organizations, KPMG finds that 80% say their information technology has been compromised by cyber attacks [9]. In the same report, only 55% of the executives report having sufficient resources to handle security incidents and a fewer 35% say they have sufficient resources to manage vendor security risks [9].

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) sets national standards for protecting individually identifiable information and the confidentiality, integrity, and availability of electronic protected health information [10]. The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 [11] addresses privacy and security concerns through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules including increasing penalties for breaches of unsecured PHI to as much as $1.5m per incident [4].

The European Union (EU) parliament approved the EU General Data Protection Regulation (GDPR) in 2016, and it became effective in May 2018 [12]. GDPR applies not only to organizations operating within the European Union, but to any organization that processes the data of any EU subject (individual). The penalties for violating the GDPR can be up to four percent of total company revenue or 20 million Euros, whichever is greater. The regulation applies to both the controllers and the processors of data, meaning the provider and any third-party processor. GDPR requires breach notification to those individuals affected by the breach within 72 hours of first becoming aware of the breach. US healthcare providers fall under GDPR regulation with respect to EU subjects whose data they hold.

The healthcare industry is considerable in size and a growing market in the United States, accounting $3.5 trillion of the gross domestic product in 2017 [13]. There are approximately 5,534 hospitals in the United States in 2016 [14], with approximately 90% of them having achieved certification in meaningful use of information technology [15] as required by the HITECH Act. By 2015, approximately 87% of all physician offices have implemented some type of EHR [15].

Research has shown that medical devices lack the security necessary to protect them from cyber criminals. For example, research reported in Bloomberg Businessweek claims that it is possible to hack a Hospira drug pump and control the settings [2], an activity that prompted one of several warnings from the FDA regarding cyber vulnerabilities in medical devices [16], [17] and an advisory [18] from the Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). In other research, TrapX Labs reports the results of a study of advanced

persistent threats at three medical institutions with medical devices serving as the primary pivot points for attackers [19]. Based on their experience, it is Trap X's belief that a large majority of hospitals are infected with malware that has remained undetected for an extended period of time.

The FDA regulates all medical devices sold and operated in the United States. The organization's roots date back to 1906 [20], with medical device regulation beginning with the Medical Device Amendments of 1976 [21], followed up in 1990 with the Safe Medical Devices Act [22]. The agency has built a strong system of ensuring devices keep patients and operators safe from harm. Cybersecurity presents a new challenge to the FDA. Concern for the threat of cybersecurity vulnerabilities in medical devices was first addressed in FDA publications in 2013 [17]. There are efforts ongoing to encourage manufacturers to consider security in the design of devices and that proper reporting and patching occurs when vulnerabilities are discovered on devices that are in use. The FDA's guidance is for manufacturers and practitioners to work together to ensure medical devices cybersecurity is the most effective.

Healthcare providers are bound to protect patient information and to keep patients safe from harm by regulations [4], [23] and optional, but important, industry accreditation. Most prominent among healthcare industry accreditation bodies is the Joint Commission [24]. As part of protecting patient information and keeping patients safe from harm, providers are required by regulation to perform risk assessments and implement reasonable controls to mitigate risk [4]. This is a complex and difficult task, particularly with medical devices, because the vulnerabilities that create risk are not always clear to the healthcare organization. Known cybersecurity vulnerabilities are

published and discoverable, however, the software and hardware components of medical devices are not always known. Furthermore, there exists no master list of the hardware and software components of medical devices that could be used for comparison against known cybersecurity vulnerabilities. These conditions make it difficult for healthcare organizations to identify and quantify the risk imposed by computerized medical devices, and therefore to maximize the effectiveness of mitigation strategies.

Existing prominent risk modelling frameworks and systems, such as those developed by National Institute of Standards and Technology (NIST) [25], International Organization for Standardization (ISO) [26], The HITRUST Alliance [27], The Center for Internet Security (CIS) [28], ISACA [29], and National Electrical Manufacturers Association (NEMA) [30] are considered for incorporation into the framework. The following tools have been identified as potential sources of information regarding threats, vulnerabilities, and medical devices. First, the continuously updated CAPEC [31] threat catalog maintained by the MITRE Corporation [32] could serve as a threat library. Second, the National Vulnerability Database (NVD) [33] maintained by the National Institute of Standards and Technology (NIST) [25] is a continuously updated vulnerability library that could be incorporated into the system. Third, the Open Vulnerability and Assessment Language (OVAL) [34] is a tool that can be used to capture information and machine states of devices on a live network. OVAL could be used to capture medical device inventory information from live medical networks. Fourth, the Security Content Automation Protocol (SCAP) [35] is a community effort overseen by NIST [25] that contains standardized expressions and reporting for the purpose of security automation. Of particular interest in SCAP is Common Platform

Enumeration (CPE) [36] which is a structured naming scheme for describing and identifying classes of applications, operating systems, and hardware devices. NIST hosts and maintains the official CPE dictionary, which is available to the public, and accepts contributions from organizations for inclusion in the dictionary. A search of the CPE dictionary reveals that it contains entries for medical devices including component specifications that have known vulnerabilities in the NVD. This could be a useful source for identifying vulnerabilities in particular medical device configurations. Finally, NEMA/MITA HN 1-2019 [37] aka ANSI/NEMA HN 1-2019 [38], the current version of a voluntary standard published by The Medical Imaging & Technology Alliance (MITA) [39], a subsidiary of NEMA [30], provides for Manufacturer Disclosure Statement for Medical Device Security (MDS2) documents. These documents, completed by device manufacturers, contain information about the security controls and handling of personally identifiable information on a medical device. The information is intended to support healthcare delivery organizations in executing risk assessments and in their management of medical device security capabilities [38]. When available, these documents can provide useful information about an individual device. Because the standard is voluntary, the information may not always be available. In addition, the information is contained on an electronic document form, so automating the collection of the data would be required to scale the use of the MDS2 form.

1.1 Purpose

Research and media reports claiming that medical devices lack the security to protect them from cyber criminals and that medical environments are at risk due to cyber-

criminal activity prompted the hypothesis that a tool for assessing and quantifying the risk posed by medical devices could provide healthcare organizations with a tool for optimizing mitigation efforts. This research seeks to answer the following research questions:

1. How are opportunities to Compromise Medical Environments Identified?
2. What are the factors that influence cyber risk assessment of medical devices?
3. How can we quantify the risk factors into meaningful/actionable information?
4. Can expert predictions be useful in quantifying cybersecurity uncertainty?

1.2 Research Goals and Contributions

This research aims to provide a framework for risk assessment of cybersecurity vulnerabilities in medical devices that is useful at the managerial and operational level within healthcare organizations. The goal is to use quantitative methods along with industry standards to arrive at risk assessment results. We build upon previous work that utilizes a database model for risk assessment of networked medical devices [40]–[42], [43] based upon a Threat-Vulnerability-Asset (TVA) data schema. The framework seeks to identify and quantify risk and to provide a healthcare organization with actionable information for prioritizing and mitigating risks.

Essential to the success of this research is the recruitment of collaborating partners in the form of healthcare organizations. The goal of collaborating with medical organizations is twofold. First, it is desirable to have healthcare organization input into the design of the framework. Second, real-world data improves testing of the model.

1.3 Dissertation Outline

The remainder of the dissertation is structured as follows: Chapter II discusses relevant medical device, vulnerability, threat, risk assessments, and frameworks research. Chapter III is an examination of the foundational work for the purpose of providing an understanding of the existing database model. Chapter IV presents our methodology. Chapter V presents a case study that identifies opportunities to compromise medical devices. Chapter VI presents a framework for assessing the risk of networked medical devices. Chapter VII presents a case study applying the framework to medical devices at a partnering healthcare facility, and chapter VIII presents conclusions and future directions.

CHAPTER II

BACKGROUND

This chapter outlines industry and government standards and published research in areas relevant to this research. First, a definition of a medical device as it pertains to this research is provided. Next, regulatory standards and guidance organizations that provide cybersecurity vulnerability and threat information used in this research are presented. Lastly, and most extensively the topic of risk is presented. Risk organizations and standard frameworks are discussed. In addition, peer-reviewed research covering methods for quantifying risk, understanding the perception of risk, and methods for predicting future outcomes are presented. Finally, the topic of Enterprise Risk Management (ERM) is presented including its history and prominent ERM frameworks.

2.1 Medical Device

The Food and Drug Administration (FDA), established in 1906 [20], regulates all medical devices sold and operated in the United States. The FDA enforces the Food, Drug, and Cosmetic Act (FD&C Act) [44] which defines a medical device as "an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part, or accessory which is:

1. recognized in the official National Formulary, or the United States Pharmacopoeia, or any supplement to them,
2. intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or
3. intended to affect the structure or any function of the body of man or other animals, and which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of its primary intended purposes.

The term "device" does not include software functions excluded pursuant to section 520(o).” [44]

The FD&C Act was amended as a result of the enactment of the 21st Century Cures Act [45]. Section 520(o) [46] of the FD&C was added to distinguish some medical technology from medical devices. Specifically, it excludes software that is intended for:

1. administrative support of a healthcare facility
2. maintaining for encouraging a healthy lifestyle
3. the maintenance and accessibility of patient and provider records
4. transferring, storing, or converting lab results or other test results

This research narrows the definition of a medical device to any device that falls within the FDA definition of a medical device and is also a networked computer device.

The FD&C Act provides for a classification of medical devices as Class I, Class II, or Class III [47]. The classification is based upon the risk to patient safety and the amount of regulatory control necessary to ensure safety and effectiveness. Class I devices

are generally the lowest risk devices, and Class III are the highest risk to safety [48]. This research will consider devices in any of the three categories.

Distinguishing medical devices from other computer devices operating on the network may not be straight forward. Medical devices may run common off-the-shelf operating systems such as Windows. Identifying medical devices based on MAC address is a possibility. Identification of medical devices by MAC address is a common method for authentication of medical devices on a network [49].

2.2 Vulnerability

With the proliferation of medical devices into healthcare has come intense interest from industry and regulators to mitigate cybersecurity vulnerabilities while maintaining patient safety. Activity includes the presentation of threat modeling for cybersecurity vulnerabilities by the FDA and a recommendation that device manufacturers have processes in place for assessing the exploitability of cybersecurity vulnerabilities, and the development of the assessment tool Common Vulnerability Scoring System (CVSS) [50] by an international industry group. In addition, the FDA provides recommendations for cybersecurity considerations to be included in the product lifecycle of medical devices [51].

NIST maintains a standards-based repository of vulnerability management data in the National Vulnerability Database (NVD) [33] using the standards in the Security Content Automation Protocol (SCAP) [35]. The repository is available to the public, and together with SCAP, enable the automation of vulnerability management. Each

vulnerability in the repository contains a severity score using the CVSSv3 [52] standard and a cross-reference to all the effected platforms.

The U. S. Department of Homeland Security (DHS) [53] Cybersecurity and Infrastructure Security Agency (CISA) [54] maintains a publicly available repository of alerts relating to security issues, vulnerabilities, and exploits. The alerts include vulnerabilities that are published in the NVD.

2.3 Threat

In recognition of the unprecedented threat to the nation posed by the malicious use of technology, in February 2018, the Attorney General of the United States ordered the creation of the Cyber-Digital Task Force to operate within the Department of Justice (DOJ) [55], [54], [50], [49], [48]. Among the priorities the task force is asked to study and report on are: “theft of corporate, governmental, and private information on a mass scale” and “mass exploitation of computers and other digital devices to attack American citizens and businesses” [55], [54], [50], [49], [48]. The task force published a report on July 2, 2018 [56]. Chapter two of the report categorizes and describes the most serious cyber schemes that are facing the nation. These are: damage through attacks such as DDoS and ransomware, data theft, personally identifiable information and intellectual property, fraud/carding schemes, crimes threatening personal privacy, and crimes threatening critical infrastructure. The report goes on to describe the most common tools being used by cyber criminals to breach security defenses, and notes that while the threats have changed over time the tools have been “remarkably resilient” [56]. The tools are: social engineering, malicious software, botnets, and criminal infrastructures often using

the Dark Web, and web hosting companies that are willing to host malicious servers, often in geographical locations with little regulation.

Chapter 4 of the report describes the DOJ's role in responding to, preventing, and managing, cyber incidents [56]. The Federal Bureau of Investigation (FBI), an agency of the DOJ, is responsible for among other things, "protecting the US against cyber-based attacks and high-technology crimes" [57]. The FBI engages the community in their preparation efforts by establishing relationships, sharing routine information, and engaging organizations and sectors that are at particular risk of cyber incidents. Table 1 shows common FBI communication reports designed to alert private industry concerning cyber threats. The reports include: Private Industry Notifications (PINs) which provide information about emerging threats and FBI Liaison Alert System (FLASH) reports that provide technical indicators gathered through investigations or intelligence. These two public communication reporting types provide actionable information to help recipients protect against cyber threats and assist in detecting exploitation. The FBI also partners with the Department of Homeland Security (DHS) and other federal agencies to produce public Joint Analysis Reports (JARs) and Joint Technical Advisories (JTAs) to alert private industry to technical details and indicators discovered through joint efforts with these federal agencies.

Table 1. FBI Public Cyber Threat Reporting.

Product	Private Industry Notifications (PINs)	FBI Liaison Alert System (FLASH)	Joint Analysis Reports (JARs) and Joint Technical Advisories (JTAs)
Author	FBI	FBI	FBI with DHS and other Government Agencies
Content	Information about ongoing or emerging cyberthreats	Technical indicators learned through investigations or intelligence	Technical indicators learned through investigations or intelligence
Audience	Private industry	Selected partners/ target industries	Private industry

2.4 Risk

The NIST definition of risk is "a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence" [58]. NIST defines Risk Management as "the ongoing process of identifying, assessing, and responding to risk [59]. They point out that managing risk requires an organization to understand the likelihood that an event will occur and the potential impact to the organization that could result from the event. With this information, an organization can determine their risk tolerance by evaluating the acceptable levels of risk for achieving the organizational objectives. Organizational risk tolerance can guide an organization's decisions related to prioritizing cybersecurity activities.

The International Organization for Standardization (ISO) [26] defines risk as "the effect of uncertainty on objectives where the effect is a deviation from the expected and

uncertainty is the state of deficiency of information related to an event, its consequence, or likelihood" [60]. ISO defines risk assessment as the overall process of risk identification, risk analysis, and risk evaluation [60].

2.4.1 Cybersecurity Risk Organizations

There are several organizations that have an interest in improving cybersecurity. These organizations have interest and influence that range from specific business sectors to national and international spheres. The organizations relevant for discussion here include NIST, ISO, ANSI, NIAP, The HITRUST Alliance, CIS and ISACA. A discussion of each follows.

2.4.1.1 National Institute of Standards and Technology (NIST).

The National Institute of Standards and Technology (NIST) [25] sets national standards and guidelines for measurement with its Information Technology Lab (ITL) [61] serving as the technical lead. Among ITLs responsibilities is the development of standards and guidelines for the security of information in federal information systems. ITL conducts research, produces guidelines, and conducts outreach efforts with industry, government, and academic organizations in information systems security and privacy. NIST's Special Publication 800-series reports the results of these activities.

NIST's role was expanded through the Cybersecurity Enhancement Act of 2014 [62] include providing guidance to critical infrastructure owners and operators by identifying and developing voluntary-use cybersecurity risk frameworks. In fulfillment of this role, NIST produced the Framework for Improving Critical Infrastructure Cybersecurity [59].

2.4.1.2 International Organization for Standardization (ISO).

The International Organization for Standardization (ISO) [26] is an international organization comprised of national standards bodies. ISO develops and publishes International Standards through stakeholder consensus. The 27000 series is comprised of information security standards that are of relevance to this work. ISO 27999 Health Informatics – Information Security Management provides provides guidelines for information security standards and practices.

2.4.1.3 American National Standards Institute (ANSI).

The American National Standards Institute (ANSI) [63] is a private non-profit organization that operates in the interest of the United States with respect to voluntary standards and conformity assessment. Their mission is to promote and facilitate voluntary consensus standards and assessment for the purpose of global competitiveness and quality of life. ANSI serves as the U S representative member of ISO.

2.4.1.4 The National Information Assurance Partnership (NIAP).

The National Information Assurance Partnership (NIAP) [64] oversees the evaluation of the security status of commercial information technology products. This organization is responsible for the implementation of the Common Criteria [65] in the United States. NIAP carries this out through the management of a program that ensures that risk assessment methods are documented, consistent, and repeatable by developing evaluation methodologies, approving testing laboratories, and ensuring that the Common Criteria is implemented consistently.

2.4.1.5 The HITRUST Alliance.

The HITRUST Alliance [27] is an international stakeholder organization composed of private and public sector representatives formed in 2007. The organization develops and maintains common risk and compliance management frameworks, related assessment and assurance methodologies for public access and utilization. Of significance to this work is the HITRUST CSF [66], a tool for regulatory compliance and risk management.

2.4.1.6 Center for Internet Security (CIS).

The Center for Internet Security (CIS) [28] is a non-profit organization focused on best-practice solutions for protecting against pervasive cyber threats. In collaboration with the global information security community, they have developed several tools to assist individuals, organizations, and governments improve their security posture. CIS offers best practices and guidelines that are free to the community as well as fee-based tools and services. Of significance to this research are the CIS Controls [67], a set of security best-practice guidelines for cybersecurity defense and CIS RAM [68], a cybersecurity risk assessment methodology.

2.4.1.7 ISACA.

ISACA [29] is an international professional association focused on optimizing IT utilization through effective technology management and governance. The organization was formed in the United States in 1967 by a group of computer systems professionals as an organization to provide a central source of information and guidance on audit controls. Originally named the Electronic Data Process Auditors' Association (EDPAA), it later became the Information Systems Audit and Control Association and eventually dropped

the full name in favor of the acronym ISACA that it uses today. ISACA is the creator of the COBIT [69] framework for information technology management and governance. In addition to COBIT, the organization also provides risk guidance through the Risk IT Framework [70].

2.4.1.8 National Electrical Manufacturers Association (NEMA).

The National Electrical Manufacturers Association (NEMA) [30] is an ANSI-accredited standards developing organization. Through its division Medical Imaging and Technology Alliance (MITA) [39], they published the standard ANSI/NEMA HN 1-2019 [38] which provides for Manufacturer Disclosure Statement for Medical Device Security (MDS2) documents. Through MDS2 documents, the standard provides support for healthcare delivery organizations in executing risk assessments and in their management of medical device security capabilities [38].

2.4.2 Risk Management Frameworks

There are several prominent risk management frameworks that are used both nationally and globally. Research is conducted to identify frameworks that are prominently used in industry with particular attention given to identify those used in the healthcare sector. An analysis of selected frameworks is done to identify the significant attributes of each with the goal of identifying attributes relevant to the healthcare domain. HIMSS introduced an annual survey in 2015 for the purpose of gaining insight into what healthcare organizations are doing to protect information assets considering the increased cyberattacks in the healthcare sector. The 2018 survey [71] produced feedback from 239 qualified information security professionals in a variety of healthcare organizations. The respondents included HIMSS members and non-members, as well as members of the

HIMSS Cybersecurity community. Of significance to this work is their response to a question regarding the use of a list of prominent cybersecurity frameworks.

Figure 1 shows the list of frameworks that were offered in the question and the response results. Respondents had the option of selecting more than one response to the question, and the choice of 'Other' was offered to the respondents. The results show that nearly 58 percent of respondents use the NIST framework, a rate much higher than any of the other options. As only about five percent of respondents selected the option of 'Other', it can be concluded that the list contains the frameworks that are used by a majority of responding healthcare organizations that use a framework. Another interesting finding in this survey is that nearly seventeen percent of respondents report that their organization uses no cybersecurity framework.

Framework	N	percent
NIST	**103**	**57.9%**
HITRUST	47	26.4%
Critical Security Controls	44	24.7%
ISO	7	18.5%
COBIT	13	7.3%
Other	9	5.1%
No security framework has been implemented at my organization	30	16.9%
Don't know	15	8.4%

Q. Which of the following security framework(s) does your organization use? Please select all that apply.

Figure 1. 2018 Survey of Cybersecurity Frameworks used in Healthcare [71].

The top five frameworks identified in this survey are among the frameworks identified for review in this research. Those covered here are: NIST Risk Management

Framework, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, Framework for Improving Critical Infrastructure Cybersecurity, ISO 27000 Information Technology – Security Techniques, HITRUST Common Security Framework, CIS Critical Security Controls, CIS Risk Assessment Methodology and COBIT.

2.4.2.1 NIST Risk Management Framework.

NIST developed a Risk Management Framework (RMF) [72] to "improve information security, strengthen risk management processes, and encourage reciprocity among organizations" [72]. RMF is intended to help organizations manage security and privacy risk, as well as to satisfy federal policy and regulation requirements such as the Privacy Act of 1974 [73], the Federal Information Systems Modernization Act of 2014 (FISMA) [74], the federal Office of Management and Budget [75] policies, and Federal Information Processing Standards (FIPS) [76]. The framework provides a means for organizations to develop security and privacy capabilities throughout the System Development Life Cycle (SDLC), to maintain situational awareness of security and privacy, and to inform senior leadership in order to facilitate decisions concerning the acceptance of risk to "organizational operations and assets, individuals, other organizations, and the Nation" [72] .

RMF is designed to be technology neutral to allow the methodology to be applied to any type of system or device, while providing for a custom set of controls and implementation details that are specific to the system or device. The framework includes seven steps that are summarized in Table 2. NIST provides supplemental guidance documents as indicated in the table.

Table 2. Seven Steps in NIST Risk Management Framework.

Steps in the NIST Risk Management Framework	
Prepare	Define the context and priorities for managing privacy and security from an organizational and system-level perspective; This step is added in the October 2018 final draft
Categorize	System and information processed, stored, and transmitted, based on impact analysis; security categorization guidance in FIPS 199 [77]
Select	An initial baseline set of security controls based on categorization; security control selection guidance in NIST SP 800-53 [78]
Implement	Implement and document how the security controls are implemented within the system and the environment
Assess	Use appropriate procedures to determine if the controls are: 1. implemented appropriately, 2. functioning as intended, and 3. producing the desired security outcome Security control assessment procedures in NIST 800-53A [79]
Authorize	Authorize operation of the system and decision that risk is acceptable with respect to: 1. organizational operations and assets 2. individuals 3. other organizations 4. the Nation Guidance provided in NIST SP 800-37 [72]
Monitor	Ongoing monitoring including: 1. assessing security control effectiveness 2. documenting changes to the system or operating environment 3. conducting security impact analysis of changes 4. reporting security state of system to appropriate organizational officials. Guidance provided in NIST SP 800-37 [72]

The prepare step involves the activities necessary at the organizational level and at the information system level to prepare for the risk assessment. The prepare step is

intended to identify and leverage existing activities being conducted within the organization and centralize them under organizational governance and provide resources to enable cost-effective consistent risk management across the organization. At the organization level, these activities include assigning roles and responsibilities, defining a risk management strategy, aggregating system level risk assessment results, identifying the control baseline and framework profiles, identifying common controls in place, prioritizing impact-levels, and continuous monitoring. At the system level, these activities include identifying the mission and business processes the system supports, identifying the stakeholders throughout the SDLC, identifying the assets associated with the system, determining the authorization boundary of the system, identifying the types of information processed, stored and transmitted by the system, identify the life cycle for all the types of information, conducting and documenting risk assessment results on an ongoing basis, defining and documenting the security requirements of the system, determining the placement of the system within the enterprise architecture, documenting the security and privacy requirements to be allocated to the system, and registering the system to inform the governing organization of the existence of the system and its key characteristics.

The categorization step involves categorizing the system in each of the three security objectives of confidentiality, integrity, and availability based on the impact to the organization should an event occur [80]. The impact categorizations provided in FIPS 199 guidance are Low, Moderate, and High. Figure 2 provides an example of a security categorization from FIPs 199. The security categorizations are then applied to each information type.

Example of Security Categorization From FIPS 199 [80]
The generalized format for expressing the security category, SC, of an information type is: **SC** information type = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)}, where the acceptable values for potential impact are LOW, MODERATE, HIGH, or NOT APPLICABLE. EXAMPLE 1: An organization managing *public information* on its web server determines that there is no potential impact from a loss of confidentiality (i.e., confidentiality requirements are not applicable), a moderate potential impact from a loss of integrity, and a moderate potential impact from a loss of availability. The resulting security category, SC, of this information type is expressed as: **SC** public information = {(**confidentiality**, NA), (**integrity**, MODERATE), (**availability**, MODERATE)}.

Figure 2. Example of Security Categorization from FIPS 199.

RMF supports the risk management process defined in SP 800-39, Managing Information Security Risk [81]. SP 800-39 guidance identifies four risk management components. They are: frame risk, assess risk, respond to risk once determined and monitor risk. Table 3 describes the components. The guidance in SP 800-39 calls for risk management to be conducted as an enterprise-wide activity that spans the three organizational tiers: strategic, managerial, and operational.

Inputs and preconditions to risk assessment, including some from the risk framing step, are identified in the guidance as: “acceptable risk assessment methodologies; the breadth and depth of analysis employed during risk assessments; the level of granularity required for describing threats; whether/how to assess external service providers; and whether/how to aggregate risk assessment results from different organizational entities or mission/business functions to the organization as a whole”[80].

Table 3. Components of Risk Management in SP 800-39 [81].

Risk Management Component	Description
Frame risk	Establish the context for risk-based decisions by describing the environment in which risk-based decisions are made; This involves identifying: a. risk assumptions b. risk constraints c. risk tolerance d. priorities and trade-offs
Assess risk	Identify threats and vulnerabilities Determination of risk a. harm (impact) b. likelihood of exploitation Supporting Inputs: a. tools to be used b. assumptions c. constraints d. roles and responsibilities e. risk data collection and communication methods f. how assessments are conducted g. frequency of assessment h. threat data collection method
Respond to risk	Provide consistent enterprise response to risk; types of responses are generally categorized as accepting, avoiding, mitigating, sharing, or transferring risk; The steps in developing a response: a. identify alternative responses b. evaluate potential responses c. select response in line with organizational risk tolerance d. implement response
Monitor risk	Monitoring on an ongoing basis using effective organizational communications and a feedback loop for continuous improvement in risk-related activities. a. Verify risk responses are in place b. Verify the effectiveness of risk responses c. Identify changes in the environment that may affect risk

There are two primary activities in risk assessment: 1. Identify threats and vulnerabilities in the environment along with likelihood and potential impacts of exploitation and 2. Determine risks to stakeholders should the identified threats exploit the identified vulnerabilities. The second step is done in consideration of the likelihood

that such events could take place. Adverse impacts can be expressed as a security objective, such as loss of confidentiality, integrity, or availability. SP 800-39 states that the usefulness of impact information is maximized by expressing it in terms of organizational mission, business function, and stakeholder.

The guidance describes risk as containing uncertainty in relation to the methods and assumptions taken when collecting the inputs of assessment. In addition, it describes risk assessment as being a process that is subjective in nature, subjective both to the experiences of the individuals involved in assessment and to the organizational culture. There is no solution to this problem offered, but the guidance suggests that organizationally defined and applied processes provide a means to identify and resolve inconsistent practices.

The risk assessment result may lead to iterative steps of risk assessment and risk response until selected objectives are achieved. Once completed, the risk assessment results conducted at each of the three tiers of the organization (strategic, managerial, and operational) provide a portfolio of risk assumed by the organization. This could lead to future work at the strategic tier of the organization, such as root cause analysis. These activities could result in future changes to organization design decisions to the extent that they can effectively reduce enterprise risk.

2.4.2.2 Supply Chain Risk Management Practices for Federal Information Systems and Organizations.

RMF contains guidance on Supply Chain Risk Management (SCRM) [72]. SCRM should be important with respect to networked medical devices because they are purchased from suppliers who design and build the functionality, including security

features in the device. Accordingly, healthcare organizations are exposed to risk from the supply chain and should understand these risks in order to make informed purchasing decisions and determine appropriate mitigation actions. Determining that the risk introduced by acquiring products from the supply chain is acceptable depends on the level of assurance that the organization can ascertain from the provider regarding the fitness of the security status of the product. Being able to determine the level of assurance of security fitness is based on the amount of influence the organization has on the supplier and the evidence presented by the provider regarding the effectiveness of security controls.

RMF describes SCRM as a complex process requiring coordination across an organization, where communication and trust relationships among internal and external stakeholders is important. SCRM activities include assessing risk, determining suitable mitigation actions, developing plans and documenting the selected mitigation actions, and monitoring and comparing performance against plans. The guidance includes the importance of tailoring the SCRM plan to the organization's particular needs. By tailoring the plan, organizations can focus their resources on the most mission critical areas specific to their risk environment.

NIST published guidance for federal organizations and agencies toward identifying, assessing, and mitigating supply chain risk in SP 800-161 [82]. This guidance could be applicable to other organizations. The guidance is precipitated by concerns for security risks that may be introduced into federal organizations by Information Communication Technology (ICT) that could contain malicious

functionality, be counterfeit, or could introduce security vulnerabilities due to poor design or manufacturing practices within the supply chain.

In the guidance NIST describes four pillars of ICT-SCRM as integrity, security, resilience, and quality. Figure 3 illustrates the inter-relationship of the four pillars. The NIST guidance addresses only the overlapping areas of the four disciplines.

Figure 3. Four Pillars of ICT-SCRM [82].

The guidance recommends that organizations develop a base level of maturity in the following key areas before implementing ICT-SCRM.

1. Ensuring that organizations understand the cost and scheduling constraints of implementing ICT SCRM
2. Integrating information security requirements into the acquisition process
3. Using applicable baseline security controls as one of the sources for security requirements

4. Ensuring a robust software quality control process
5. Establishing multiple sources for critical system elements

The guidance recommends that organizations develop a formal process for reaching this level of maturity including dedicated resources.

Figure 4 describes risk resulting from the likelihood that threats may exploit vulnerabilities and the potential impact that may occur.

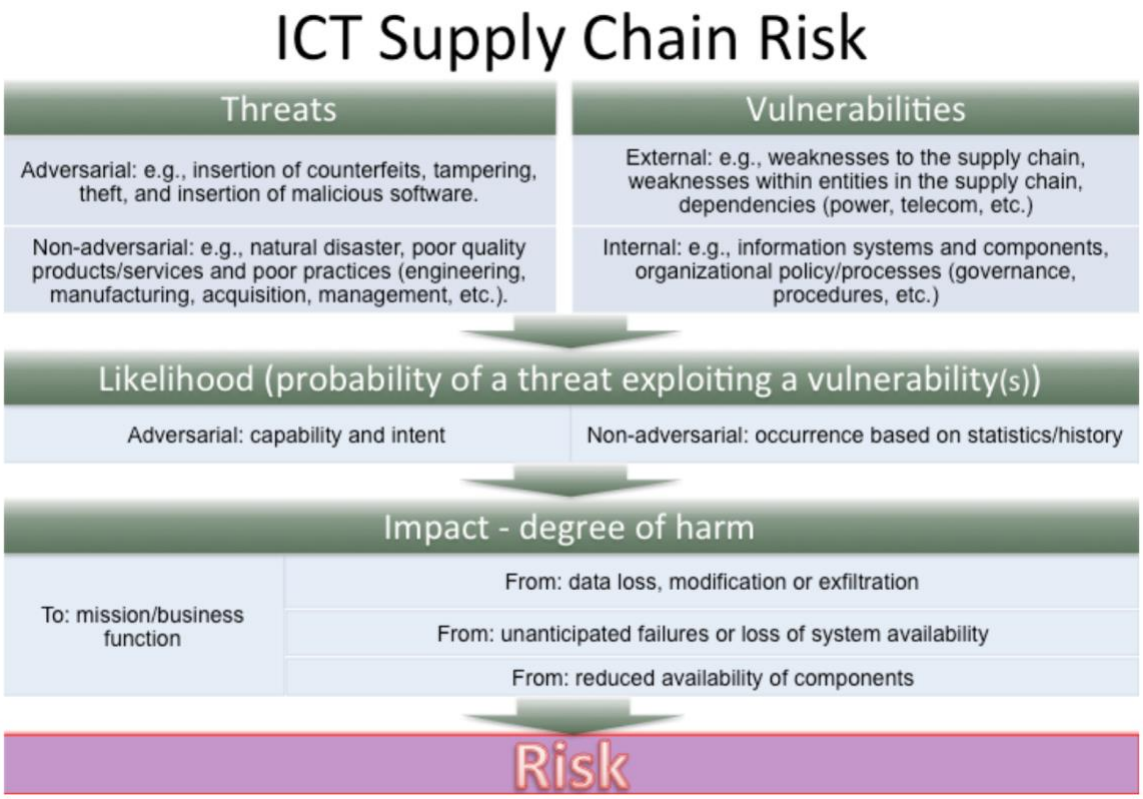


Figure 4. ICT Supply Chain Risk [82].

2.4.2.3 Framework for Improving Critical Infrastructure Cybersecurity.

The Framework for Improving Critical Infrastructure Cybersecurity was

developed by NIST for voluntary use by critical infrastructure owners and operators [59]. Critical infrastructure is defined in the U. S. Patriot Act [83] as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." [83]. The healthcare sector of the U. S. economy is identified as one of the nation's critical infrastructure sectors [84].

The goal of the framework to provide critical infrastructure sectors of the U. S. economy with a tool for improving their resilience to cybersecurity threats and vulnerabilities. The framework is designed to be industry independent and can be useful to organizations designated as critical infrastructure as well as to organizations not designated as critical infrastructure. The framework guides cybersecurity activities based upon business drivers and consideration for the technology required to meet business objectives within the specific risks, priorities, and systems of each organization.

The framework consists of three parts: the framework core, implementation tiers, and the profile. The core is the set of activities, desired outcomes, and references that are common across critical infrastructure sectors. The core is composed of four elements: functions, categories, subcategories, and information references. Figure 5 shows the structure of the framework core. The categories and subcategories are populated with the outcomes and sub-outcomes of the respective function.

The implementation tiers indicate the organizations views and processes in place regarding cybersecurity risk. There are four tiers: partial, risk informed, repeatable, and adaptive. While organizations who are at lower tiers are encouraged to consider moving

to a higher tier, the purpose of identifying a tier is to gain awareness of the current posture. Progression to a higher tier is encouraged when a cost-benefit analysis indicates it to be a feasible and cost-effective means to a reduction in cybersecurity risk.

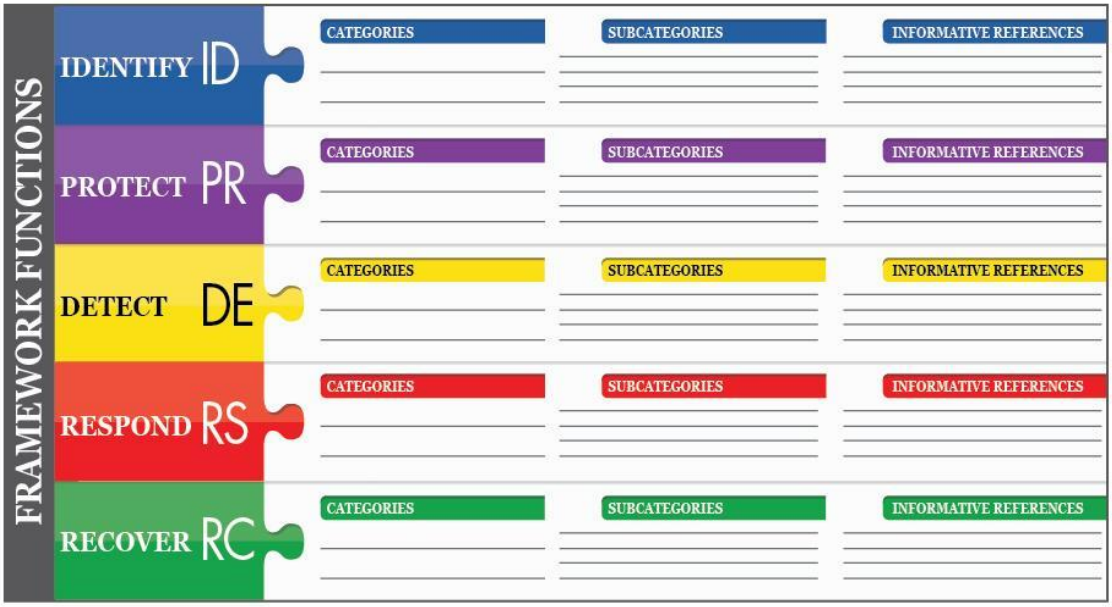


Figure 5. NIST Cybersecurity Framework Core Structure [59].

The profile is the complete core framework that an organization has identified based on its review of the functions in light of the organizational needs and priorities. Profiles can be established for both the as-is and the desired or target state of the organization. A comparison can be made of the as-is and the target profile to identify opportunities for improvement.

The framework, not intended to replace a risk management process, is intended to be a component of a risk management process that identifies cybersecurity risks and how they are managed [59]. Quantifying risk is outside of the scope of the framework.

2.4.2.4 ISO 27000 Information Technology – Security Techniques.

ISO standards for the risk management of information is found in the 27000 series of standards as shown in Figure 6. ISO uses the term Information Security Management System (ISMS) to describe the policies, procedures, guidelines, and associated resources and activities managed by an organization for protecting information assets [60].

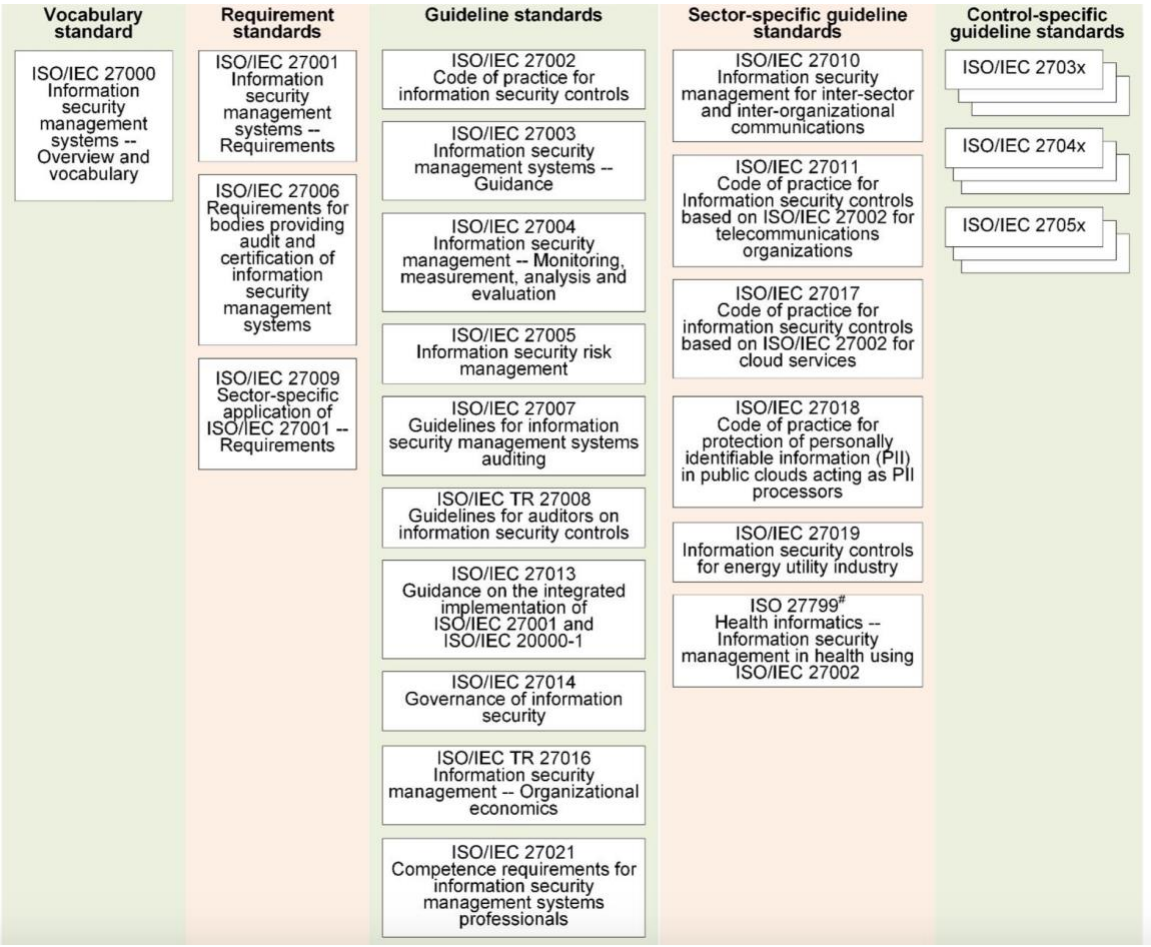


Figure 6. ISO ISMS Family of Standards and Relationships.

Risk assessment falls within the ISO 27001 Risk management standard. ISO identifies necessary components of a risk assessment as a risk analysis and a risk

evaluation, where a risk analysis is a systematic approach of estimating the magnitude of risks, and risk evaluation is a process of comparing estimated risks against the risk criteria to determine the significance of risks [60]. The precursor to risk analysis is the identification of relevant assets and information, and risk evaluation culminates with results that inform the organization's risk management decisions.

The steps involved in the ISO 27001 risk assessment are:

1. Identification
    a. Identify assets within the scope of the risk assessment
    b. Identify threats
        i. Natural or human
        ii. Accidental or deliberate
        iii. Inside or outside of the organization
    c. Identify vulnerabilities
    d. Identify controls that can be put in place
    e. Identify consequences of the exploitation of vulnerabilities
2. Analysis (Qualitative analysis and/or quantitative analysis)
    a. Likelihood
        i. Attacker skills required
        ii. Attacker motivation
        iii. Difficulty of attack
    b. Impact
        i. Effects on confidentiality, integrity, availability
        ii. Cost of asset
3. Evaluation
    a. Quantitative: Risk = Likelihood x Impact
    b. Qualitative – Risk Matrix
4. Results
    a. Risk evaluation
    b. Risks to prioritize

2.4.2.5 HITRUST Common Security Framework.

The HITRUST Common Security Framework (CSF) [66] is developed and supported by the HITRUST Alliance [27] as a tool for addressing security considerations in the adoption of health information systems and exchanges. Specifically, the framework aims to address the following challenges that are prevalent in the healthcare sector: numerous and sometimes inconsistent requirements and standards, compliance issues, concern over current breaches, and the growing risk and liability associated with information security in the healthcare sector. The framework was designed to be used by any organization that creates, accesses, stores, or exchanges protected health information [66].

Beginning in v9.2 of the CSF, the HITRUST Alliance took steps to make the framework more agnostic due to seeing an increase in the adoption of the HITRUST CSF outside of healthcare. This was done by moving HIPAA and healthcare-specific requirements into a separate HIPAA (healthcare) industry specific segment, thereby making it easier for organizations in any industry to adopt the framework [66].

HITRUST CSF is composed of 14 control categories, 49 control objectives, and 156 Control Specifications. The control objectives and specifications are based on ISO/IEC 27001:2005 (requirements) and ISO/IEC27002:2005 (controls) [85]. The following are integrated into each control: the NIST Special Publication 800-series security framework documents [86], ISO/IEC 27799: 2008 (controls and guidelines for managing health information security) [87], HIPAA [88], the Payment Card Industry Data Security Standard (PCI) [89], COBIT [69], and state requirements. The resulting HITRUST CSF, according to the alliance, is an industry overlay [90] of NIST SP 800-53

[78] (Security and Privacy Controls for Information Systems and Organizations) moderate-impact minimum security control baseline for the healthcare industry. The alliance further states that the HITRUST CSF supports the NIST Framework for Improving Critical Infrastructure Cybersecurity [59] requirements for an industry-specific cybersecurity program.

The 14 control categories each have a number of associated objectives and specifications. Table 4 shows the categories and the number of control objectives and control specifications associated with each.

Table 4. HITRUST CSF Control Categories.

Control Category Number	Control Category Description	Number of Control Objectives	Number of Control Specifications
0	Information Security Management Program	1	1
1	Access Control	7	25
2	Human Resources Security	4	9
3	Risk Management	1	4
4	Security Policy	1	2
5	Organization of Information Security	2	11
6	Compliance	3	10
7	Asset Management	2	5
8	Physical and Environmental Security	2	13
9	Communications and Operations Management	10	32
10	Information Systems Acquisition, Development and Maintenance	6	13
11	Information Security Incident Management	2	5
12	Business Continuity Management	1	5
13	Privacy Practices	7	21

Each control category is composed of a reference number and title and a statement of the control objective. Although the control categories are numbered, HITRUST does not imply the importance of the categories by the numbering order.

Each HITRUST control contains a control specification, a risk factor, the implementation requirement, control assessment guidance, and a cross-reference between each implementation requirement level and the requirements and controls of other common standards and regulations, referred to as standard mapping.

2.4.2.6 CIS Critical Security Controls.

CIS Critical Security controls [67] are a set of actions for cybersecurity defense created by The Center for Internet Security (CIS) [28], a non-profit organization that facilitates a consortium of volunteer public and private sector collaborators. The controls are designed to prevent or detect the most common causes of cybersecurity events. They are based upon current threat data and information vetted by the consortium of cybersecurity professionals. All controls are justified by actual attack data and are updated as new attacks are identified. The controls encompass prevention, detection, and disruption of security compromises. This research is based on version V7.1 of the CIS Controls [67].

CIS controls are designed to provide defense-in-depth through a set of actions intended to mitigate the most common cybersecurity attacks. They reflect five tenets of an effective cyber defense system as defined by CIS. The tenets are identified in Table 5.

There are 20 controls that are divided into three categories: Basic, Foundational, and Organizational. The categories are designed to help an organization get started by implementing the Basic controls first, and then progressing to the Foundational and Organizational controls. Table 6 shows the categorized CIS Controls.

Table 5. CIS Controls 5 Critical Tenets of an Effective Cyber Defense.

	Tenet	**Description**
1	Offense informs defense	Controls are exclusively those that have been shown to stop real-world attacks.
2	Prioritization	Prioritize controls within an individual environment based on their ability to provide the greatest risk reduction, protect against the most dangerous threat actors, and their feasibility within the computing environment.
3	Measurements and metrics	Establish metrics to provide a shared language for executives, IT specialists, auditors, and security officials to facilitate swift identification and implementation of adjustments.
4	Continuous diagnostics and mitigation	Continuous measurement, testing, and validation of the effectiveness of security measures to drive prioritization of next steps.
5	Automation of defenses	Automation of defenses enable organizations to achieve reliable, scalable, and continues measurement.

Version 7.1 of the Controls introduced a concept referred to as Implementation Groups (IGs) to describe different levels of organizations that may be implementing the Controls. There are three IGs, with IG 1 being a very small company with a low level of sensitive data to protect and usually a low level of cybersecurity expertise, IG 2 is a medium-sized organization, and IG 3 is a large corporation with highly sensitive data to protect.

Each of the 20 controls has several sub-controls to define implementation details. Each of the sub-controls identifies which of IGs should be expected to perform the sub-control. The goal of the sub-controls identified for each IG is to make the controls reasonable for organizations of all sizes.

Table 6. CIS Controls.

Basic	**Foundational**	**Organizational**
1. Inventory and control of hardware assets	**7.** Email and web browser protections	**17.** Implement a security awareness and training program
2. Inventory and control of software assets	**8.** Malware defenses	**18.** Application software security
3. Continuous vulnerability management	**9.** Limitation and control of network ports, protocols and services	**19.** Incident response and management
4. Controlled use of administrative privileges	**10.** Data recovery capabilities	**20.** Penetration tests and red team exercises
5. Secure configuration for hardware and software on mobile devices, laptops, workstations and servers	**11.** Secure configuration for network devices, such as firewalls, routers and switches	
6. Maintenance, monitoring and analysis of audit logs	**12.** Boundary defense	
	13. Data protection	
	14. Controlled access based on the need to know	
	15. Wireless access control	
	16. Account monitoring and control	

2.4.2.7 CIS Risk Assessment Methodology (CIS RAM).

CIS RAM [68] was co-developed by CIS [28] and cybersecurity consulting firm HALOCK [91]. The purpose of CIS RAM is to assist organizations in planning and justifying the implementation of the CIS Controls [67] and to apply them in a manner that addresses the unique needs of the organization. It conforms to and supplements established risk assessment methods such as ISO 27005 Information Security Risk Management [92] and NIST Special Publication 800-30 Risk Management Guide [93]. CIS RAM supplements these standards by helping organizations evaluate risks and

safeguards using the concept of “due care” and “reasonable safeguards” that regulators and the legal community use to evaluate whether organizations act as a “reasonable person”. By “due care”, CIS refers to Duty of Care Risk Analysis (DoCra) [94], a public standard for risk analysis that includes a legally defensible cost-benefit analysis for the purpose of balancing security safeguard benefits and their cost.

CIS RAM provides three sets of instructions for implementation based upon the organization’s level of cybersecurity maturity and in line with the NIST Cybersecurity Framework’s [59] three-tiered approach to implementation. The activities applied in all three CIS RAM levels are described in Table 7.

CIS RAM recommends an ordinal scale for assessing both the impact and the likelihood of each risk. For example, a scale of one to three, with each level having a clear text description. Once each risk is assigned an impact and a likelihood ordinal scale value, the two numbers are multiplied together to develop a risk score. In determining acceptable risk, the organization determines the highest risk score is deemed acceptable, and safeguards are identified to reduce each risk that has a score above the acceptable risk level.

Table 7. CIS RAM General Risk Assessment Activities.

Analyze the observed risk	define the scope; identify assets; develop risk assessment and acceptance criteria; gather evidence; model risks; evaluate risk based on impact and likelihood; compare assessment to acceptance to criteria
Propose safeguards	Recommend safeguards for unacceptable risks from CIS Controls; evaluate safeguards through cost-benefit analysis

Each of the three tiers of implementation in CIS RAM approach risk assessment from a different basis, which is intended to support the organization's level of cybersecurity maturity. Tier 1 is a control-based risk assessment where the organization looks at generic systems, devices and applications. Tier 2 is an asset-based risk assessment where the organization looks at specific systems, devices and applications and their sub-components. Tier 3 is a threat-based risk assessment where the organization looks at specific systems, devices and applications within the context of specific threats.

2.4.2.8 Control Objectives for Information and Related Technologies (COBIT).

COBIT [69], created by ISACA, is a framework for the governance and management of IT. This section gives a brief overview of COBIT 5 as it relates to risk and provides a review of ISACA's IT security risk assessment guidance, which is ancillary to COBIT.

The COBIT framework addresses IT management and governance from an enterprise-wide perspective beginning with a goals cascade based on the premise that all organizations exist for the purpose of creating value, that is realizing benefits at an optimal cost while optimizing risk. The term cascade refers to how the goals of an organization cascade from stakeholder drivers to stakeholder needs to enterprise goals, to IT-related goals, and finally to enabler goals. Figure 7 illustrates the COBIT 5 goals cascade. Of note, risk is a consideration near the top of the cascade, within the stakeholder needs. The guidelines emphasize the importance of customizing the cascade to meet the organization's goals and using the cascade as a flexible guideline because organizational goals change and fluctuate over time.

Stakeholder needs translate into enterprise goals. The framework consists of a set of generic stakeholder needs and enterprise goals that were developed using the Balanced Scorecard [95] method and a list of common goals. An organization may use these sets and customize them for itself.

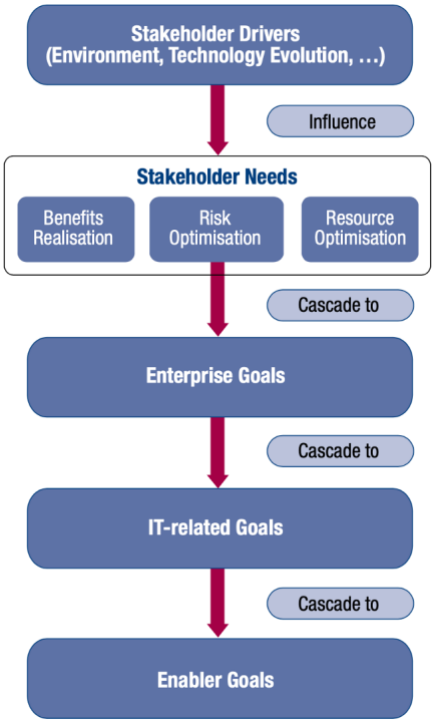


Figure 7. COBIT 5 - Goals Cascade Overview.

Enterprise goals require a set of IT-related outcomes which cascade into IT-related goals. The IT-related goals cascade into enabler goals which are required to achieve the IT-related goals. The framework contains seven categories of enablers. They are: principles, policies and frameworks; processes; organizational structures; culture, ethics and behavior; information; services, infrastructure and applications; people, skills and competencies.

ISACA's risk assessment guidance [96] documents how to conduct an IT risk assessment. The guidance defines risk as "the combination of the probability of an event and its impact" [96]. ISACA recommends that organizations create a risk assessment strategy that complements and champions enterprise goals with the purpose of reducing and mitigating risks. They recommend that risk assessment follow the generic risk assessment methodology steps of: identify and value assets, identify known threats, identify vulnerabilities, identify risk and determin**e** the risk treatment.

ISACA identifies the starting point of the risk assessment process as the identification of the enterprise's risk appetite. They recommend this be described quantitatively in monetary terms to increase clarity and avoid confusion. In addition to a quantitative identification of risk appetite, a secondary baseline for communicating risk magnitude is reputational damage, although it is difficult to quantify.

In asset valuation, ISACA includes systems, applications, data, storage and communication mechanisms as assets to be valued. Considering three general valuation methods: qualitative, quantitative and semi-quantitative, ISACA recommends a quantitative valuation as a measure that provides for clear and consistent interpretation across the enterprise. They strongly discourage a semi-quantitative approach as potentially profoundly misleading, for example, one that assigns monetary values to ordinal scale values such as 'high', 'medium', or 'low'.

ISACA also recommends identifying the processes in the enterprise's value chain and which assets are involved with each process. This enables an understanding of the impact of a compromised asset on the organization's overall operations. Accordingly,

ISACA recommends that risk assessment include a mapping of the relationships between assets and processes.

ISACA recommends identifying risk factors next, beginning with areas of risk. They identify two broad approaches to risk identification as threat assessment and vulnerability assessment. Risk identification can be done using a top-down or bottom-up approach. A top-down begins with a potential threat and considers each asset and how it may be affected. A bottom-up approach begins with an asset and considers the negative outcomes that could occur with that asset.

ISACA describes the intent of threat sources as a key factor in threat identification and categorizes intent as arising from malicious intent, accidental actions, or natural occurrences such as weather. Understanding intent could lead to discovering additional vulnerabilities, and organizations can apply threat knowledge to risk treatment decisions.

ISACA describes vulnerability assessment as a structured approach that can be conducted using manual and automated processes. Vulnerabilities are primarily limited to weaknesses that are already known. These include weaknesses identified in audit reports, identified by the enterprise's incident response teams or software security analysts, detected by applying third-party vulnerability intelligence, or published in the NVD [33]. ISACA cautions that vulnerability assessment reporting can be misleading when statistical analysis is viewed in summary and when readers fail to recognize that vulnerability assessment only includes known vulnerabilities.

A clear understanding of the controls that are in place to modify the state of vulnerability is a component of vulnerability identification. ISACA points out that most

controls do not eliminate threats, rather they reduce threats, and an important part of vulnerability assessment is understanding the extent to which a control limits a vulnerability. Controls may be technical, such as hardware or software, or non-technical, such as policies, administrative actions, and physical mechanisms.

Calculating risk, which is the probability that a vulnerability will be exploited, is the next step. ISACA recommends quantifying risk in monetary terms where possible but recognizes that difficulty in finding solid data on which to base a quantification may limit the options for quantifying risk. Another difficulty is that unknown vulnerabilities represent a gap in the basis for calculating risk.

Once risk has been calculated, the areas of risk should be logged in a risk register. The risk register can serve as a historical record and as a knowledge base for matters of risk. The register can inform managerial decisions, provide visibility into risk governance and provide retrospective insight into threat patterns. ISACA identifies risk treatment as the conclusion of risk assessment, with four possible risk treatment categories: accept, transfer, mitigate and avoid. These are standard categories used by NIST and other organizations to identify risk treatments options [72], [59], [81].

Lastly, ISACA identifies limitations in risk assessment. Primarily, qualitative analysis is subjective and can lead to different interpretations of risk across the enterprise. Assigning monetary values to qualitative ordinal scales can increase the confusion. Quantitative data from objective sources lacks bias and is therefore the ideal solution, however this often is not possible in risk assessment. They describe expert opinion using a qualitative approach as potentially offering more clarity and flexibility in interpretation than quantitative numbers that imply objective sources of data when there is none.

2.4.2.9 Factor Analysis of Information Risk (FAIR).

FAIR [97] is an open standard cyber risk framework that was developed by the FAIR Institute, a consortium of professionals with a broad range of industry backgrounds. The framework was intended to provide a means for identifying risks and presenting them to business leaders in terms that clearly explained the magnitude of risk and the value of mitigations. Quantifying risk was the solution they arrived at in developing the framework. In addition to quantification, they also use expert judgment in the prediction of several factors. The first is assessing the capability of potential adversaries, groups they refer to as threat actors. Next is the frequency with which they would expect a threat actor to attempt to exploit a vulnerability. Lastly, they use expert judgment to estimate the magnitude of the loss that could occur if the threat actor were to be successful in an exploitation attempt.

The FAIR framework relies on Beta PERT distribution and Monte Carlo simulation to produce risk results. Figure 8 shows the FAIR ontology.

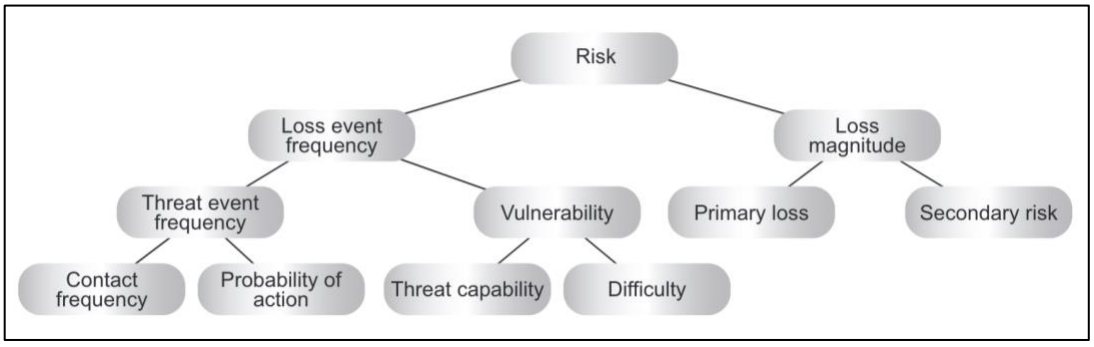


Figure 8. FAIR Ontology.

2.4.3 Risk Assessment

This research defines risk assessment as a component of overall risk management where potential threats are identified and prioritized into risks, and controls are identified that can reduce risk to acceptable levels [98]. This research defines risk management as the overall process of understanding, mitigating and controlling risk through risk assessment, risk mitigation, operational security, and testing [99]. Risk analysis is a component of risk assessment where gathered data is reviewed and analyzed [99].

Risk assessment is a periodic and objective analysis of the current security controls that protect an organization's assets [99]. There are four key deliverables in risk assessment: Identify threats to the organization's mission, prioritize those threats by risk level, identify mitigating controls or safeguards, and publish an action plan [98]. The goal of risk assessment is to reduce risk to a manageable level. Figure 9 illustrates the relationship between risk management, risk assessment, and risk analysis. This research is focused on the cybersecurity risks imposed by networked medical devices.

Figure 9. Risk Management, Assessment, Analysis Relationship.

In a seminal paper on risk [100], Kaplan identifies risk analysis as consisting of an answer to three questions: *What can happen?; How likely is it that that will happen?; and If it does happen, what are the consequences?* This research seeks to provide a framework to facilitate answering these questions as part of a risk assessment framework.

2.4.4 Quantifying Risk

Methodologies and strategies for quantifying risk have been applied in many disciplines including energy [101], [102], finance [103], insurance [104], and project management [105]. A survey of risk quantification across disciplines is done to assess how risk is quantified in a variety of domains.

Early work in quantifying risk was done by Starr [106] in the area of comparing societal benefits of technologies to the risks associated with those technologies. The goal of the research was to answer the questions "how safe is safe enough?" The calculations were basic comparisons of perceived benefits to estimated fatalities and provide insight into the general public's risk appetite.

Cox [107] explores the use of risk matrices as sources of risk information. He relies on mathematical and logical fundamentals to illustrate the limitations of using risk matrices. He demonstrates how matrices and provide risk ratings that are inconsistent with underlying quantitative risks, and how matrices do not necessarily support effective resource allocation toward mitigations. Cox concludes that while risk matrices are widely used and convenient, they often do not support good decision making, and they should be used with caution.

Kaplan introduced quantitative methods to risk analysis. His work includes probabilistic risk analysis in nuclear energy, both of the risk of accidents in nuclear

energy plants and the risk of transporting spent nuclear fuel by trains [100]. Kaplan demonstrated the use of probability as a means of systematically quantifying risk related to rare events.

Kaplan distinguishes between probability and statistical methods [100]. He describes statistics as the study of frequency, where it is a science of handling data. Conversely, probability he describes as the science of handling a lack of data. Kaplan asserts that in the absence of data, probability is the only means of prediction. He uses Bayes' Theorem to determine a probability curve that includes consideration for risk scenarios that are known as well as those that are unknown. He demonstrates the value of considering risk as a curve rather than a single number. Kaplan discusses acceptable risk and the difficulty with this topic. He asserts that risk cannot be considered in isolation, rather risk must be considered from a decision theory point of view considering cost, benefits, and risk. In considering acceptable risk, the optimum mix of cost, benefit, and risk should be considered.

Meyer [105] developed a process for quantifying risk in project management and applied it to a real capital expenditure project in the mining industry. The process consists of quantifying risk for the three risk elements that affect project management. These are schedule, cost, and performance. Quantified risk assessment in each of these areas provides information for developing effective mitigation strategies and appropriate contingencies with the goal of minimizing the impact of risks on the project. In the project management discipline contingency is considered in relation to the effect risk has on the schedule estimate and the cost estimate of the project. Quantifying the effect of

risk on a project allows for estimates to include lower and upper limits of time and cost, thereby better informing management.

The Project Management Institute process for risk management includes the development of a risk register that begins with a qualitative risk assessment that evaluates each risk in terms of the probability of the risk occurrence and the impact that the risk would create on the project. The risk register is an important input into Meyer's process for quantifying risk. The resulting risk assessment considered three types of risk: project risk, which comes primarily from the risk register; estimation accuracy risk which reflects uncertainty in the accuracy of the estimate; and systemic risks, which are risks relative to the overall environment.

2.4.4.1 Measurement.

Quantifying cybersecurity risk involves measurement. Hubbard defines measurement in the context of cybersecurity risk assessment as "a quantitatively expressed reduction of uncertainty based on one or more observations" [108]. This definition has a mathematical foundation rooted in the field of "information theory", the study of the quantification, storage, and communication of information, developed by Claude Shannon in the 1940s [109]. Shannon uses the term entropy to describe uncertainty.

2.4.4.1.1 Bayes' Theorem is a mathematical formula for calculating probabilities that was developed by the mathematician and theologian Thomas Bayes and published posthumously in 1764 [110]. Bayes theorem was conceived out of desire to calculate the probability of an event occurring under certain circumstances when very little data is available to support a calculation of the probability. Bayes developed a rule, or formula,

to calculate the chance that an event would occur between an upper and lower conditional probability. The rule is based on some knowledge or condition that may be known about the event. The mathematical formula known as Bayes Theorem is shown in Figure 10.

$$P(A \mid B) = \frac{P(B \mid A)\, P(A)}{P(B)}$$

Figure 10. Bayes' Theorem.

P(A|B) is referred to as the posterior and represents what is already known about the probability of A given B. It is interpreted as the likelihood of an event A occurring, given that B is true. Conversely, P(B|A) is the likelihood of event B occurring, giving that A is true. P(A) is the prior information we have, the probability of A, and P(B) is the probability of B. The Bayesian result can be interpreted as the degree to which a belief (A) should change as a result of related evidence (B).

There are three defining attributes of the Bayesian approach as identified by Shafer [111]. First, the approach relies on a complete probabilistic model of the domain. That is, the domain of probabilities must total one. Second, subjective judgements are substitutes for empirical data, and third, the theorem is the primary mechanism for updating beliefs in light of new information.

2.4.4.1.2 The Dempster-Shafer Theory of Evidence originated with the work of Dempster [112] in the 1960's on the theory of probabilities with upper and lower bounds and was extended by his student Shafer [111] in 1974. It has since been used in artificial intelligence and expert systems as a method for modelling reasoning under uncertainty.

The theory has grown into a rich research area of belief functions [113]–[115]. A review of scholarly articles using the search term 'Dempster-Shafer' reveals that research in this area has seen a steady increase through the year 2010, and it has remained quite active since then.

Two primary features of the Dempster-Shafer theory of evidence are that it is not necessary to have beliefs that total unity, and that measures may be assigned overlapping sets and subsets of hypotheses. In this regard the theory offers an improvement over Bayes' Theorem that may be beneficial when analysis is presented with only weak information sources. In addition, it provides flexibility to vary the allocation of belief to suit the extent of knowledge.

2.4.4.1.3 Analytic Hierarchy Process (AHP) [116], introduced by Thomas L. Saaty in the early 1980's, is a multi-criteria decision-making approach for determining weights of risk factors in pairwise comparisons. AHP is concerned with the scaling problem, what numbers to use, and how to correctly combine numbers resulting from them. A scale of measurement in the context of AHP consists of a set of objects, a set of numbers and a mapping of objects to numbers. A contribution of AHP is how to derive relative scales from expert judgement or data from a standard scale, and how to perform calculations on the scales avoiding useless or misleading results. This is maintained by composing weighting with respect to all criteria before normalization to a standard scale.

2.4.4.2 Beta Distribution.

Beta distribution is used in probability theory and statistics as a continuous distribution of probabilities on a scale of zero to one. Beta distribution is used with Bayes' Theorem to update the probability of a hypothesis to model random behavior.

This is useful when estimating a population proportion, for example, the likelihood of a risk that has very little historical data on its exploitation [108].

2.4.4.3 Monte Carlo Simulation.

Monte Carlo simulation is a technique for simulating scenarios by randomly selecting values for uncertain variables from a pre-defined range of probabilities and using the values in a model [117]. Monte Carlo simulation can be operationalized in computer simulation as a technique for generating a large number of random scenarios based upon probabilities for inputs [118]. It was instrumental in the simulations required in the Manhattan Project and at Los Alamos in the 1950s in the development of the hydrogen bomb [117]. It can be useful in modeling where there is a great deal of uncertainty. Monte Carlo simulation can be used to generate thousands, or even millions, of possible outcomes. Today Monte Carlo simulation is used widely in many fields including engineering, physics, research and development, business, and finance [117]. This technique could be useful in risk analysis to visualize risk [108].

2.4.5 Risk Perception

The perception of risk may have a significant role in risk assessment. Perception is involved in the inputs to risk assessment as well as in the decisions made by leaders with respect to risk. This research is likely to result in the need to consult with cybersecurity experts for inputs related to probability and impact of the exploitation of cybersecurity vulnerabilities. This warrants and review of research in the area of the accuracy of expert forecasts. In addition, a review of research into risk perception may be useful in guiding the presentation of risk assessment results to organization leaders.

2.5 Prediction

Prediction of future outcomes has been studied in the social sciences [119]-[120], in statistics, and in economics [121], [122]. Predictions are made in two general classes: prediction based on intuition or experience also referred to as clinical judgment, and prediction based upon statistical models, also referred to as actuarial judgment [123]. In clinical judgment, the process for arriving at the prediction is a mental process that does not follow specific rules, and it is often difficult for the judge to describe the process [119]. In statistical prediction a mathematical model is created to calculate the prediction. Three pieces of information are necessary in statistical prediction: prior or background information, evidence specific to the individual case being predicted, and the expected accuracy of the prediction [124].

Ashenfelter [121] showed that a statistical model could be used to outperform expert opinion in predicting the future the value of Bordeaux wines. Predicting the future price of wines, an important factor for wine investors, is traditionally done by world-renowned wine experts. Ashenfelter demonstrated that using a simple statistical model to predict the future price of wines outperformed wine experts. His model, based upon three characteristics of the weather during the growing season, resulted in predictions of the price of mature wines that were superior to the prediction of wine experts. The correlation between his predictions and actual prices is above ninety percent, where wine experts were inconsistent substantially less accurate.

2.5.1 Clinical judgement vs. Actuarial Judgement

Meehl [119] introduced clinical and actuarial judgement to a wide range of social scientists in 1954. His work stimulated interest and studies in the area. Clinical judgement refers to a procedure where the judge makes predictions using informal and subjective methods. Actuarial judgement refers to the use of the statistical inference in making predictions. In actuarial judgement conclusions are drawn using statistical methods, the human judge is not used, and judgements are based upon empirically established relationships and evidence.

Meehl [119] specified conditions for a fair comparison of the two methods. First, both judgements must be based on the same data, although the strategy for each may be formulated using different methods. Second, conditions that can inflate the accuracy of actuarial methods must be avoided. For example, the accuracy of an actuarial result could be based on chance. To avoid this, the method should be cross-validated by applying it to a separate case. Cross-validation reduces the chance of artificial inflation in accuracy of actuarial results.

Kahneman and Tversky [124] explored intuitive prediction. Among their findings is that regression to the mean is counter-intuitive and difficult for subjects to apply in the process of prediction. This is even the case with study participants who were well-exposed to statistical regression. They conclude that when making judgments under uncertainty people do not appear to follow the rules of chance or the statistical theory of regression in evaluating current evidence to make judgments about the future. Instead, people make predictions based on representativeness, that is they choose outcomes that more closely represent the inputs, or current evidence. While this method of prediction

may be accurate in many cases, it ignores information such as probability of the prior outcome and the reliability of the evidence. For example, when predicting the major of a graduate student, one group of subjects is given a list of majors and asked to estimate the percentage of students in each major, or the base rate. Another group is given a short personality sketch of a student and asked to determine how similar the student is to a student representative of each of the same list of majors. A third group was given the same short personality sketch and asked to predict the major of the student from the list of majors. Their findings were that there was a high correlation of .97 between representativeness and likelihood, and a low correlation -.65 between likelihood and base rates. Subjects exceedingly ignored the base rates and predicted the major based upon the personality sketch, predicting the students major based on how representative the personality sketch was of the stereotype of a student in a particular major.

Kahneman and Tversky [124] examined the psychology of intuitive prediction, specifically sources of unjustified confidence in prediction and fallacious intuitions concerning regression effects. They found that regression is counterintuitive and difficult to apply. It is intuitive to predict that outcomes should be representative of inputs, and this intuition remained strong despite considerable exposure to statistics. They conclude that in making judgments under uncertainty people do not appear to follow the rules of regression or statistical theory of prediction. Rather, people predict by representativeness by the degree to which outcomes represent the essential features of the inputs, or prior information. They note that in some cases this is valid, but in some cases it is not. In cases where representativeness is not a reflection of the outcome, factors such as of the

likelihood of the prior information and the probability of accuracy are generally ignored by the intuitor.

Dawes et al. [123] compare clinical judgment and actuarial judgement. Qualitative observations can be coded quantitatively, and therefore can be inputs to actuarial judgements. They also observed that the combination of clinical and actuarial judgement can be a third judgement strategy. However, they find a fallacy in this approach when the resulting judgements are dichotomous, for example, if the possible results of the judgement are either 'True' or 'False'. In this case, if the clinical and actuarial judgements agree with each other, then the combination is unnecessary. However, if the clinical and actuarial judgements disagree with each other, they cannot both be valid.

Dawes et al. [123] describe the results of three tests of clinical vs. actuarial judgement. All three tests were conducted in the social science domain, all met Meehl's [119] criteria for a fair comparison, and all three represent judgements that are not artificial and represent common practice for which special expertise is claimed. In all cases, the actuarial models produced more accurate results than the expert clinical judgements. This was even the case when the experts were given the results of the actuarial model for the case before they made their judgement.

Dawes et al. summarize the results of over 100 studies that were all in the domain of diagnosing and predicting human behavior. The actuarial judgement was equal to or more accurate than the clinical judgement in almost every case. Dawes et al. conclude that after the results of 100 tests, while there are no conclusions that can be made about the validity of any one of the actuarial models, it can be generally concluded that the

advantage of the actuarial method of judgement is general and can likely be applied across many unstudied domains.

Kahneman and Klein [125] explore differences in expert judgments, particularly identifying the activities in which skilled judgements develop with experience, and the activities in which experience is likely to lead to overconfident judgments rather than genuine skill. The goal of the research was to identify the areas in which expert judgment is worthy of trust. Klein was a practitioner and scholar in the area of naturalistic decision making and Kahneman was a practitioner and scholar in the area of heuristics and biases. These two areas are described here.

Naturalistic Decision Making (NDM) focuses on understanding intuition by examining the successes of expert intuition, and traces its roots to de Groot's study of master chess players [126]. Early work in NDM was a study to determine the decision making process of commanders of firefighting companies [127]. In this domain commanders are required to make decisions amid conditions of uncertainty and time pressure. The study revealed that commanders often considered a single decision without evaluating alternatives. The decision was based on recognizing patterns from a range of real world and virtual experiences to identify a plausible option. Commanders then assessed that option, and if it seemed appropriate, they would implement it. If it needed modifications to be appropriate for the situation, that was done. If it could not be easily modified, the next most plausible option was considered. Klein et al. [127] termed this approach as recognition-primed decision strategy. The approach was successful because it used the commanders tacit knowledge advantageously [127]. The recognition-primed decision is consistent with de Groot's [126] work and has been replicated in other

domains including systems design, military command and control, offshore oil installation management, and neonatal nursing [125], [127], [128].

NDM has also resulted in failures in decision-making. A catastrophic event in 1988 where a U.S. Navy cruiser shot down an Iranian commercial airliner [129] has been the subject of extensive investigation by NDM researchers. An outcome of this research was the initiation of a research and development program by the U.S. Navy called Tactical Decision Making Under Stress (TADMUS) [130].

Contrasting NDM is Heuristics and Biases (HB), an approach skeptical toward expertise and intuitive judgments. This work is founded in the work of Paul Meehl [119]. Meehl's work involved the review of approximately 20 studies, predominantly from clinical psychology settings, that compared the accuracy of expert judgments to statistical models. The statistical models were more accurate than the expert judgments in nearly every case. Kahneman described similar results from his experience in assessing candidates for acceptance into military officer training [124]. Kahneman coined the term *illusion of validity* to describe the unwarranted sense of validity that comes with intuitive judgment [125].

In the first study of HB, Tversky and Kahneman [131] examined the performance of researchers in choosing the number of cases needed for a psychological experiment. The participants comprised researchers competent in statistics, including two authors of statistics textbooks. The subjects answered questions about sample sizes that were appropriate for different research study scenarios. The result of the study was that researchers failed to follow statistical rules to which they were familiar and drew

incorrect conclusions when they followed their intuitions. Tversky and Kahneman conclude that faulty statistical intuitions survive both experience and formal training.

Kahneman and Klein [125] ultimately conclude that the process of skill acquisition that leads to reliable expert judgements requires both an environment that provides high-validity and an environment that provides an adequate opportunity to learn skills. By high-validity they mean environments that provide a stable relationship between observable cues and subsequent events or between observable cues and outcomes. The absence of high-validity environments leads to unpredictable outcomes. Further, they conclude that while reliable expert judgement cannot develop in unpredictable environments, individuals will sometimes make successful predictions, but only be chance. They also conclude that environments with weak regularity and low-validity can sometimes support the development of algorithms that produce results that are better than chance and better than human judgment. However, the algorithms achieve limited accuracy.

Cybersecurity events have weak regularity, and cybersecurity experts usually do not receive feedback to validate judgements. Therefore, cybersecurity experts are operating in an environment that does not support the development of sound expert judgements as described by Kahneman and Klein [125]. Accordingly, cybersecurity experts are not in an environment that supports the development of expertise in order to accurately predict the likelihood of adverse events. Bayes' theorem, conceived out of a desire to determine the probability of an event occurring under circumstances when very little data is available to support a calculation of the probability, offers a potential

solution. Bayes' theorem allows us to predict probability based upon prior knowledge even when that knowledge is limited.

Bayes' theorem offers a solution to the problem of limited data available to assess cybersecurity risk. However, predicting cybersecurity risk requires input from cybersecurity experts. Based on research into prediction, low accuracy in prediction would be expected from these experts. A related area of research is in the area of calibrating, or training, experts to be more accurate in their judgments.

2.5.2 Calibration

Calibration is a term that describes the process of training a person to more accurately assign probability assessments [132]. Research has shown that humans are not naturally very good at assessing probability [133], [132]. However, experiments have shown that they can be trained to be better at it. Training, or calibration, is well-documented and has been studied with experts in many different areas such as sports picks, psychological diagnosis, investments, trivia estimates, and lie detection [133]. In the studies, large numbers of estimates are collected from individual experts and then compared to observed outcomes. The findings are conclusive and repeated [132]. Without training almost all expert's predictions deviated significantly from observed outcomes. Applying training methods greatly improved the experts estimates of subjective probability.

The findings suggest that people are overconfident of their judgements of general knowledge that is of moderate or extreme difficulty. Furthermore, overconfidence increases with difficulty and decreases as difficulty decreases. Sieber [134] suggests common reasons that difficult predictions lead to more over confidence is that subjects

reduce the complexity of the decision making process by employing any of the following: ignoring conflicting information, failing to generate plausible alternatives, and failing to reflect on what is known or to seek additional information.

In one study [132] subjects were given thirty general two-alternative questions to answer along with their probability assessment. Then they were given an additional ten questions. The instructions for the additional ten questions included first writing down all the reasons that supported or contrasted both of the responses. Then they were to answer the questions with their probability assessment. The method of answering the additional ten questions significantly improved their accuracy. An additional study of this method concluded that an effective remedy to overconfidence is to search for reasons that one might be wrong [135].

One research study speculated that calibration for the prediction of future events may be different than calibration of general knowledge questions [136]. If so, this would limit the application of research with general-knowledge questions to the prediction of future events. However, the study contained general knowledge questions that were more difficult than the future event prediction questions, which could explain the disparity they found. Additional studies demonstrated that calibration for future and past events were identical [132].

Lichtenstein et al. [132] compare a study of physicians' assessments of the probability of a given diagnosis based upon an examination to a study of the predictions of precipitation by weather forecasters. They found the weather forecasters to be significantly more accurate and described them as superbly calibrated. They identified several factors that they believe favor weather forecasters. First, they have been making

probabilistic forecasts for years; second, the task is repetitive; third, the hypothesis is always the same (will it rain?); fourth, the outcome feedback is well-defined and promptly received. This contrasts with physicians who consider a wide array of hypotheses daily, the feedback is not always prompt and sometimes never received.

Lichtenstein et al. [132] presented a comprehensive review of research literature on calibration. The conclusions they demonstrated to support the importance of calibration are the following:

1. making uncalibrated decisions when the payoffs are very large, errors are very large, or when errors compound, the expected loss from erroneous predictions of probability could be very large;
2. assessors should not be expected to be well-calibrated when explicit or implicit rewards for their assessment do not motivate honesty. For example, subtle pressure to not appear foolish or to impress management may result in poor calibration;
3. Receiving feedback regarding the outcomes after every calibration assessment is important to successful training.

No published studies on calibrating cybersecurity expertise have been found. However, the variety of experts that have been trained suggests that calibration may be well-suited for cybersecurity experts.

2.6 Enterprise Risk Management

Enterprise Risk Management (ERM) has its beginnings in the early 2000's with the separate work of The Casualty Actuarial Society [137] and The Committee of

Sponsoring Organizations of the Treadway Commission (COSO) [138] who published ERM frameworks [104], [139] in 2003 and 2004 respectively. The Casualty Actuarial Society defines ERM as: "…*the discipline by which an organization in any industry assesses, controls, exploits, finances, and monitors risks from all sources for the purpose of increasing the organization's short- and long-term value to its stakeholders*" [104]. COSO defines ERM as: "…*a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives*" [140]. Each of the organizations and their framework is described here.

The Casualty Actuarial Society (CAS) [137], founded in 1914, is a credentialing and professional education organization focused on property and casualty risks. A casualty actuary is a professional trained in the analysis, evaluation and management of risk exposure.

The CAS framework describes risks along two dimensions: type of risk and risk management process steps. Table 8 shows the CAS ERM Framework. Precisely determining the proper type of risk is less important than recognizing and identifying all material risk factors that can influence the value of the organization.

The process steps include establishing the enterprise risk management context – external, internal and risk management contexts. Identifying the external context begins with defining the relationship of the enterprise to its environment including analyzing Strengths, Weaknesses, Opportunities, and Threats (SWOT), identifying the organizations stakeholders, and communication policies with stakeholders. Identifying

the internal context involves understanding the overall objectives of the enterprise including its strategy and key performance indicators and identifying the oversight and governance structure. The risk management context involves identifying the relevant risk categories, the amount of coordination throughout the organization and the adoption of common risk metrics.

Table 8. CAS ERM Framework.

ERM Framework				
	Types of Risk			
Process Steps	Hazard	Financial	Operational	Strategic
Establish Context				
Identify Risks				
Analyze/Quantify Risks				
Integrate Risks				
Assess/Prioritize Risks				
Treat/Exploit Risks				
Monitor & Review				

Identifying risks involves documenting the conditions and events that represent threats to the achievement of objectives or represent opportunities for achieving competitive advantage. Next is analyzing and quantifying risk, creating probability distributions of outcomes where possible. Integrating risks involves identifying correlations in risks and aggregating all risk distributions, expressing the results in terms of impact on the enterprise's key performance indicators. Assessing/prioritizing risk involves determining the contribution of reach risk to the enterprise's risk profiles and prioritizing risks to facilitate decisions as to the appropriate treatment of each. The process of treating/exploiting involves any number of strategies including decisions to

avoid, retain, reduce, transfer, or exploit risks. The next step is ongoing monitoring and review, which leads to an ongoing process of risk management.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) [138] is a council of volunteer organizations that was organized in 1985 to sponsor a commission aimed at identifying causal factors in the private sector issue of fraudulent financial reporting, and evolved to include three interrelated subjects: enterprise risk management, internal control, and fraud deterrence. In 2004, COSO published an Enterprise Risk Management (ERM) Framework, which was updated in 2017. The updated framework reflects changes that have taken place in risk management since the original frameworks and stresses the importance of considering risk in the strategy-development process and in driving organizational performance. An important change in the update is attention to cybersecurity risk and how to include it at the enterprise level [141]. The ERM framework recommends the use of a standard cybersecurity framework such as NIST, ISO 27001/2 [26], or the AICPA Cybersecurity Risk Management Reporting Framework [142], and it provides guidance on integrating cyber risk management into ERM.

The COSO ERM framework is composed of twenty principles that are divided into five components of risk management [141]. The five components of risk management are: Governance and Culture, Strategy and Objective-Setting, Performance, Review and Revision, and Information, Communication, and Reporting [141].

The American Society for Healthcare Risk Management (ASHRM) [143] published an ERM framework [144] for healthcare in 2014 along with guidelines to assist

healthcare organizations in its implementation. The steps in the risk management framework include:

1. Risk and opportunity identification
2. Risk evaluation and assessment
3. Strategic risk response and implementation
4. Review, evaluation and monitoring

The main difference between the COSO framework and the ASHRM framework is that the COSO frameworks presents ERM as the work of the executive leadership in an organization, and the ASHRM framework presents ERM as the work of risk professionals that receive oversight from the organization's leadership. Other than that foundational difference, the frameworks are similar.

A distinguishing factor of the CAS framework is that it calls for the identification of risks that should be avoided or minimized as well as opportunistic risks that can be exploited to increase the enterprise's value. The guidance CAS gives enterprises is that informed risk-taking can be a means to competitive advantage. This distinction, while interesting, does not seem to be relevant for cybersecurity risk in network medical devices.

In a 2015 survey [145] of manufacturing companies conducted by Deloitte, the Manufacturers Alliance for Productivity and Innovation (MAPI) revealed that most (93%) of respondents place the ownership of organizational risk with the full board of directors or within the audit committee of the board of directors. Only two percent of respondents report having a risk committee responsible for organizational risk. The study sought to uncover how the risk landscape has changed in manufacturing. The

environmental factors impacting the industry's response to risk include the potential obsolescence posed by changing customer preferences and new products and applications of technology. Consequently, organizations are increasing the pace at which they innovate and execute change. They discovered that the increasing pace of technological advances poses a significant challenge to risk professionals. While technology is providing improved analytical tools and predictive modelling capabilities, technological advances place greater emphasis on data security and cyber vulnerabilities. The results of the study indicate that risk professionals are facing a need to evolve risk assessment to be more analytical, agile, effective at modelling risk, and to embed risk within all levels of an organization. They are also finding the need to change the frequency of assessment cycles.

The MedDevRisk framework could contribute to the risk identification component of an organization's overall ERM. In the case of the COSO ERM framework, the outputs of MedDevRisk could serve as inputs to the performance component of the framework. In the case of the CAS ERM Framework, outputs of MedDevRisk could serve as inputs to the *Identify Risks* process step. In addition, MedDevRisk could also contribute to the Review and Revision Principle of COSO ERM framework and the *Monitor and Review* process step of CAS ERM Framework by providing updated information regarding risk remedy and mitigation actions. It could also contribute to the Information, Communication, and Reporting principle of COSO ERM framework through data and the reporting of data from MedDevRisk.

CHAPTER III

RELATED WORK

The risk assessment framework that is developed in this research is based upon foundational work by several researchers. Each of the works is described below.

3.1 Foundational Relational Database Model

Pardue et al. [41] developed the foundational database-driven approach to risk assessment upon which this research is built. Their work is based on prior conceptual work in information security. The research method was a proof of concept using a hypothetical scenario in the healthcare domain. Pardue et al. underpin their work by identifying the essential elements for information security assessment as Threat, Vulnerability, Asset and Control (TVA-C) from the work of Hoffman, et al. [146] and Whitman [147] as the core structure for their database design. To this list of elements Pardue et al. add Threat Source, Threat Action, Cause, and Domain along with relevant associative tables to complete the structure of their relational database. These essential elements are operationalized as entities in the relational model.

Risk assessment is defined by Pardue et al. as "identification of threats vulnerabilities and assets and estimation of relative riskiness" [41]. They further their definition of risk assessment from the work of Shou and Shoemaker [148] to include the ability to "delineate both the strategy to reduce the likelihood of a risk occurring (preventative measures) as well as the measures to respond effectively if a risk becomes a

direct threat (reactive measures)"[148]. Pardue et al.'s definitions for the entities in the database are contained in Table 9.

Table 9. Pardue et al.'s Definitions for Data Entities in Relational Model [149].

Pardue et al. Definitions for Data Entities	
Threat	"the event or circumstance that can result in adverse impact on an organization"
Vulnerability	Per NIST 800-3, a flaw or weakness in system security procedures, design implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.
Asset	**Asset** – Pardue et al. do not provide an explicit definition for an asset, rather, they provide the examples of data, images, hardware, software, networks, people and procedures in the domain of a security environment.
Control	countermeasures designed to restrict, monitor, and protect assets against a threat, thereby minimizing the possibility of a threat exercising vulnerability.
Threat Source	a classification of an agent that either deliberately or accidently exercises a vulnerability. An example is "human-deliberate insider".
Threat Action	The unique combination of a threat, asset, and vulnerability.
Cause	The motivational and situational factors associated with threat sources
Domain	The context for the security environment.

Pardue's goal was to construct a relational database model that is sufficiently abstracted so as to be applicable to a variety of domains. Pardue's work demonstrates that a threat list can be derived specific to a security context from a generic threat database. The ability to rank risks in the database was recognized as a desirable feature for future

work. In 2009, Pardue et al. proposed a risk assessment method for ranking risks [150] . They propose that the approach could be incorporated into their relational database model. Discussion of this method is in section 3.2 below.

A conceptual difference in Pardue et al.'s work and this work is that in Pardue's work assets are generalized. That is assets are not specific to a manufacturer's model number or serial number, rather assets are generalized by the type of asset. For example, an asset in Pardue et al.'s database may be described as a wireless router [41]. Accordingly, threats are generalized and not specific to a particular manufacturer's model. This research seeks to identify vulnerabilities specific to an asset by considering the hardware, operating system, and software of an asset at the model and serial number level where applicable.

3.2 Risk Assessment Using Threat Trees and Monte Carlo Simulation

Pardue et al. proposed a risk model and technique for risk assessment of Direct Recorded Electronic (DRE) voting machines based on attack trees and Monte Carlo simulation [150]. The proposed risk assessment model uses threat trees for assessing risk. Threat trees are derived from Schneier's work using attack trees as a methodology for describing the security of systems [151]. Pardue et al. describe the difference between an attack and a threat as being that attacks are deliberate acts, and threats encompass both deliberate and unintentional acts. They chose a tree structure as the means for documenting threats because, by being an abstraction, the structure allows for comparative reasoning of threats.

They consult NIST 800-30 Risk Management Guide for Information Technology Systems [93] for guidance in developing the threat tree. A two-phase process is used that coincides with the first four steps of the nine-step risk assessment process described in NIST 800-30. They use the NIST definition of a threat – "the potential for a particular threat-source to successfully exercise a particular vulnerability"[93]. Their stated reason for focusing on threats first as being because the identification of threats is the first step in assessing risk.

In the first phase of developing the threat tree, the researches characterized the DRE voting system using Unified Modeling Language (UML) [152]. This step models step one of the NIST-800-30 risk assessment process: system characterization [93]. They explain their choice of UML as being because it provides a systematic means of identifying and documenting system vulnerabilities as well as identifying vulnerable people, technology, and processes. The characterization is based on extensive literature review and information collected in a face-to-face meeting with a panel of domain and security experts consisting of election officials, a representative from NIST, security experts, voting equipment vendors, voting equipment testing labs, election law attorneys, and academics.

In the second phase of developing the threat tree, Pardue et al. go through multiple steps to identify voting system threats with corresponding vulnerabilities and potential controls. This phase model steps two through four of the NIST-800-3 risk assessment process: threat identification, vulnerability identification, and control analysis [93]. The results are cataloged into a threat matrix and organized into a threat tree. First, each researcher independently developed a list of threats, vulnerabilities, and controls

based upon literature review and the model of the system that was developed in phase one. The controls are selected from NIST 800-53 [153]. Then they merge them together and eliminate duplicates. Next, they craft the resulting threat matrix into an initial "straw man" threat tree that they distribute to the domain and security experts for review. From the review they received several hundred suggestions for revisions that were reconciled and implemented into the threat tree by the research team [149].

Pardue et al. convened a panel of domain experts to validate the threat tree. The makeup of this panel is similar to the panel that reviewed the UML diagrams in phase one. In general, the panel deemed the DRE threat tree to be "representative, accurate, and useful" [149]. Pardue et al. therefore propose using the threat tree as the basis for risk assessment. They suggest a Facilitated Risk Analysis Process (FRAP) [154]. FRAP is a group exercise for analyzing and prioritizing risks where the group is composed of domain experts and a facilitator.

Risk is assessed as the product of probability and impact. The NIST definition of risk, "the net negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence" [93], is used. Further, they condition or adjust probability by assessing motivation as a characteristic of the attacker and complexity as a characteristic of the threat.

3.3 Concept for Medical Device Specific Domain Model

Cerkovnik proposed a medical-device-specific concept for modeling the cybersecurity risk posture of healthcare organizations [42]. His work builds upon Pardue et al.'s [41] database driven model for risk assessment by identifying information specific

to the needs of medical device risk assessment. Cerkovnik's database provides a means to identify medical devices and categorize them according to a risk factor, controls, countermeasures, and other attributes that may be of interest to those managing the security of medical devices in a healthcare setting.

In Cerkovnik's work, devices for modeling were selected from the FDA's web-based public 510(K) database by conducting searches records from the years of 2009 through 2014 where network capable medical devices were identified by using search terms such as "link", "smart", and "wireless". The results of the search were further refined to include only devices that had a network interface and were designed expressly for the use of clinicians in a healthcare setting. The search identified six devices that were used in the model.

Once the devices were entered into the relational database, queries were made to identify vulnerabilities and threats that may be associated with them. The information available in the database allowed for sorting the results based on risk, asset value, likelihood of attack, date of last patch, and device attributes that may be of interest to a healthcare facility.

In conclusion, Cerkovnik replaced the database of Pardue et al. with a simpler version. He created a table called tblDevice, but in removing the table tblAsset and its auxilliary tables, some of the ability to store information about and classify assets (devices) is reduced. However, Cerkovnik added auxlliary tables to describe attributes such as how devices interact with data, perform authentication, are physically secured, support data backups, and their security configuration features. These additions offer an

enhanced ability to understand the security posture and report on assets. Merging these two databases is an essential next-step in this work.

3.4 Merged TVA for Medical Device Specific Domain

Seale [40] continued the work of Cerkovonik by merging his database concept with the work database of Pardue et al. [41]. In addition, the model is expanded to include industry standard threat modeling tools and frameworks. The tools considered were STRIDE [155], OWASP [156], NIST Risk Management Framework [157], CVSSv2 [158], CVE [159], NVD [33], and CWE [160].

The research addresses the questions of whether the relational model can be improved by leveraging existing threat modeling and vulnerability assessment tools and frameworks, and if a relational database based on threat-vulnerability-asset associations can be used to generate actionable threat assessment criteria for healthcare organizations regarding medical devices.

After examining the standard threat modeling tools and frameworks identified in the research plan, Seale chose STRIDE [155] for threat modeling, CVE [159] as the source for identifying vulnerabilities, and CVSS [158] to provide ranking metrics. Both CVEs and associated CVSS scores are available in the NVD [33].

The research used SQL views to identify and report threats for each of the STRIDE categories (spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privileges) [155] based upon keyword searches of the text descriptions of threats in the database.

Seale identified relevant CVEs in the NVD by conducting a key term search of the NVD. Terms such as medicine, medical device, insulin pump, infusion pump, defibrillator, and pacemaker were used in the search of the NVD. The search revealed a total of 17 CVEs. Eight of the CVEs were related to the search term insulin pump. Seale selected one of the insulin pumps and inserted that device and its relevant information into her relational database. The information inserted included the relevant threat and vulnerability information that was gathered from the CVE data.

Seale validated the relational model by performing an experimental case study based on a collection of real-world medical devices provided by the University of South Alabama Human-Patient Simulation Unit. Seale received inventory data related to network-capable medical devices that were in use in the Unit. Searches for potential vulnerabilities were conducted using manufacturer reports/user manuals and online sources of information where cybersecurity vulnerability information can be found. The following online sources were searched: FDA MAUDE [161], FDA Medical Product Safety Network (FDA Medsun) [162], FDA 510(k) Pre-Market Notification database [163], FDA Recalls [164], and the NVD [33]. In addition to manufacture reports/users manuals and standard online sources, Shodan [165], a search engine for discovering network connected devices was used to search for the existence of subject devices exposed to the public internet.

The search results demonstrated that there is little cybersecurity vulnerability information available about the medical devices used in the study in public sources. However, there was enough information gathered based on the devices and similar devices to apply a cybersecurity risk assessment in the case study.

The research demonstrated the use of a relational data model based on threat, vulnerability, and asset associations for medical devices could be used to generate actionable threat assessment criteria for healthcare organizations. Furthermore, the model was improved by leveraging existing threat and vulnerability assessments and data.

3.5 The Addition of Vulnerability and Asset Management

Hodges [43] continued the work of Seale by adding a vulnerability evaluation tool to collect device data and match it to known vulnerabilities and a cybersecurity attack modeling tool to better understand adversary attack strategies and identify mitigations. The vulnerability evaluation tool using OVAL [34] provides and automated process for collecting device software components and configuration information and comparing it to published CVEs. This information could inform network administrators of software on medical devices and when a patch may be available. In addition, Hodges added adversarial information through the use of the attack modeling framework CAPEC [31] to provide an adversarial view of how vulnerabilities could be exploited on medical devices. The adversarial view also provides insight into how other areas of the network may be secured in order to protect a device.

An important contribution of Hodges is the incorporation of CVE data into the database allowing for CVEs to be connected to assets through the results of the OVAL evaluation process. Hodges created an automatic process for populating the database with CVE and CAPEC data, which provided a significant improvement.

Hodges selected the Open Vulnerability and Assessment Language (OVAL) [34], an open international community standard for the assessment and reporting of the

machine state of computer, as the tool for collecting and evaluating device configuration information and comparing the configuration information to CVEs.

Common Attack Pattern Enumeration and Classification (CAPEC) [31] was selected for attack modeling tool. This community resource also provides mitigations that can be put in place to reduce the likelihood of a successful attack. CAPEC could be useful in identifying other areas of the network, outside of the medical devices, that may need to be secured and monitored.

Hodges validated the methodology by performing a case study. Like Seale [40], Hodges' case study is based on a collection of real-world medical devices provided by the University of South Alabama Human-Patient Simulation Unit. To collect device data, Hodges installed the necessary software on the devices in the Unit to run the OVAL evaluation tool. The medical devices tested were Apple devices running various versions of MacOS 10. OVAL version 5.10.1.17 was installed on each machine, and OVAL characteristics files were collected locally on each device. The collected data included operating system, installed software, and software configurations in the form of OVAL system characteristics files [34]. The OVAL characteristics files were then compared to OVAL definition files [34] maintained by the Center for Internet Security [28]. The OVAL definitions files contain information about security advisories of vulnerable configurations. The OVAL process makes a comparison of the OVAL system characteristics files to the OVAL definition files and yields an OVAL result file which describes the vulnerabilities present in the device as a result of any matches between the system characteristics file and the vulnerability definition files. The OVAL result file includes any CVEs related to device configurations including the CVE number and title.

Because one of the goals of the research was to be able to remotely collect device configuration data, Hodges conducted a proof of concept of remote collection of OVAL system characteristics data from an Apple devices running MacOS. This proof of concept was done on a device not on the Human-Patient Simulation Unit network. A software tool called jOVAL Professional [166] was used for this test. jOVAL is a tool that allows for the remote collection of OVAL characteristics files for devices, a comparison of the characteristics files to OVAL definition files, and a report of the OVAL result.

Hodges modified the Seale's database to include CPE [167], CVE [159], OVAL results [34], and CAPEC [31]. In doing so the information stored about devices was expanded to include the components of a device since CPEs are related to device components and the components may have CVEs. The new table tblAssetVulnerability is an intersection table serving as a central hub for connecting assets to the many vulnerabilities and CAPECs that may exist for them. CVE data is stored in the table tblVulnerability and the database has been normalized to allow for one CVE to be associated with many assets and many assets to be associated with any one CVE. The newly added tblCAPEC likewise supports CAPECs being associated with many assets and many assets being associated with any one CAPEC. The new table tblOVAL contains OVAL results as created from the OVAL evaluation of device characteristics against OVAL vulnerabilities [28]. There may be many OVAL results associated with any one device. Figure 11 shows the updated database schema resulting from Hodges work.

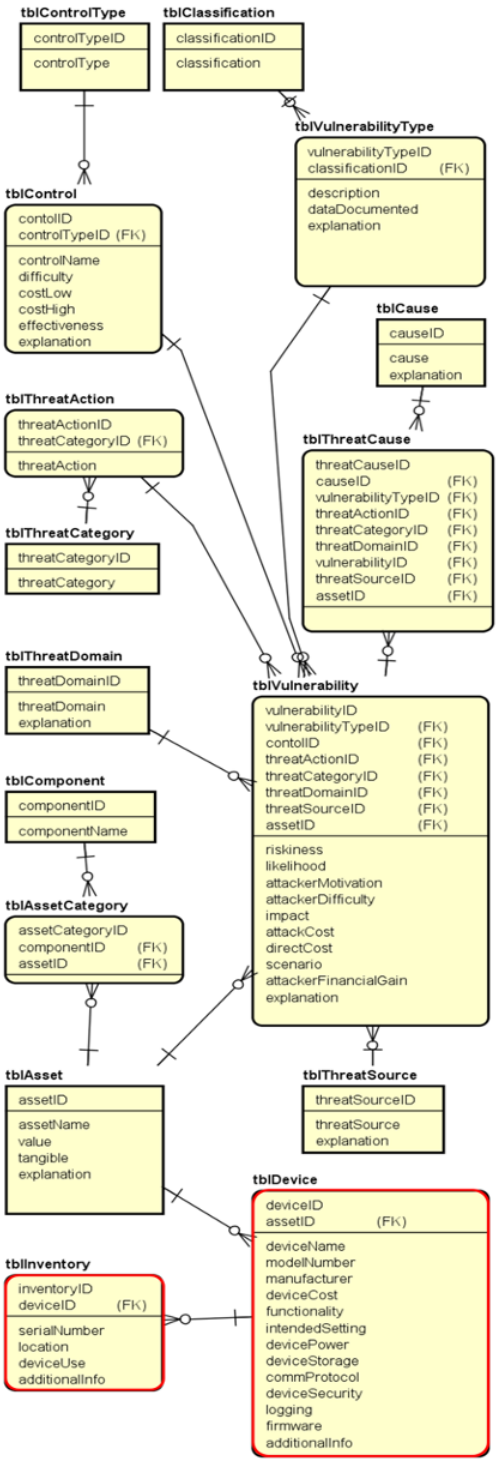


Figure 11. MedDevRisk Schema.

A contribution of Hodges was the automation of importing CVE [159], CAPEC [31], and OVAL [34] results data into the database. This is done through a series of Python scripts that retrieve data from XML files. In the case of CVE and CAPEC, XML downloads are available to the public by the curators of each of the data sources. In the case of the OVAL results files, the XML files were generated by the OVAL evaluation tool. The process of inserting OVAL records into the database also makes consideration for existing OVAL records in the database and updates them with any changes found.

The process of importing CAPECs is similar to that of importing OVAL results into the database. The source of CAPEC XML files is MITRE Corporation's CAPEC website [31]. XML downloads of version 3.0 of CAPEC attack patterns are downloaded and imported into the database. The process accommodates any updates found to CAPEC records that already exist in the MedDevRisk database.

CVE data was imported from XML data feeds made available by NIST on the NVD website [33]. The CVE data imported into the database was from 2006, the earliest year CVEs were created, through 2018. Like OVAL results and CAPEC records, the import updates existing CVE data as necessary and adds new records.

Connections between OVAL results records and CVE records are done through the CVE_ID. Each CVE as a unique ID, and each OVAL result contains the CVE_ID for the CVE that relates to the vulnerability described in the result. Likewise, CVE records contain CWE_IDs which can be used to connect CVEs to any CAPECs that may exist. Not every CAPEC has an associated CWE.

Hodges also developed a method for determining which values in the database tables tblThreatSource, tblThreatAction, and tblControl would be associated with

vulnerabilities. In assessing the values of tblThreatSource and tbleThreatAction, she evaluated the manual method used by Seale, and employed an automated method for evaluating the descriptions of CVEs. CVEs that were identified by the OVAL evaluation were analyzed. A list of key words was identified and used to assign the appropriate source(s), action(s), and control(s) to each CVE. In the case of controls, tblControl contains controls that were developed by Pardue et al. and continued by Seale. In addition, controls exist in Hodges' new table tblCAPEC. The tblControl is kept by Hodges because it is needed in cases where there is no CAPEC associated with a vulnerability.

Hodges also classified vulnerabilities using the classifications that were initiated by Pardue et al. [41] and continued by Seale [40]. In identifying the classification identification value for vulnerabilities, Hodges employed a similar method used to identify threat sources, threat actions, and controls. Hodges evaluated the descriptions of vulnerabilities that were included in the OVAL results. Classifications were assigned to vulnerabilities based on the evaluation criteria.

Hodges research created risk assessment reporting with the modified database. This was done by modifying Seale's [40] STRIDE and TVA reporting queries to reflect the database changes and by creating new queries for reporting assessments based on OVAL results and mitigation reporting queries based on CAPEC information and, in cases where CAPECs do not exist, controls stored in the database as identified by Pardue, et al. [41]. In addition, Hodges created vulnerability reporting based on the adversary's viewpoint. This is done using data retrieved from CAPEC imports and stored in the database. The adversarial reporting provides insight into the adversary by providing the

steps an adversary may take and the techniques they may use to exploit a vulnerability. Hodges concludes that the vulnerability reporting based on CAPEC data provides well-rounded mitigation strategies. For example, understanding the steps an attacker may take to identify the existence of an exploit a vulnerability provides information into other areas of the network that can be used as pivot points to exploit vulnerabilities on a device. This information can enable cybersecurity mitigation strategies to be developed for other areas of the network alongside the medical devices.

Hodges recommends future work to include making changes to the values in the threat and vulnerability descriptor tables in the database to make them more genrealized. In addition, the import process could be improved by adding the creation and update of tblAssetVulnerability records as OVAL results, CVEs, and CAPECs are imported into the database. Hodges identified a lack of industry standard security information on medical devices, and suggests that this could be improved by future researchers doing the following things. Since OVAL records are based on Common Platform Enumeration (CPE) [168] and there are very limited published CPEs for medical devices, future researchers could create CPEs for medical devices and submit them to MITRE for approval and incorporation into the public data repository. In addition to limited CPEs, Hodges also noted limited OVAL definition files for medical devices. These could be created by future researchers and submitted to CIS [28] for approval and incorporation into the public data repository.

In addition to recommended future work, Hodges pointed to a limitation of the research in that the CVE download used was based on XML files. The XML option had limited data and is planned for replacement by NIST with the newer JSON format that is

available. Hodges also noted that the JSON data feed contains more robust data such as impact score, likelihood, and attacker cost that is missing from the XML files. The XML download option was retired in October 2019 [169], so future work must move to the JSON download format.

CHAPTER IV

METHODOLOGY

In this research, we expand the previous work using a database-driven approach to risk assessment that is based on the elements of TVA-C, and we propose and develop a novel framework for real-world asset-based cybersecurity risk assessment. Using a series of three papers, we investigate a real-world medical environment, establish a risk assessment framework, and demonstrate the framework using data received from a partnering healthcare facility.

Figure 12 illustrates the dissertation research activities.

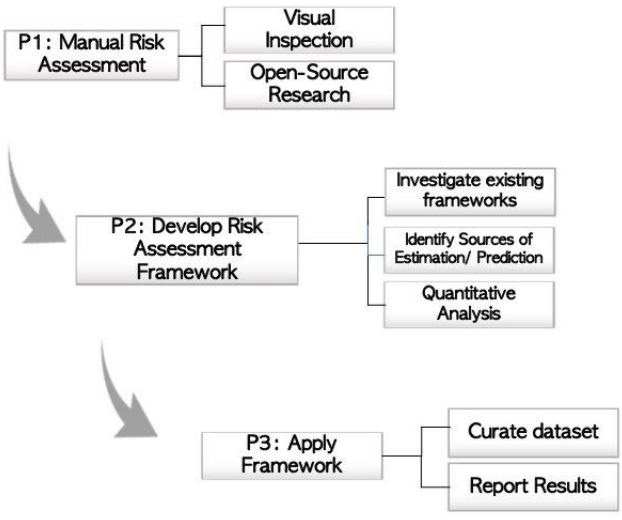


Figure 12. Three Paper Plan.

4.1 Manual Risk Assessment

Chapter V contains our published work [170] where we conducted a visual inspection of a robotic surgical environment at a local healthcare facility. The visual inspection resulted in a list of networked medical device assets that were observed in the robotic surgery room. We identified network vulnerabilities and general access vulnerabilities during the inspection and in our open-source research. These findings represented several potential points of attack that support the hypothesis that live computer-facilitated surgical environments are at risk of being compromised in healthcare facilities.

4.2 Developing a Risk Assessment Framework

Chapter VI contains our published work [171] where propose a risk assessment framework. The framework incorporates sources of vulnerability and threat information, the use of established methods for expert prediction, and methods for quantifying risk and thereby reducing the uncertainty in risk.

4.3 Applying the Framework

In Chapter VII we apply the framework to a subset of data received from a partnering healthcare organization. The results of the assessment include reporting that summarizes and provides insights into risk that can be used by a healthcare organization to prioritize mitigation efforts and investment in resistive controls that can reduce risk.

CHAPTER V

IDENTIFYING OPPORTUNITIES TO COMPROMISE MEDICAL ENVIRONMENTS

5.1 Abstract

The amalgamation of computerized equipment into medical arenas is creating environments that are conducive to security breaches. While previous medical device research has been conducted on medical training equipment, wearable and implantable devices, and on telesurgical systems, there has been minimal research investigating cyber-security vulnerabilities in real-world computer-facilitated surgical environments. The research contribution is an initial empirical analysis of the viability of security vulnerabilities in a computer-facilitated surgical environment. The preliminary results of this investigation generated information that can be used to develop Security Criteria for Integrated Medical Devices.

5.2 Introduction

The rampant amalgamation of technology into the healthcare industry is introducing opportunities for new cyber-attack vectors. Combine this phenomenon with research that indicates that digital evidence, in general, is continuing to integrate and escalate in importance in legal situations, and it is only a matter of time before medical

devices are going to be investigated [172], [173]. The proliferation of technology into the healthcare arena is being encouraged by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 which requires the implementation of Electronic Health Records (EHR) for all healthcare providers that participate in Medicare or Medicaid [4]. Complicating matters, the Federal Bureau of Investigation (FBI) predicts that enticing exploitation opportunities will be created in EHR software and medical devices when companies are required to transition to EHR environments [174]. The FBI report goes on to state that the healthcare industry is not prepared to protect against basic cyber-attacks, much less more sophisticated Advanced Persistent Threats (APTs).

Echoing this idea, a Ponemon Institute [6] press release reports that criminal attacks in the healthcare industry have increased 125 percent from 2010 to 2015. The press release also emphasizes that most healthcare organizations are not prepared to handle cyber threat environments [6]. Confirmation of this statement is visible in a recent news report where Hollywood Presbyterian Medical Center recently acquiesced to a ransom-wear attack [8]. A recent article in Bloomberg Businessweek states that it is possible to hack a Hospira drug pump [2]. This activity prompted a warning from the FDA [16].

Manufacturers are required to report to the FDA all incidents in which a device they manufactured may have contributed to serious injury or death, or has malfunctioned and recurrence on the device or similar devices could contribute to harm or death [161]. The FDA records all reports in the publicly available Manufacturer and User Facility Device Experience (MAUDE) database [161]. Although, the “FDA receives several

hundred thousand Medical Device Reports (MDRs) of suspected device-associated deaths, serious injuries and malfunctions" [161], there is no requirement for timely reporting.

Research has shown that there is significant under reporting and late reporting of MDR incidents [175]. Hence, it is realistic to conclude that the MAUDE database does not provide a complete and up-to-date source for analyzing current security problems with medical devices. Furthermore, because cybersecurity risk assessment and adherence to a cybersecurity framework are recommended by the FDA but not required [51], [176], it is plausible to believe that medical equipment with security vulnerabilities are approved by the FDA for use in hospital settings.

Reports claiming that the healthcare industry is at risk of cyber-attacks, data signifying increased attacks in healthcare environments, and claimed vulnerabilities in specific medical devices prompted the hypothesis that live computer-facilitated surgical environments are at risk of being compromised in healthcare facilities. The hypothesis raises several research questions that need to be explored in order to address the hypothesis:

1. From an open-source intelligence perspective, is it possible to identify plausible points of attack?
2. Is it possible to identify potential attack points by examining an existing footprint?

The research contribution is an initial empirical analysis of the viability of exploiting cyber-security vulnerabilities in computer-facilitated surgical environments and to provide a foundation for future work. The paper is structured as follows: Section 5.3 discusses relevant medical device research. Section 5.4 presents the methodology.

Section 5.5 presents the results of the research. Section 5.6 draws conclusions and presents future work.

5.3 Related Works

The continued integration of technology into the medical field coupled with increasing proliferation has stimulated interest in medical security research. Research includes, but is not limited to, the security of medical training devices [177], implantable devices [178]–[180], wearable technology[181], and telesurgical robots [182], [183].

Venkatasubramanian et al., [184] examine the challenges and research directions in Medical Cyber Physical Systems (MCPS). The authors identify the recent increase in the interoperability of medical devices as providing advantages and improvements in healthcare delivery, while also creating greater attack surfaces. They state that it is essential interoperable medical devices be secure for the primary reasons of their propensity to be deployed in life critical situations and to have access to sensitive health information. The researchers categorize the goals of an attacker as: destroy equipment, disturb operation, reprogram, denial of service, and eavesdrop. They conclude that the domain of MCPS provides a unique set of challenges that are distinct from other cyber physical systems.

Glisson, et al.'s [177] research in compromising a medical training mannequin demonstrates that it was relatively easy for undergraduate students inexperienced in techniques of security vulnerability exploitation to gain access to a medical device using readily available open-source software. The students were able to exploit vulnerabilities in the network security solution and the network protocol to gain access to the device and

to launch a successful denial of service attack. The research provides an initial empirical analysis of the viability of compromising a medical device.

Rushanan, et al. [179] examine the security vulnerabilities of implantable medical devices (IMDs) and body area networks (BANs). Their research reviews the security goals of confidentiality, integrity and availability that should be maintained through the entire life cycle of the device and a list of specific privacy criteria that should exist on the same timeline. They develop an adversary and a threat model and analyze the vulnerabilities of each security and privacy goal against each threat. The researchers point to the increasing complexity of software coupled with the increase in FDA recalls related to software as evidence of a need for research into improving the trustworthiness and reliability of software in IMDs and BANs. In addition they expose the possibility of Electromagnetic Interference (EMI) attacks and eavesdropping on signals previously thought to be private, indicating a need for more research into security and privacy of these devices. The authors indicate that limited access to only older devices is a prevalent research obstacle. They advocate the need for researchers to have access to modern medical devices in order to improve research effectiveness.

Camara, et al. [180] presents a survey of security and privacy challenges with IMDs. The researchers discuss relevant mechanisms proposed to address these issues including their suitability, advantages, and drawbacks. They employ Microsoft's threat category model of Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege (STRIDE) to classify the threats. In conclusion, the authors call for interdisciplinary cooperation among researchers to ensure patient safety

and privacy and security of data. They further call for users of IMDs to know details about the functioning and possible threats in order to raise security awareness.

Malasri et al. [178] identify security threats facing wireless implantable devices. They classify wireless implantable devices into three categories: identification, monitoring, and control devices. Identification devices are defined as those used to provide personal information, which are vulnerable to harvesting, tracking, cloning, relay, and physical compromise attacks. The researchers define monitoring devices as those used to provide physiological information about the patient. These are vulnerable to the same attacks as identification devices with the addition of the potential for an attacker to falsify the patient's identity or generate false patient data. In addition, monitoring devices are vulnerable to denial-of-service attacks. They define control devices as those capable of modifying the physiological characteristics of a patient. This category includes devices that dispense drugs such as insulin pumps and devices that regulate organs such as pacemakers. Control devices are vulnerable to all the threats faced by monitoring devices. In addition, these devices are vulnerable to wireless reprogramming attacks which have the potential to cause direct harm to a patient. The authors identify relay and physical attacks, denial of service attacks, and wireless reprogramming attacks as open issues requiring more research.

Li et al. [181] examine wearable technology, specifically a popular glucose monitoring and insulin delivery system, for security vulnerabilities. With the device user's manual and publicly available information, the researchers are able to eavesdrop on the communication of the glucose monitoring and insulin delivery system. Furthermore, because there is no encryption used in the communication, they are able to

determine the PIN of the device and send packets that could affect the functioning of the device.

Bonaci, et al. [182] experimentally evaluate the scope and impact of a myriad of potential cyber security threats against the Raven II telesurgical robot, a robot used in research and not approved by the FDA for live surgery. All the threats evaluated are related to intercepting and compromising network communication between the robot and the surgeon console. The researchers are able to successfully breach several elements of the system over a wide attack surface, and present recommendations for securing each. Their purpose is to increase awareness of security issues in cyber physical systems. They further believe that the vulnerabilities identified in their evaluation are not limited to teleoperated surgical robots, but to all teleoperated robots.

Lee and Thuraisingham [183] at the University of Texas at Dallas (UTD) collaborated with researchers at the University of Washington BioRobotics Lab (BRL) to develop a security enhanced Interoperable Telesurgery Protocol (ITP). ITP defines the structure of communications between surgical robots and controllers, has been adopted by fourteen research groups, and has been used successfully in testing interoperability between the research groups. The researchers enhanced ITP to address the security elements of communication, authentication, authorization, and security policy development and enforcement. They conclude that secure ITP offers a proof of concept and a framework for the development of security appropriate for the rigorous requirements of telesurgery.

Cooper, et al. [175] conducted a study to evaluate robotic surgery device related complications reported to the FDA. The study compared 12 years of MAUDE data

(January 2000 to August 2012) to court records found in LexisNexis [185] and PACER [186] databases. The results of this study showed there was significant under reporting and late reporting of MDR incidents.

Previous medical device research has identified security issues, safety issues, deliberated challenges and proposed solutions. However, there is minimal empirical research investigating cyber-security issues in live computer-facilitated surgical environments. There is also minimal research identifying criteria that can be utilized to mitigate attacks in production environments.

5.4 Methodology

Oates [187] defines a case study based on previous research by Yin [188] as an "empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident." Oates goes on to state that a case study seeks to obtain detailed insight into the object of the investigation. Hence, this research is an exploratory case study that investigates the identification of cyber-security vulnerabilities in production computer-facilitated surgical environments. Any surgical environment could have been chosen for evaluation. As a matter of convenience, a computer-facilitated surgical environment that contained a da Vinci surgical robot at a local medical facility was selected for examination. Robotic surgical systems are one of the most complex medical devices on the market, and they are playing an increasingly important role in surgical procedures. They were used in over 1.75 million procedures in the decade between 2005 and 2015 [189]. Intuitive Surgical, Inc., manufacturer of the da Vinci Surgical System reports

roughly 652,000 procedures were executed in 2015, up approximately 14 percent from 2014 [190].

The **first step** was to investigate manufacturer documentation and relevant literature for information on the architecture of the da Vinci surgical robot. Intuitive Surgical, Inc.'s website provides information about the company and the da Vinci Surgical System family of products. A review of the site categories of company, products, training, support, and clinical evidence was conducted to gather information relative to the architecture of the system and the context in which it operates.

The **second step** examined the functional footprint of a live production system. The robotic surgical environment at a local medical facility was visually inspected. Two surgical nurses on the robotic surgical operating room team and their supervisor assisted with the inspection.

The **third step** was an investigation to identify the da Vinci operating system. Open-source Intelligence (OSINT) techniques were employed in an attempt to ascertain public information [191]. This step in the investigation can be refined into the following steps.

1. Popular search engines were used to conduct an Internet search. The terms provided in Table 10 were used for the initial search.
2. Follow up searches using popular search engines and social media outlets were conducted using additional terms and names discovered in step one.
3. Additional information obtained in step two, such as reference to patent information, was investigated to determine if they were related/relevant to Intuitive Surgical, Inc.

Table 10. Internet Search Terms.

Step	Search Terms Used
1.	Intuitive Surgical, operating system
2.	Intuitive Surgical, real time operating system
T	Intuitive Surgical, RTOS

5.5 Results and Analysis

The first step produced documentation on how the system is constructed, including all of the parts and how they communicate. The da Vinci Surgical System is a robotic surgical system developed by Intuitive Surgical, Inc. The FDA, which regulates the sale of all medical devices in the United States [192], approved the da Vinci Surgical System for sale in the year 2000. There are four primary components of the da Vinci Surgical System: the surgeon console, patient-side cart, surgical instruments, and vision system [193]. The surgeon console is designed for the surgeon to operate from a seated position. It contains a 3D image viewer and handheld master controls that receive the surgeon's hand movements for translation to movements of the surgical instruments. The patient side cart includes either three or four robotic arms that move in response to the surgeon's hand control movements. The surgical instruments include a full collection of instruments available for use in surgical procedures that are connected to the robotic arms and can be exchanged during surgery. The vision system contains a 3D high definition endoscope (flexible tube with camera and light), image processing equipment, and a display that is viewable by operating room personnel [194]. The website goes on to state that the vision system equipment is stored in an open cart referred to as the vision cart.

Intuitive Surgical offers a service for remote monitoring of the equipment both during operative procedures and while the equipment is idle [195]. This service requires an Internet connection to the device through an Ethernet port or a wireless LAN connection installed on the da Vinci [195]. The online information indicates that the Internet connection allows Intuitive Surgical technicians to passively monitor logs and to proactively monitor and review system performance logs for preventative maintenance purposes. The information from the website claims that the da Vinci system does not store any patient data and has no interfaces to other data systems.

The second step investigates a practical implementation of the equipment. A da Vinci Si Surgical Robot, a Stryker high definition camera, a Karl Storz video display system, and an EHR system were observed. As described in the documentation the da Vinci is composed of a surgeon console, a patient-side cart with four robotic arms, and a vision cart which houses the central computer and a viewing monitor. Surgical instruments and an endoscope are attached to the robotic arms as needed for each procedure. The surgeon console and patient side cart are each connected to the central computer via optical fiber cable for video and data communication between the components. The Stryker high definition camera is used when video recording of a surgical procedure is needed, and the Karl Storz video display system is used to present visual displays of data and images from various hospital systems as needed during surgical procedures. Figure 13. Robotic Operating Room Layout, shows the layout of the robotic surgical operating room observed in this investigation.

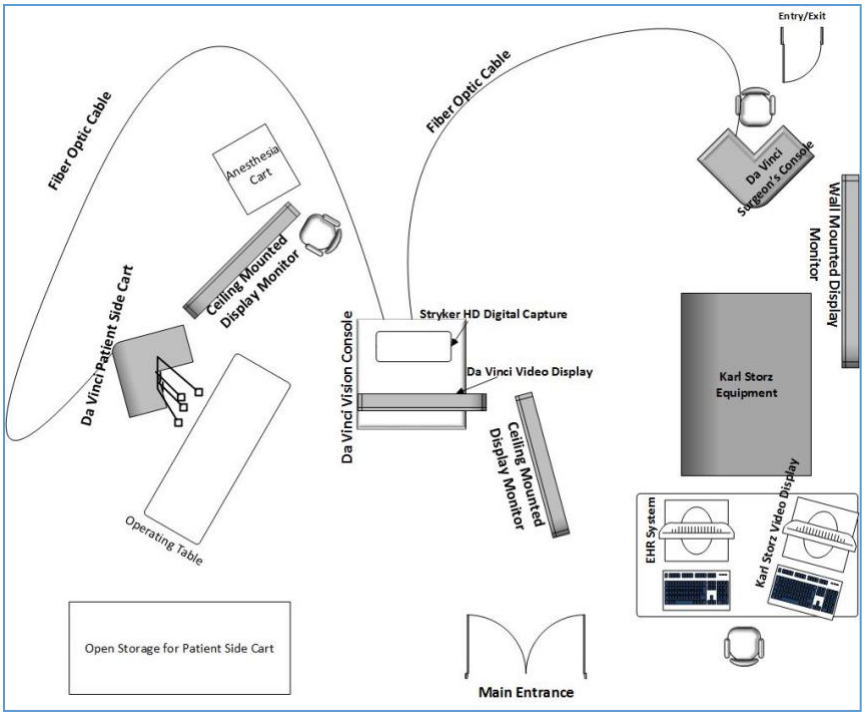


Figure 13. Robotic Operating Room Layout.

A visual inspection of the da Vinci Si Surgical Robot revealed many connectivity options on the back of the da Vinci central computer located in the vision cart. There are three optical fiber ports of which two are in use for connections to the central computer from the surgeon console and the patient-side cart. There is an Ethernet RJ45 port in use that connects to a SonicWALL firewall located at the bottom of the cart through an Unshielded Twisted Pair (UTP) cable. Connected to another port on the firewall is a UTP cable that is rolled up and not connected to anything on the other end. The surgical nurses explained that this would be used for software updates and manufacturer monitoring if it were connected to the Internet. There are several video connections available. Two S-video connections are labeled left and right core video. Tip-Ring-Sleeve (TRS) jacks in Red, Green, Blue, and White (RGBW) are labeled as touch screen video, which is a

function of the video display mounted on the vision cart. A Digital Visual Interface (DVI) connection is labeled touch screen camera. There are several video output options including one DVI, one composite, one S-Video, and one Serial Digital Interface (SDI), with the composite connection being the only one in use. The touchscreen audio has an undetermined connector type being used, an unused headphone mini-jack, and an unused pair of TRS jacks for audio-input and audio-output. There is a Small Form-Factor Pluggable (SFP) network port in use. There is an unused RS-232 serial port, Video Graphics Array (VGA) port and R45 network jack. Lastly, there are three 20-pin circular connectors for power input with two in use. The wireless LAN network interface described in the vendor documentation was not observed. However, no external indicators are necessary for this interface.

Atop the vision cart behind the da Vinci video display is a high definition camera that can be used to record the surgical procedure. It is a Stryker model 240-050-88 [196]. This device has many connection ports on the back. The base communication module on the rear lower left contains the following ports: 1 Personal System 2 (PS2) mouse, 1 PS2 keyboard, 4 Universal Serial Bus (USB), 1 RJ45, 1 parallel, 1 VGA, 1 RS-232 serial, 1 audio microphone and speaker. Built into the back plain in the upper right is a plethora of video input/outputs including a camera port, audio input/output, video input/output, and coaxial composite in/out. There are 6 interface card slots in the lower right. Two of them have cards in them. One has two DVI ports, and the other has three IEEE 1394 high-performance serial bus ports. A DVD burner and high definition screen are located on the front of the device. A search of the vendor's website was unsuccessful in revealing when the Stryker model number 240-050-88 was manufactured. A patent number on the back

of the device was used in an Internet search. The exploration revealed a U. S. patent that was issued in 2004 [197].

Two desktop computers were observed in the operating room. One is the user interface to the Karl Storz Video Display system. This system controls three video display monitors around the room. It interfaces with the various hospital systems to provide access to data and images from these systems for display on the monitors around the surgical room. For example, x-rays from the hospital Picture Archiving and Communication System (PACS) can be displayed during surgery. The second desktop computer is an interface to the hospital EHR system. It is noted that this computer's operating system is Microsoft Windows XP. USB ports were observed on both computers. Located behind the operating table is a wheeled anesthesia console that is not part of this investigation.

A visual examination of the operating room revealed several potential security vulnerabilities, such as exposed USB ports, potential Internet connectivity, an out of support operating system, and minimal physical access restrictions. The visual examination revealed at least nine exposed USB ports. Active USB ports inherently trust connected storage mediums. Stuxnet, a worm that infected one of Iran's nuclear facilities, is suspected of being transferred to air-gapped computers via a USB drive [198]. Hence, USB devices can be used to install malicious software on devices that contain active USB ports. Complicating matters, the evolution of USB attacks has resulted in modified firmware [199]. The firmware on a USB device can be manipulated by an attacker allowing them to take surreptitious actions against the host computer including injecting malicious scripts and capturing data [199]. This type of attack has been labeled as a

BadUSB attack [199]. These types of attacks are plausible if an infected USB device were inserted into an active USB port in the operating room.

The Stryker high-definition camera contains two IEEE 1394 ports. NIST published a security vulnerability summary due to a design flaw in the specification for 1394 that allows for an attacker to gain read and write access to sensitive memory on the host device [200]. The vulnerability appears to have been corrected with an update to the specification in 2008 [201]. It is unclear which version of the IEEE 1394 specification is used on this device. Because the patent for the Stryker device was issued in 2004 [197], it is possible that the vulnerable specification is employed.

Ethernet is an IEEE standard for Local Area Network (LAN) connectivity. LAN access presents two points of attack. The first potential point of attack comes from another device that is connected to the network. The second potential point of attack comes when a LAN has access to a Wide Area Network (WAN), primarily the Internet. In the implementation observed, an Ethernet cable was not connected to a LAN or WAN. However, it is possible that this connection is used when the vendor applies updates and downloads performance logs from the system. The wireless LAN connection described in the vendor literature is another point of attack. Hence, it is possible for an implementation of the da Vinci Surgical Robot to have an active Internet connection at all times via a wireless connection. A wired or wireless connection to the Internet provides a potential attack vector for the injection of malicious software and/or the exfiltration of sensitive data.

Windows XP on the EHR system computer presents another vulnerability. Support for Windows XP was ended by Microsoft in April 2014 [202]. Accordingly, no

security updates are provided by Microsoft. This leaves the operating system vulnerable to malicious software attacks. In addition, software programs running on Windows XP may not be updated by respective vendors creating additional security vulnerabilities.

Lastly, physical security could be tightened in the environment. Enhanced physical security controls would minimize unauthorized access to the equipment. Enhanced monitoring software could minimize the possibility of unintentional individual system and overall operating room compromises as well.

The manufacturer does not identify the operating system used in the da Vinci Surgical Robot. Hence, the third step seeks to identify the operating system of the da Vinci. While recent research indicates that Open-Source Intelligence (OSINT) search behaviors, procedures, and practices are still being refined, it does indicate that these techniques are being used in a variety of online investigations [191]. The third step used OSINT to determine the operating system used by the da Vinci. The preliminary investigation focused on search engines and social media outlets to acquire publicly available information. To investigate this issue, search engines were used to identify companies that listed Intuitive Surgical as a client. Publicly available search engines were then utilized to cross reference identified companies with products and employees of Intuitive. At this point, cross reference searches were conducted with the previous results and surgical patents. The investigation revealed information that suggests the operating system is or has possibly been at some point in time a specific Real Time Operating System (RTOS). It also revealed two robotic surgical related patents that were applied for in 2009 and 2010 and assigned to Intuitive Surgical in 2015 [203], [204].

The preliminary results of this investigation produced data that can be used in the development of Security Criteria for Integrated Medical Devices (SCIMD). The primary data suggest that network connections, live ports, operating system vulnerabilities, and physical access should be considered when securing robotic operating room environments.

5.6 Conclusions and Future Work

The reality is that computer-facilitated surgical environments are complex atmospheres that will continue to be integrated into the medical field. Open-source analysis reveals that data can be acquired from the Internet that can be used to identify plausible points of attack. On-site analysis identified network vulnerabilities, general access vulnerabilities, and open-source opportunities to acquire relevant data. In this particular scenario, the LAN capabilities provided potential attack vectors from local and Internet-connected devices. In addition, open USB ports and antiquated operating systems provide additional paths for compromising devices. The OSINT investigation indicates that the operating system could be an RTOS. The data collected from the on-site analysis identified several potential points of attack. Hence, the initial analysis supports the hypothesis that live computer-facilitated surgical environments are at risk of being compromised in healthcare facilities. The preliminary investigation contributes to the development of SCIMD.

Future research will expand the criteria that can be used to mitigate an attack in computer-facilitated environments. This will necessitate the examination of a variety of medical environments, such as hospitals, outpatient medical facilities, doctors' offices,

and simulation labs to identify and refine the criteria needed to secure a variety of medical environments. In conjunction, research should also investigate reverse engineering medical equipment in computer-facilitated surgical environments to discover security vulnerabilities, identify relevant residual data that is present after interactions and establish forensic procedures for investigating medical equipment. Further research will investigate potential security vulnerabilities inherent in RTOSs and identify design considerations that can mitigate these vulnerabilities. Building on this line of thought, future research will identify performance problems with medical equipment that could be indicative of a cyber-attack. These problems will be translated into practical exercises that can be used to train medical professionals to detect performance problems with medical equipment that could be indicative of a cyber-attack.

CHAPTER VI

A QUANTITATIVE RISK ASSESSMENT FRAMEWORK FOR THE CYBERSECURITY OF NETWORKED MEDICAL DEVICES

6.1 Abstract

Medical devices are increasingly the source of cybersecurity exposure in healthcare organizations. Research and media reports demonstrate that the exploitation of cybersecurity vulnerabilities can have significant adverse impacts ranging from the exposure of sensitive and personally identifiable patient information to compromising the integrity and availability of clinical care. The results can include identity theft and negative health consequences, including loss of life. Assessing the risk posed by medical devices can provide healthcare organizations with information to prioritize mitigation efforts. However, producing accurate risk assessments in environments with both sparse historical data and a lack of validation regarding the accuracy of forecasts is particularly challenging.

We present a risk assessment framework for quantifying the risk posed by connected medical devices in trusted healthcare networks. Our framework is built upon prominent existing frameworks and guidance for general risk assessment and cybersecurity risk assessment. We add a method for quantifying risk, which to our knowledge is novel in the context of medical devices on trusted networks. The

framework provides a structure for combining publicly available information along with expert elicitation about threats, vulnerabilities, and consequences. The goal is to provide healthcare organizations with actionable information for prioritizing and mitigating risks in medical devices.

6.2 Introduction

Cybersecurity incidents are on the rise, and organizations face the challenge of protecting against attacks from an adversary that is increasing in sophistication [205]. Healthcare organizations are experiencing significant security incidents [206], [207]. Research has demonstrated that medical devices pose cybersecurity vulnerabilities in healthcare networks and that they are being used as key pivot points by attackers to establish command and control within networks from where data can be exfiltrated and ransomware may be launched [19], [208]. Email phishing attacks are reported as a significant source of cybersecurity exposure [206], and while antivirus protection may quickly clear malware from workstations, the malware may swiftly spread to medical devices where they are not as well protected [2]. Once on an unprotected medical device, malicious actors can investigate network resources and plan their attack. In addition, while Internet of Medical Things (IoMT) devices add value to healthcare delivery, they also present cybersecurity challenges to healthcare organizations [209].

The effect of cyberattacks in healthcare can be the disruption of information technology operations, the unavailability of clinical care, or damage to systems and devices [206]. The extent of adverse impacts to patient health due to cybersecurity events is largely unknown due to a lack of mechanisms to examine patient safety in the context

of cybersecurity [210]. However, two legal proceedings alleging deaths related to ransomware attacks on hospital networks have been reported [211], [212].

Reports that medical devices are at increased risk of cybersecurity vulnerabilities, evidence signifying increased attacks in healthcare environments, and claimed vulnerabilities in specific medical devices prompted interest in defining a framework for conducting risk assessment specific to medical devices. We present a risk assessment framework for networked medical devices that can serve as input into overall risk management.

Section 6.3 provides related work to our approach and section 6.4 proposes a risk assessment framework for networked medical devices. In section 6.5 we conclude with the merits and limitations of the proposed framework and discuss future work.

6.3 Related Work

Lee et al., [213] examine the challenges and research directions in Medical Cyber Physical Systems (MCPS). The authors identify the increase in the interoperability of medical devices as providing advantages and improvements in healthcare delivery, while also creating greater attack surfaces. They state that it is essential interoperable medical devices be secure for the primary reasons of their propensity to be deployed in life critical situations and to have access to sensitive health information. They conclude that the domain of MCPS provides a unique set of challenges that are distinct from other cyber physical systems. While they identify cybersecurity challenges in networked medical devices, they do not propose a solution for assessing the risks.

Sappal and Prowse [28] propose a method for lifecycle management of connected medical devices that emulates electromechanical preventative maintenance and technology management corrective maintenance practices that are already established in healthcare organizations. It provides for lifecycle management of connected medical devices through tracking, scoring, and reporting on cybersecurity vulnerabilities by medical devices. While their approach does not attempt to assess or quantify risk, it provides a means to prioritize vulnerabilities by a weighted average that includes device function, location, operating system, a medical device CVSS score [29], and the failure consequence.

Kaplan and Garrick [100] describe risk as in terms of an overall risk triplet – threat, vulnerability, and consequence. The triplet addresses respectively what can happen, how likely it is to happen, and what are the consequences if it does happen. Kaplan and Garrick demonstrate that probability of frequency aligns with the Bayesian approach. Our framework adopts this conceptual view of risk and relies upon it in our definition of risk.

The domain of cybersecurity risk is one that lacks historical data on which to predict future outcomes [108]. Eliciting the judgment of experts has been used to support risk estimation in domains where there is little historical data on which to predict outcomes [214], [215]. Krisper, et al. [216] demonstrate a process of using multiple experts and combining their judgments using a weighted average based on their performance in earlier calibration tests with one cybersecurity risk scenario.

Lichtenstein and Fischoff [133] demonstrate that training experts to improve probability assessments can be an effective means for improving their accuracy. They

demonstrate a process of eliciting subjective probabilities from the experts and providing immediate feedback on their performance. Practicing this training technique provides an environment that supports improvement in probability estimates with minimal training. These techniques have been used across domains including nuclear energy [217] and conservation science [218]. This research demonstrates the value of calibration in improving expert judgment.

Pardue et al. [37] developed the foundational database-driven approach to risk assessment upon which this research is built. The research method was a proof of concept using a hypothetical scenario in the healthcare domain. Pardue et al. underpin their work by identifying the essential elements for information security assessment as Threat, Vulnerability, Asset (TVA) from the work of Hoffman, et al. [38] and Whitman [39] as the core structure for their design. We build upon the structure provided in this research and add quantification of risk.

Previous risk assessment research has identified security challenges in medical devices, proposed solutions for vulnerability management, applied expert judgment to risk assessment, and proposed solutions. However, there is minimal empirical research investing a cybersecurity risk assessment framework that provides a quantified estimate of the expected loss related to the exploitation of vulnerabilities specific to medical devices. We propose a framework that provides for the identification of risk scenarios considering published cybersecurity vulnerabilities, the identification of threat actors, and the estimation of impact using expert elicitation and weighted criteria that serves to reduce the uncertainty associated with the impact of risk scenarios. The risk assessment

provides quantified estimates of risk scenario magnitudes that can be used to prioritize risk mitigation efforts and serve as input to an overall risk management program.

6.4 Framework for Risk Assessment of Networked Medical Devices

In this research, risk is defined as a measure of the extent to which the organization is threatened by a circumstance or event, expressed as a function of the adverse impact of the circumstance or event and the frequency of its occurrence:

$$R_e = F_e I_e$$

In our framework we refer to circumstances or events as risk scenarios. It is not uncommon for risk to be a function of likelihood and impact. We use frequency instead of likelihood for its suitability for quantifying risk over a given time period.

Existing risk assessment frameworks were investigated to gain insight into methodologies. While any of a number of frameworks could have been chosen as guides to developing a medical device risk assessment framework [66], [67], [219], [220], several sources were selected for their suitability to this context. First, the Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) [59] was selected as the overall guide for conducting the risk assessment. The choice for the Cybersecurity Framework was based on the prevalence of this framework's use in the healthcare sector [71] and its use in conducting risk assessments at our partnering healthcare facility. In addition, the approach to risk assessment in the Cybersecurity Framework is intended to be consistent with the approaches described in the ISO/IEC standards [219], a prominent risk assessment tool set. Second, the NIST SP 800-30 Guide for Conducting Risk Assessment [58] is used for the stepwise structure it provides. Third,

the Factor Analysis of Information Risk (FAIR) [97] framework is relied upon in this research in the process of identifying assets, assessing threat actor capabilities, threat event frequency, loss event magnitude, and in quantifying risk. FAIR provides structure and detail in areas where the Cybersecurity Framework and NIST SP 800-30 are more general.

The risk assessment function within the Cybersecurity Framework includes identifying vulnerabilities, receiving threat intelligence from information sharing forums, identifying internal and external threats, identifying potential impacts and likelihoods, based on the four-step process of the NIST SP 800-30 Risk Assessment Process is shown in Figure 14. A description of the execution of each of the steps in this research follows.

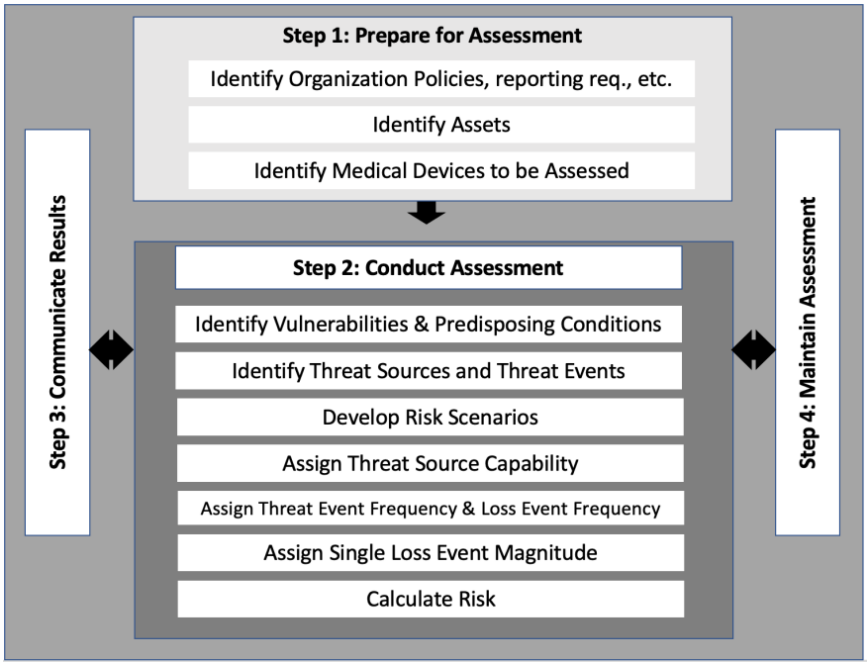


Figure 14. Medical Device Risk Assessment Framework.

6.4.1 Step 1: Prepare for Assessment

The purpose of preparing for the risk assessment is to establish the context and scope of the assessment. This may include identifying organizational policies and requirements for the risk assessment and identifying reporting requirements and methodologies to be used. While this will vary among organizations, identifying the assets, the medical devices, and the timeframe for the assessment is essential to preparing for the risk assessment of medical devices.

6.4.1.1 Identify Assets.

In a medical device risk assessment, it would be logical to consider the medical devices to be the asset. However, Landoll [99] defines assets in risk assessment as those items considered valuable to an organization and its stakeholders. Examples of assets in the context of a healthcare organization may be patient safety, Protected Health Information (PHI), and business revenue. In reflecting on the organization's assets to be protected based on FAIR guidance [97], it became clear that the medical devices themselves are not the assets of value to the organization and its stakeholders. Rather, medical devices may contain assets or be paths to assets.

The process of identifying the assets to be protected involves identifying the things of value to the organization and its stakeholders that could risk well-being if they were to be lost or damaged. Asset identification and asset valuation is obtained by eliciting experts such as organization leadership like finance leaders and executives. In addition to the identification of the assets, an asset valuation can be provided by these experts. Valuation of the assets helps to estimate the potential impact of a risk scenario and to evaluate appropriate controls [99].

6.4.1.2 Identify Target Devices.

The OCTAVE Allegro framework [220] describes information asset containers as places where information assets are stored. Medical devices may be containers for information assets, and they may also be paths to assets. We conclude that medical devices can be in a category that is analogous to the OCTAVE information asset container. We therefore develop a component of the framework for medical devices that is separate from the assets to be protected. We refer to this component as Target Devices.

The target devices selected for a risk assessment are identified by the organization in the preparation step as identified in NIST SP 800-30. The preparation step precedes the risk assessment therefore the process of selecting the medical devices is not discussed in detail here. The device selection could be all or a subset of networked medical devices.

Once device selection is made, an inventory of medical devices is examined and curated to include all the following that apply: asset model number, operating system and version, firmware version, and all installed software with its version. Collecting all of this information may present a challenge for some devices because visibility into the components of medical devices is not always possible and is an ongoing challenge [221]. With this limitation, every effort should be made to identify the components of each device.

The Security Content Automation Protocol (SCAP) [35] is a community effort overseen by NIST that contains standardized expressions. Of interest to us in SCAP is Common Platform Enumeration (CPE) [36] which is a standard method for identifying hardware, software, and operating systems. NIST hosts and maintains the official CPE dictionary, which is available to the public. A search of the CPE dictionary reveals that it

contains entries for medical devices, including component specifications that have known vulnerabilities in the NVD. Because CPE follows a rules-based nomenclature, the CPE can be derived for each medical device and its components. This can then be used to search the NVD for vulnerabilities. We identify the CPE for each medical device and its components to assist later in the identification of published vulnerabilities.

6.4.2 Step 2: Conduct Risk Assessment

The risk assessment can begin once preparation is complete. Our framework is composed of the identification the risk triplet of threat, vulnerability, and consequence [100] that can negatively impact the organization and its stakeholders through damaging the value of assets. The risk assessment tasks are: identify vulnerabilities and predisposing conditions, identify threat sources and events, develop risk scenarios, assign threat source capability, assign threat event frequency, assign single-loss event magnitude, and calculate risk as the expected loss magnitude. Each task is described here.

6.4.2.1 Identify Vulnerabilities and Predisposing Conditions.

Vulnerabilities associated with each of the devices that are reported by the manufacturer should be logged and used in the risk assessment process. In addition, Open Source Intelligence (OSINT) [222] techniques can be used to identify cybersecurity vulnerabilities that may have been reported by other parties.

Common Vulnerabilities and Exposures (CVEs) [33] is a program under the direction of the MITRE Corporation for the purpose of maintaining a list of publicly known cybersecurity vulnerabilities. CVE is intended to be a comprehensive catalog of publicly disclosed cybersecurity vulnerabilities. The NVD is a publicly searchable database that contains each CVE along with some additional information. It includes a

textual description of the vulnerability that may be useful in characterizing the risk scenario(s) that could result in an exploitation. NVD also provides links to external information about the vulnerability. Attributes useful to risk assessment are provided in the NVD, such as a list of all affected hardware and software using CPEs [36]. The CPE is helpful in identifying exactly which computing components are affected by the CVE. In step 1, preparation, we established CPEs associated with each target device to facilitate searching the NVD. A Common Vulnerability Scoring System (CVSS) base score [223] is assigned to each vulnerability in the NVD.

The CVSS base score is composed of two sets of metrics – exploitability metrics and impact metrics, and it provides qualitative and quantitative values. While the CVSS score is not intended to be a measure of risk, there are several metrics in the base score that can be useful in characterizing risk. The metrics we identify to be useful are the Exploitability sub score and the set of impact metrics - Confidentiality, Integrity, and Availability (CIA) Impacts. The exploitability sub score indicates the ease and technical means by which a vulnerability can be exploited. The CIA impact metrics reflect the consequences of a successful exploitation.

We use the CIA triad as security effect attributes in our estimation of adverse impacts. We define security effect attributes as those that effect the systems and/or information assets of the organization. The CIA triad is a widely accept model for information security [224]. Our impact assessment considers the potential compromise of one or more of the CIA components.

Predisposing conditions are those conditions that could contribute to the likelihood that one or more threat events would result in negative consequences [225].

Conditions of interest for each device include: whether it contains PHI, the physical security status of the device, the FDA class [48] of the device, if it is receiving software and firmware updates, and if the device has been designated as 'end of life' or no longer supported with updates by the manufacturer. Table 11 shows example predisposing conditions of interest in risk assessment. These attributes are examples of those that can be useful in understanding the riskiness of the device.

Table 11. Medical Device Predisposing Condition Attributes.

Medical Device	**Physical Status**	**FDA Class**	**PHI ?**	**Getting Updated?**	**End of Life?**
Device 1	In secure room; user authentication required	3	Y	Y	N
Device 2	user authentication required	2	N	Y	N
…	..				
Device n	mobile; authentication required	2	Y	N	Y

6.4.2.2 Identify Threat Sources and Threat Events.

This research considers threats that are specific to the medical devices, described as the information system level in NIST SP 800-30 [58]. In this assessment, threats are decomposed into threat sources and threat events.

6.4.2.3 Identify Threat Sources.

Threat sources are characterized as the intent or method targeted at a vulnerability, or a situation and method that may accidentally exploit a vulnerability [58]. The definition of a threat source used in this research is anything that is capable of acting in a manner that can result in harm [97]. Threats sources, as shown in Table 12, are

generalized as: adversarial/malicious and human errors of omission or commission [58]. They are identified as groups rather than individuals. For example, a threat actor may be a malicious insider, but not a specific individual within the organization.

Threat sources per NIST SP 800-30 are categorized as adversarial, accidental, or structural [58]. This research considers adversarial/malicious and accidental/error threat sources. The structure category is not included as threat sources here because it does not fit with the definition of a threat source that is defined in this research. Furthermore, in reviewing the subcategories provided in NIST SP 800-30, they represent vulnerabilities in the context of medical devices and are considered in that step of the assessment. For example, aging software or operating systems are vulnerabilities in our framework.

Table 12. Sample Threat Agent Library.

Threat Source	Motive	Primary Intent	Sponsor-ship	Preferred Target characteristics	Preferred targets	Capability	Personal Risk Tolerance	Concern for Collateral Damage
Established Cyber-criminal Organization	Financial or PHI	Data gathering and/or dis-ruption of services	Not known	Easy financial gains via remote means	Entities with financial resources or high value assets or IP	Well-funded trained and skilled	Very high	Medium
User (error)	Unmoti-vated Error	goodwill	none	Systems they access	no preference	Low to high depending on system	Low to mediu m	High

The FAIR methodology references the work of Intel [226] in the establishment of a threat agent library. Table 27 shows the attributes that we identify for establishing a threat agent library based on the work presented in the FAIR methodology [97] along

with example threat actors and values. Each of these characteristics bears significance in understanding the threat posed by each source. In developing the threat agent library, a panel is formed of security experts from within the organization and/or industry experts consulted with from outside of the organization who are familiar with the organization's security infrastructure and relevant threat intelligence. The threat agent library should be updated on a regular basis to reflect the state of threats to the organization.

6.4.2.4 Threat Source Capability Estimation.

For each threat source identified in the threat agent library, the capability of the source to compromise assets is estimated by the panel of security experts through an elicitation process. Experts should first be calibrated using established methods for improving the accuracy of expert judgment [133]. The experts in this elicitation would be security experts who have knowledge of the threat agents and the security infrastructure of the organization. The predictions elicited are a general assessment of each threat source's exploitation capability. Included in the assessment is the estimated threat actor capability - minimum, maximum, and most likely - and the expert's level of confidence in the estimate. We use a scale of 1 to 100 to for each estimate. These estimates will be used to perform a PERT distribution of the capability of the actor in measuring the threat event frequency. Table 13 shows a sample threat source capability.

6.4.2.5 Identify Threat Events.

Threats events are specified as single events, actions, or circumstances. Threat events are characterized by the tactics, techniques, and procedures (TTPs) utilized by the threat source.

Table 13. Threat Source Capability.

Threat Source/Agent	Threat Type	Actor Threat Capability Min	Actor Threat Capability Max	Actor Threat Capability ML	Threat Actor Capability Confidence
Insider	Malicious	40	85	50	90
Cybercriminal organization	Malicious	60	90	80	90
User (error)	Error	40	90	50	90

Threat events are identified by reviewing available documentation. For example, there may be documentation that identifies general threats discovered through regulatory compliance processes in the organization. Next, OSINT techniques and review of industry resources should be conducted to identify threat events. This review corresponds to the subcategory "ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources" in the Cybersecurity Framework [59]. Additional threat events can be obtained from examples provided in NIST SP 800-30 [58]. Threat event information may also be gathered from descriptions provided in CVEs discovered in the vulnerability identification process.

6.4.2.6 Develop Risk Scenarios.

We develop risk scenarios for every combination of asset, target medical device, threat source, and CIA impact combination. We begin developing scenarios by listing all the vulnerabilities present for each medical device. For each of these pairs, we identify which assets could be impacted by the vulnerability. For each of these triplets, we identify the threat sources in the threat actor library that would likely be able to and/or

interested in exploiting the vulnerability. Lastly, we identify each of the CIA effects that could occur for each of these possibilities. The resulting list are the risk scenarios that could result in exploitation of any of the vulnerabilities identified.

This list of risk scenarios should contain the following single-valued attributes: asset, target medical device, vulnerability, threat source, and potential CIA effect. Table 14 shows a list of example scenarios.

Table 14. Example Risk Scenarios.

Scenario	**Asset**	**Target Device**	**Vulnerability**	**Threat Source**	**CIA Effect**
AA	Asset 1	Medical Dev 1	CVE ID (or none)	Threat Source 1	C or I or A
AB	Asset 1	Medical Dev 1	CVE ID (or none)	Threat Source 2	C or I or A
AC	Asset 2	Medical Dev 2	CVE ID (or none)	Threat Source 1	C or I or A
..	..				
ZZ	Asset n	Medical Dev n	CVE ID (or none)	Threat Source n	C or I or A

In addition to the risk scenarios resulting from known vulnerabilities, consideration should be given for the possibility of unknown vulnerabilities being exploited. An organization may choose to take the approach that all networked medical devices could be exploited, or they may choose to evaluate them based on the characteristics of the device that were collected in the identification step. For any medical devices with no known vulnerabilities that could have a particular CIA effect, a group of risk scenarios should be developed considering the assets, the threat actors, and the CIA impacts.

6.4.2.7 Assign Threat Source Capability Estimate to Each Risk Scenario.

For each of the risk scenarios, assign an estimate of the threat actor's capability to exploit the vulnerability resulting in the CIA effect, including the minimum, maximum, most likely, and confidence in the estimate. In most cases these values can be taken directly from the threat source capability estimate made earlier in the process. However, if the actor's capability estimate would be different for the given scenario, these values can be changed to reflect the expert opinion of the actor's capability in that scenario.

6.4.2.8 Assign Threat Event Frequency Estimate to Each Risk Scenario.

For each risk scenario, employ expert elicitation to estimate the frequency with which they predict that a threat agent will act in a manner that could result in loss within the given time frame. As in the estimation of threat actor capability, experts not already calibrated should first be calibrated using established methods for improving accuracy [133]. These experts would be security experts who have knowledge of the security infrastructure of the organization and have reviewed available threat intelligence and vulnerability information. The timeframe is that which is identified by the organization in the preparation step. An example would be a one-year timeframe. The estimates include a minimum frequency, maximum frequency, a most likely frequency, and a confidence in the estimate. These values are used to calculate a PERT distribution of threat event frequency as shown here.

$$Threat\ Event\ Frequency\ (TEF) = \frac{Min\ TEF + (4 * Most\ Likely\ TEF) + Max\ (TEF)}{6}$$

Loss event frequency is calculated by multiplying the threat actor capability by the threat event frequency. Loss event frequency, as distinguished from threat event

frequency, is the frequency with which we expect the threat source to successfully exploit the risk scenario resulting in a negative impact to the organization. This value would be less than or equal to the threat event frequency.

*Loss Event Frequency = Threat event frequency * Threat Actor Capability*

In cases where there is an identified CVE in the risk scenario, we find additional information to help us understand severity of the vulnerability and therefore, the frequency with which a risk scenario may be exploited. We use the exploitability subscore [33] of the CVSS score [223], discussed in the vulnerability identification step, to further refine the loss event frequency.

The exploitability subscore is derived from a combination of the CVSS metrics of attack vector (network, local, physical), level of attack complexity (high, low), privileges required (none, low, high), and whether interaction with a user is required. The CVSS exploitability subscore is a numeric value between 0.12 and 3.9 based upon the CVSS v3.1 formula [223]. We use the exploitability sub score by converting it to a percentage of the range 0.12 to 3.9 to serve as a relative indicator of the vulnerability's exploitability, and we multiply this value by the PERT distribution of our expert's estimation of threat actor capability (TAC) as shown below.

$$\text{Vulnerability} = \frac{(CVE\ Expoitablity\ sub\ score - 0.12)}{3.9 - 0.12} x \frac{Min\ TAC + (4\ x\ Most\ Likely\ TAC) + Max\ TAC}{6}$$

The modified calculation for the loss event frequency is shown here.

*Loss Event Frequency = Threat event frequency * vulnerability)*

6.4.2.9 Assign Single Loss Event Magnitude to Each Risk Scenario.

For each risk scenario, we employ expert elicitation to estimate the magnitude of a single loss event. This estimate is the magnitude of a potential single event loss without consideration for frequency. The experts in this elicitation would be business experts from within the organization. It may include financial experts, legal experts, or others who would have knowledge of the value of the assets and the potential impacts that could result from exploitation of a particular asset. The estimates include minimum loss, maximum loss, a most likely loss, and a confidence in the estimate. These values are used to calculate a PERT distribution estimate the single loss event magnitude. It will be multiplied by the frequency estimate gathered above to determine the magnitude within the timeframe chosen for the risk assessment.

In addition to the estimation of loss magnitude, in risk scenarios where there is an identified CVE, a loss magnitude multiplier is calculated using attributes of the CVE. We use the CIA impact [33] of the CVSS score [223], discussed in the vulnerability identification step, to further refine the loss magnitude. The CIA impacts each have a value of high, low, or none.

Table 15. Loss Magnitude Multiplier.

CVE CIA Impact value	**Loss Magnitude Multiplier**
If CVE CIA Impact = Low	1
If CVE CIA Impact = High	1.05
If CVE CIA Impact = None	1
If no CVE or known exploit	1

We choose a loss magnitude multiplier of 1.05 if the impact metric value is high and a multiplier of 1 for values of low or none. Our rationale is that the expert estimation is sufficient for anything that is not characterized as a high impact. Each risk scenario contains only one CIA impact, so there is one multiplier for each scenario. Table 15 shows the loss magnitude multipliers. The calculation for Single Loss Magnitude follows.

$$\text{Single Loss Magnitude} = Loss\ Magnitude\ Multiplier\ x\ \frac{Min\ Single\ Loss\ Mag\ Est. + (4 * Most\ Likely\ Single\ Loss\ Mag\ Est.) + Max\ Single\ Loss\ Mag\ Est.}{6}$$

$$\text{Single Loss Magnitude} = Loss\ Magnitude\ Multiplier\ x\ \frac{Min\ Single\ Loss\ Mag\ Est. + (4 * Most\ Likely\ Single\ Loss\ Mag\ Est.) + Max\ Single\ Loss\ Mag\ Est}{6}$$

6.4.2.10 Calculate the Expected Loss Magnitude for each Risk Scenario.

The expected loss magnitude, or the quantified risk, is calculated for each risk scenario in consideration of the threat source, the threat source capability, the exploitability of the vulnerability, the impact effect, and the single loss expectancy, multiplied by the threat event frequency estimate to arrive at an estimate of the loss that could be experienced within the timeframe of the risk assessment. The calculation is shown here.

Risk = Expected Loss Magnitude = Single Loss Magnitude * Loss Event Frequency (7)

6.5 Discussion and Future Work

The results of the assessment can be communicated through reporting, sorting, and summarizing the details in a manner that is informative to the organization. In addition, Monte Carlo simulations can be performed using methods such as beta distributions.

The framework provides a method for quantifying risk, which to our knowledge is novel in the context of medical devices. The use of expert judgment is necessary in making predictions in domains such as cybersecurity that lack historical data or regularity. Methods for calibrating experts have been established and shown to improve expert judgment. We propose that a reduction in the uncertainty about the riskiness of the cybersecurity status of medical devices can be achieved using this framework.

The next step in the risk management process is to identify mitigations or controls that can reduce the loss magnitude. This is a combination of controls that are already in place and controls that can be implemented. In doing so, a process for quantifying the reduction in loss magnitude that may be done following the same strategy as has been used to estimate the loss magnitude and the threat actor capability here.

Automating the methodology used in this framework using a relational database with automation of inputs of vulnerability information can be conducted to make this scalable to the full medical device inventory of a healthcare organization.

CHAPTER VII

APPLYING A QUANTITATIVE RISK ASSESSMENT FOR THE CYBERSECURITY OF NETWORKED MEDICAL DEVICES

7.1 Abstract

Cybersecurity exploitation is on the rise in the healthcare sector. Medical devices are increasingly the source of cybersecurity exposure and present unique challenges to understanding the risks they pose. The exploitation of cybersecurity vulnerabilities in medical devices can have significant adverse impacts ranging from the exposure of personally identifiable and sensitive patient information to compromising the integrity and availability of computerized resources. Understanding the cybersecurity risk presented by these devices can provide an organization with the opportunity to proactively mitigate risks. However, producing accurate risk assessments in environments with both sparse historical data and a lack of validation regarding the accuracy of forecasts is particularly challenging.

In previous work we presented a risk assessment framework for quantifying the risk posed by connected medical devices in a healthcare organization. The framework provides a structure for combining publicly available information along with expert elicitation about threats, vulnerabilities, and consequences. In this work we illustrate the framework through a case study that assesses risk in medical devices using a dataset

provided by a partnering healthcare organization. We simulate values for expert judgment forecasts to see how different values affect the assessment of risk.

7.2 Introduction

In February 2018, The Council of Economic Advisers to the President of the United States (US) reported that malicious cyber activity cost the US economy an estimated $57 to $109 billion in 2016 [1]. The report places healthcare at approximately seven percent of the Gross Domestic Product, yet it experienced more than 15 percent of the reported cybersecurity breaches in 2016 [1]. This report, among others [2], [3], highlights the cybersecurity risk exposure present in the healthcare sector.

Cybersecurity incidents are on the rise, as is the sophistication of cyberattacks. According to the 2022 Verizon Data Breach Investigations Report (VDBIR) [205], there was a 13 percent increase in ransomware attacks from 2020 to 2021, and complex attacks that leverage malware and/or hacking was the top attack pattern for malicious actors. This demonstrates an increase in advanced persistent threats and highly skilled attackers. As a result, organizations face the challenge of protecting against attacks from an adversary that is increasing in sophistication. Paralleling the VDBIR, ThoughtLab's 2022 study of 1,200 organizations across 14 business sectors [227] revealed that respondents reported more than a 20 percent increase in material data breaches between 2020 and 2021. This provides additional evidence of an increase in successful exploitations. ThoughtLab's study points to an increase in digital transformation, digital integration with suppliers and partners, an increase in the attack surface, and an increase in cybercriminal activity as trends that are contributing to the problem.

Healthcare organizations are experiencing significant security incidents [206], [207]. Research has demonstrated that medical devices pose cybersecurity vulnerabilities in healthcare networks, and that they are being used as key pivot points by attackers to establish command-and-control within networks from where data can be exfiltrated and ransomware may be launched [19]. Email phishing attacks are reported as a significant source of cybersecurity exposure [206], and while antivirus protection may quickly clear malware from workstations, the malware may swiftly spread to medical devices where they are not as well protected [2]. Once on an unprotected medical device, malicious actors can use the malware to investigate network resources and plan their attack. The effect of cyberattacks can be the disruption of information technology operations, and sometimes the disruption of clinical care or damage to systems and devices, with ransomware on the rise [206]. The extent of adverse impacts to patient health due to cybersecurity events is largely unknown due to a lack of mechanisms to examine patient safety in the context of cybersecurity [210]. However, two legal proceedings alleging deaths related to ransomware attacks on hospital networks have been reported [211], [212].

Research has shown that medical devices lack the security necessary to protect them from cyber criminals. For example, research reported in Bloomberg Businessweek claimed that it is possible to hack an infusion pump and control the settings [2], an activity that prompted one of several warnings from the FDA regarding cyber vulnerabilities in medical devices [16], [17] and an advisory [18] from the Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). In addition, legacy systems are pervasive in healthcare organizations [206]. In

another example, TrapX Labs reported the results of a study of advanced persistent threats at three large medical institutions finding medical devices serving as the primary pivot points for attackers [19]. Based on their observation in a number of hospitals, it is Trap X's belief that a large majority of hospitals are infected with malware that has remained undetected for an extended period.

In response to repeated cyber intrusions and the threat they represent to cyber systems, government has responded with regulation and guidance addressing the private sector and federal information systems. Among them, Executive Order 13636 "Improving Critical Infrastructure Cybersecurity" [228] in 2013, and later the Cybersecurity Enhancement Act of 2014 [62], calling for the government and private sector critical infrastructure operators to share information and collaboratively implement risk-based standards. Presidential Policy Directive 21 [229] called for a public-private partnership in strengthening the resilience of critical infrastructure cybersecurity. NIST was tasked with the role of developing cybersecurity risk frameworks for voluntary use by critical infrastructure organizations. The Federal Information Security Modernization Act (FISMA) of 2014 [74] put in place requirements for federal agencies to improve the cybersecurity stature of federal information systems. HR 7898 [230], known as the HIPAA Safe Harbor Law, enacted in January 2021 allows for good cybersecurity practices of healthcare organizations to be taken into account when determining penalties for HIPAA [231] violations and when determining extent and duration of HIPAA audits. HR 7898 thereby incentivizes healthcare organizations to employ best practices and document those practices. Through this combination of regulation, guidance, and

incentives, government and the private sector are guided to build increased cyber defenses.

Agencies, working with the private sector responded to the guidance and regulations. NIST developed the first release of "Framework for Improving Critical Infrastructure Cybersecurity" [232] in 2014. This framework was developed in collaboration with the private sector and academia as a voluntary tool for improving the security of critical infrastructure information systems. NIST also developed the 800 Series Publications [233] to address the security and privacy needs of federal information systems. It provides recommendations, guidelines, and technical specifications, including SP-800-30 "Guide for Conducting Risk Assessments" [58] to address and support the needs of federal information systems. The SP 800 Series Publications could also be of use to non-federal organizations that seek to improve the privacy and security of their information systems.

Mitigating risks and managing cybersecurity vulnerabilities in medical devices are necessary, yet it takes resources that are finite within an organization [234]. Therefore, prioritizing activities that mitigate the highest exposure risks is essential to effective risk management. Automated systems exist that can collect medical device information automatically from network traffic data and provide tools for assessing and managing risks [235]–[237], [238]. These tools can reduce the human effort involved in risk management and provide insights that may otherwise be unavailable. However, to our knowledge there are no risk assessment tools that quantifies the risk posed by cybersecurity exposure in networked medical devices. In addition, while the available tools can provide insight into risk, some healthcare organizations may not have access to

them due to limited budgets [234], making accurate inventory collection and risk management more challenging.

In previous research [171] we proposed a risk assessment for network medical devices. This research demonstrates the framework using medical device data provided by a partnering healthcare organization. The results provide a quantification of risk that can allow healthcare organizations to prioritize risks and apply mitigation efforts to reduce risk most effectively. Building on the work of Pardue et al. [41], the risk model we use is based on the factors of Threat, Vulnerability, and Asset, and Control (TVA-C), and we extend the model to include quantification of risk. The results of the risk assessment can also serve as input into an organization's overall risk management program.

In previous research we defined a framework for the cybersecurity risk assessment of medical devices. In this research we use a case study to apply the framework using medical device data received from a partnering healthcare organization.

This research seeks to answer the following questions:

1. Is it possible to apply our framework to real word medical devices and arrive at quantified risk results?
2. Is a manual risk assessment using our framework a practical solution for healthcare organizations?

In section 7.3 we present related work. In section 7.4, we summarize the risk assessment framework that was proposed in previous research. In section 7.5, we demonstrate the frameworks using a subset of medical devices from a partnering healthcare facility, we discuss the results and future directions in Section 7.6, and Section

7.7 contains our conclusion and future research directions. In Appendix B we conduct an analysis to compare our risk to the risk score provided in the dataset from our partnering organization and to the CVSS score on each CVE.

7.3 Related Work

Venkatasubramanian et al., [184] examine the challenges and research directions in Medical Cyber Physical Systems (MCPS). The authors identify the recent increase in the interoperability of medical devices as providing advantages and improvements in healthcare delivery, while also creating greater attack surfaces. They state that it is essential interoperable medical devices be secure for the primary reasons of their propensity to be deployed in life critical situations and to have access to sensitive health information. The researchers categorize the goals of an attacker as: destroy equipment, disturb operation, reprogram, denial of service, and eavesdrop. They conclude that the domain of MCPS provides a unique set of challenges that are distinct from other cyber physical systems.

Sappal and Prowse [239] propose a method for lifecycle management of connected medical devices that emulates electromechanical preventative maintenance and technology management corrective maintenance practices that are already established in healthcare organizations. They propose modifications to an existing maintenance management system used at a healthcare organization that is the subject of their research. The modifications provide a method for lifecycle management of connected medical devices through tracking, scoring and reporting on cybersecurity vulnerabilities by medical devices. While their approach does not attempt to quantify risk, it provides a

means to prioritize vulnerabilities by a weighted average that includes device function, location, operating system, a medical device CVSS score [240], and the failure consequence.

The domain of cybersecurity risk is one that lacks historical data on which to predict future outcomes [108]. Eliciting the judgment of experts has been used to support risk estimation in domains where there is little historical data on which to predict outcomes [214]–[216]. Krisper, et al [216] demonstrate a process of using multiple experts and combining their judgments using a weighted average based each participant's performance in earlier calibration tests. While expert judgment has been criticized for weaknesses in accuracy, methods have been developed and demonstrated to improve the accuracy of experts and provide useful inputs to risk assessment and a reduction in uncertainty [132], [108]. These methods include training experts to improve subjective probability assessment through a process known as calibration. In this process subjective probabilities are elicited from the experts and immediate feedback on their performance is provided. Practicing this training technique provides an environment that supports improvement in probability estimates with minimal training. A successful training practice that has been shown to reduce the tendency for people to be overconfident in their estimates is to ask them to think of at least two reasons to be confident in their estimate and two reasons that their estimate may be incorrect.

Ganon et al. [241] propose multicriteria decision framework that provides a structured process for selecting among risk management control alternatives. Controls are compared based on their estimated ability to reduce the overall risk triplet (threat,

vulnerability, consequence) [100] of a risk scenario. The process includes expert elicitation as an option for estimating criteria values.

Pardue et al. [41] developed the foundational database-driven approach to risk assessment upon which this research is built. Their work is based on prior conceptual work in information security. The research method was a proof of concept using a hypothetical scenario in the healthcare domain. Pardue et al. underpin their work by identifying the essential elements for information security assessment as Threat, Vulnerability, Asset and Control (TVA-C) from the work of Hoffman, et al. [146] and Whitman [147] as the core structure for their database design. To the core structure, Pardue et al. add Threat Source, Threat Action, Cause, and Domain along with relevant associative tables to complete the structure of their relational database. These elements are operationalized as entities in the relational model. Risk assessment is defined by Pardue et al. as "identification of threats vulnerabilities and assets and estimation of relative riskiness" [41]. They further their definition of risk assessment from the work of Shou and Shoemaker [148] to include the ability to "delineate both the strategy to reduce the likelihood of a risk occurring (preventative measures) as well as the measures to respond effectively if a risk becomes a direct threat (reactive measures)" [148].

Previous risk assessment research has identified security issues in medical devices, deliberated challenges, and proposed solutions. However, there is minimal empirical research investing a cybersecurity risk assessment framework that provides a quantified estimate of the expected loss related to the exploitation of vulnerabilities specific to medical devices. We demonstrate a framework that we proposed in previous work to arrive at such quantification of risk. The framework provides a process for the

identification of risk scenarios considering published cybersecurity vulnerabilities, the identification of threat actors, and estimation of impact using expert elicitation and weighted criteria that serves to reduce the uncertainty associated with the impact of risk scenarios. The risk assessment provides quantified estimates of risk scenario magnitudes that can be used to prioritize risks and can serve as input to a risk management program.

7.4 Framework for Risk Assessment of Networked Medical Devices

In previous work [171] we presented a risk assessment framework for quantifying the risk posed by connected medical devices in trusted healthcare networks. Our framework is built upon prominent existing frameworks and guidance for general risk assessment and cybersecurity risk assessment. We add a method for quantifying risk, which to our knowledge is novel in the context of medical devices on trusted networks. The framework provides a structure for combining publicly available information along with expert elicitation about threats, vulnerabilities, and consequences. The goal is to provide healthcare organizations with a tool for identifying, prioritizing, and supporting actions to mitigate risks in medical devices. The framework is shown in Figure 15.

We define risk *(R)* as a measure of the extent to which the organization is threatened by a circumstance or event (*e*), expressed as a function of the adverse impact *(I)* of the circumstance or event and the frequency*(F)* of its occurrence.

$$R_e = F_e I_e$$

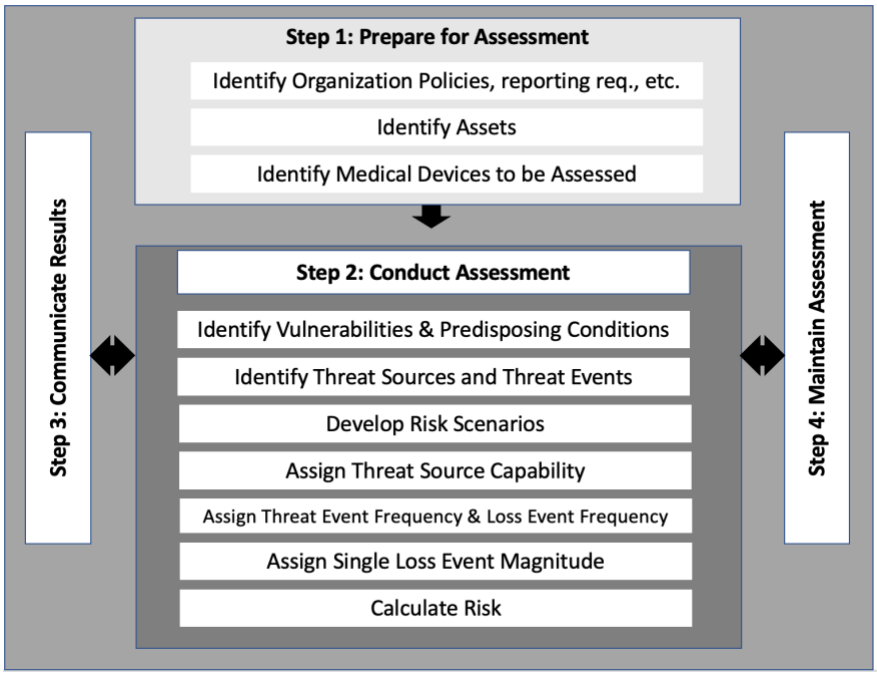


Figure 15. Medical Device Risk Assessment Framework.

Existing risk assessment frameworks were investigated to gain insight into methodologies that could be useful in assessing cybersecurity risk in medical devices. Components of several risk frameworks were adopted in the framework for their suitability to this context. First, the Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) [59] was selected as the overall guide for conducting the risk assessment. The choice for the Cybersecurity Framework was based on the prevalence of this framework's use in the healthcare sector [71] and its use in conducting risk assessments at our partnering healthcare facility. In addition, the approach to risk assessment in the Cybersecurity Framework is intended to be consistent with the approaches described in the ISO/IEC standards [219], a prominent risk assessment tool set. Second, the NIST SP 800-30 Guide for Conducting Risk Assessment

[58] is used for the stepwise structure it provides. Third, the Factor Analysis of Information Risk (FAIR) [97] framework is relied upon in this research in the process of identifying assets, assessing threat actor capabilities, threat event frequency, loss event magnitude, and in quantifying risk. FAIR provides structure and detail in areas where the Cybersecurity Framework and NIST SP 800-30 are more general.

7.5 Case Study Framework for Risk Assessment of Networked Medical Devices

A proof-of-concept case study is conducted using the proposed risk assessment framework to quantify the risk posed by networked medical devices. The framework is modelled in consideration of existing frameworks that provide a base structure for risk assessment. The case study is performed on a subset of medical devices from a real-world healthcare facility to determine the potential adverse impacts to the organization and its stakeholders that could be experienced through cybersecurity exposure of the medical devices being assessed. These adverse impacts are those that effect the Confidentiality, Integrity, or Availability (CIA) [224] of the systems and/or information assets of the organization.

7.5.1 Step 1: Prepare for the Assessment

The purpose of preparing for the risk assessment is to establish the context and scope of the assessment. This may include identifying organizational policies and requirements for the risk assessment and identifying reporting requirements and methodologies to be used. While this will vary among organizations, identifying the assets, the medical devices, and the timeframe for the assessment is essential to preparing for the risk assessment of medical devices.

Preparing for the assessment as guided by NIST SP 800-30 [58] includes identifying the purpose, the scope, the assumptions, the sources of information, and the risk model to be used in the assessment. The purpose of our case study is to assess the cybersecurity risk posed to a healthcare organization and its stakeholders by its networked medical devices. This is done by selecting a subset of devices from a data file of networked medical devices received from the organization. They represent the scope of the risk assessment. We select a timeframe of one-year for our risk assessment. Thus, we are assessing the cybersecurity risk posed by the networked medical devices in our scope over the course of the next year. Support for our choice of the annual time frame is that within FAIR, this is the most commonly used time frame [97].

The sources of information for the risk assessment include the information provided in the device inventory data file, documentation provided by the healthcare organization that identifies general threats discovered through regulatory compliance processes within the organization, the National Vulnerability Database (NVD) [33], the Cybersecurity and Infrastructure Security Agency (CISA) ICS-CERT Advisories [242], and manufacturer advisories. In addition to these sources, additional information related to devices, threats, and vulnerabilities may be discovered through Open Source Intelligence Techniques (OSINT) [222].

7.5.1.1 Identify Assets.

The identification process involved identifying the things of value that could be compromised by a cybersecurity exposure resulting from an exploited medical device.

Table 16 lists the assets that will be considered in this research. Other assets, such as business reputation, could also be relevant, but these assets are selected as the most significant and can provide a demonstration of the assessment process.

Table 16. Assets Selected for Assessment.

Business Revenue
Conf. Bus. Info
Patient Safety
Personally Identifiable Information
Protected Health Information

7.5.1.2 Identify Target Devices.

The devices, or systems, to be assessed were selected from a sample of medical device data received from a collaborating healthcare facility. The device data was received in an electronic format that had been extracted by the healthcare facility from a system they use to manage the cybersecurity of medical devices. The data sample contained 3,520 individual medical device records, representing 147 unique device models and 48 different manufacturers.

We selected a subset of medical devices from the data to demonstrate the framework. The selection process began by identifying the types of devices to be included in the assessment. From a total of 147 different device types in the source data, a selection of recognizable device types was chosen. Table 17 lists the medical device types selected for analysis.

Table 17. Medical Device Types Selected for Manual Risk Assessment.

Medical Device Type
Blood Gas Analyzer
Digital Radiography
ECG
Infusion Pump

Table 18. Medical Device Models Selected for Manual Risk Assessment.

Medical Device Type	**Model Description**	**Manufacturer**	**Operating System**
Blood Gas Analyzer	i-STAT 1	Abbott	Proprietary
Digital Radiography	DRX-Revolution	Carestream	Windows 10 1607
ECG	PageWriter TC70	Philips	Windows 10 1607
Infusion Pump	8015 PC Unit	Becton Dickinson	Proprietary Enea OSE v4.5.2
Infusion Pump Gateway	Alaris Systems Manager	Becton Dickinson	Windows Server 2016 1607

To identify specific device models for the manual risk assessment, one model of each device type was selected. The selection process involved identifying models where there was enough information in the source data to identify the specific model as closely as possible. In addition, we sought to have a variety of manufacturers to the greatest extent possible. Table 18 lists the device models selected. In one case, the infusion pump, there are multiple models selected because the device operates as a system of devices

In addition to the manufacturer and model of each device, the operating system is identified in the source data. This gave us the opportunity to consider operating system-specific vulnerabilities in the devices.

7.5.2 Step 2: Conduct Risk Assessment

Conducting the risk assessment involves seven steps; identify the vulnerabilities and predisposing conditions, identify threat sources and events, develop risk scenarios, assign threat sources and capabilities to risk scenarios, assign threat event frequency and loss event frequency to risk scenarios, assign single loss event magnitude to risk scenarios, and calculate the expected loss magnitude, or risk, for each risk scenario. Each step in the assessment is described here.

7.5.2.1 Identify Vulnerabilities and Predisposing Conditions.

This research identifies vulnerabilities for the devices as those published as common vulnerabilities and exposures (CVEs) in the National Vulnerability Database (NVD) [33] and any vulnerabilities identified in manufacturer advisories. For each device and its operating system, a search is conducted of the NVD. In addition, a search is conducted for manufacturer alerts related to the device. Table 26 in Appendix A identifies the vulnerabilities for each device that are found in the NVD along with a summary of each vulnerability.

Next, Open Source Intelligence (OSINT) [222] techniques were used to identify cybersecurity vulnerabilities that may have been reported by the manufacturer or other parties. For each device, searches were conducted through publicly available sources using the search terms found in Table 19.

All sources discovered using OSINT techniques to find vulnerabilities in the devices selected in this research were vulnerabilities already identified in the CVEs in Table 26 in Appendix A. Although no new information was discovered, this search process could have resulted in new discovery.

Table 19. Search Terms Used to Identify Cybersecurity Alerts.

Search Terms Used in OSINT
Manufacturer name + “ ” + Model description + “ product alert”
Manufacturer name + “ ” + Model description + “ product advisory”
Manufacturer name + “ ” + Model description + “ security alert”
Manufacturer name + “ ” + Model description + “ cybersecurity vulnerability”
Manufacturer name + “ ” + Model description + “ security vulnerability”

7.5.2.2 Identify Threat Sources and Events.

Applying the framework, threats are composed of threat sources and threat events. Once threat sources are identified, we gather relevant factors about each source that helps us characterize our understanding of their general capability to compromise assets. The process for identifying threat sources and threat events is described here.

7.5.2.2.1 Identify Threat Sources in our framework involves following Intel’s methodology [226] for identifying threat sources through the use of a panel of security experts. We simulate Intel’s methodology for identifying threat sources by reviewing available documentation. The first is documentation provided by the healthcare organization that identifies general threats discovered through regulatory compliance processes in the organization. Next, NIST SP 800-30 provides examples of threat sources for consideration.

Next, a review of open-source information was conducted to identify threat sources. This review corresponds to the subcategory “ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources” in the Cybersecurity Framework [59]. First, a review of alerts from the Cybersecurity and Infrastructure Security Agency (CISA) [54] National Cyber Awareness System [243]was conducted.

Alerts were searched for the years 2019 through 2021 that contained the search term ‘health’ and excluded the search term ‘COVID-19-related research’. The rationale for excluding this search term is that these alerts would be relevant to a research setting and not a clinical setting. Second, additional threat source and event information was obtained from NIST risk assessment guidance [58]. Threat event information was gathered from the descriptions provided in the CVEs.

Threat sources per NIST SP 800-30 [58] are categorized as adversarial, accidental, or structural [58]. We identified the categories of adversarial/malicious and accidental/error threat sources as relevant to our risk assessment. The “structural” category in SP 800-30 is not included as threat sources here because it does not fit with the definition of a threat source that is defined in this research. Furthermore, in reviewing the subcategories provided for structure threat sources in the guidance, they represent vulnerabilities in the context of medical devices and are considered in that step of the assessment. For example, aging software or operating systems are considered vulnerabilities in our framework. Table 20 contains the threat sources that we identified for this assessment.

7.5.2.2.2 Threat Source Capability Estimation follows the guidance of Intel [226] and FAIR [97] to develop a threat agent library that contains relevant factors about each threat source, such as motive, intent, capability, and risk tolerance. An assessment of each threat source was conducted by reviewing research and media sources related to exploitations by each occurring in healthcare and other industries [205], [227], [206], [210]. This assessment simulates what could be elicited from experts in the organization

Table 12 in Appendix A shows the Threat Agent Library that was created for this assessment.

Table 20. Threat Sources Identified in Risk Assessment.

Category	Subcategory	Source	Description
Adversarial /Malicious	Malicious Individual	Outsider	Individuals that seek to exploit the organization's dependence on cyber resources
		Insider	
		Trusted or privileged Insider	
	Criminal Organization	Established Cybercriminal organization	Groups that seek to exploit the organization's dependence on cyber resources
	Nation-State	Rogue Nation	Nation states that seek to exploit the organization's dependence on cyber resources
Accidental/ Error	User	User	Erroneous actions taken by individuals while executing their everyday responsibilities.
		Privileged User/ Administrator	

For each threat source identified in the threat agent library, the capability of the source to compromise assets is estimated. Table 21 shows our estimation of each threat source's capability to exploit a vulnerability. We use a scale of 1 to 100 to for each capability estimate, and for our confidence level in the estimate. We refer to this as a general capability base because it may be used in a risk scenario, or it may be adjusted in an individual scenario to reflect our estimate of the source's capability with respect to that particular risk scenario.

7.5.2.2.3 Identify Threat Events considers events described in the CVEs [33] associated with the medical devices, in CISA advisories [242] related to vulnerabilities in

the devices, in manufacturer advisories, and in media reports of actual exposures. The threat events identified were characterized by the effect its exploitation would have on CIA. Each threat event could have one or more of these effects. Table 22 shows the CVEs that were discovered for our target medical devices and possible CIA effects identified for each CVE. For medical devices that had no published vulnerabilities, a risk scenario was created with each of the threat sources and each of the CIA effects with an estimated likelihood. This allows for the possibility of zero-day exploits [244], or the exploitation of vulnerabilities that are not yet known. Likewise, in cases where a particular threat source was unable to produce one or more of the CIA effects through any of the vulnerabilities on a particular medical device, a scenario was considered with those threat sources and each of those CIA effects to allow for the possibility of those zero-day exploit effects.

Next, each vulnerability, threat source, CIA effect triplet was evaluated to determine if the threat source could possibly carry out the threat event. A list of possible triplets was developed.

Table 21. Threat Source General Capability.

Threat Source/Community	**Threat Type**	**Actor Threat Capability Min**	**Actor Threat Capability Max**	**Actor Threat Capability Most Likely**	**Threat Actor Capability Confidence**
Insider	Malicious	40	85	50	80
Outsider	Malicious	50	85	55	80
Trusted or privileged Insider	Malicious	80	99	98	80
Cybercriminal organization	Malicious	60	90	80	80
Rogue Nation	Malicious	95	99	98	80
User (error)	Error	40	90	50	80
Privileged User/Admin (error)	Error	80	99	98	80

Table 22. CIA Effect(s) Possible for Each CVE.

Vulnerability ID	CIA Effect (s)
2016-8375	Confidentiality, Integrity, Availability
2016-9355	Confidentiality, Integrity, Availability
2017-0079	Confidentiality, Integrity, Availability
2017-8543	Confidentiality, Integrity, Availability
2017-8589	Confidentiality, Integrity, Availability
2018-14799	Confidentiality, Integrity, Availability
2018-14801	Confidentiality, Integrity, Availability
2019-11479	Availability
2020-25165	Availability
2021-26424	Confidentiality, Integrity, Availability

7.5.2.3 Develop Risk Scenarios.

Following our framework, we develop threat event scenarios for every combination of asset, target medical device, vulnerability, threat source, and CIA effect combination. We begin developing threat scenarios by listing all the vulnerabilities present for each medical device. For each of these pairs, we identify which assets could possibly be impacted by the vulnerability. For each of these triplets, we identify the threat sources in the threat actor library that would likely be able to and/or interested in exploiting the vulnerability. Lastly, we identify each of the CIA effects that could occur for each of these possibilities. The resulting list are the risk scenarios that could result in exploitation of any of the vulnerabilities identified.

In addition to the risk scenarios resulting from known vulnerabilities, consideration is given to the possibility of unknown vulnerabilities being exploited. For any medical devices with no known vulnerabilities that could have a particular CIA affect, a group of risk scenarios is developed considering the assets, the threat actors, and

the CIA effect. We also consider risks that could occur as a secondary effect. For example, if an adversary obtained network access credentials due a vulnerability in one medical device, they may be able to use the network access credentials to gain access to assets other than those accessible through the medical device and thereby cause further impact effects than those identified in the vulnerability. Following the framework, we develop a list of 258 risk scenarios. Table 23 shows a sample of the risk scenarios that were developed in our case study.

7.5.2.4 Assign Threat Source Capability Estimation to Scenarios.

For each risk scenario we estimate the capability of the threat source to cause the identified effect. In most cases the threat source capability in the threat actor library that we identified earlier in the risk assessment could be applied to the scenario. However, in some scenarios we adjusted the capability of the source to exploit the scenario. For example, there was a vulnerability that required physical access to exploit. We consider a rogue nation to be a quite capable threat source in general, however, in this case we considered the rogue nation's capability to be reduced substantially due to their physical distance from the medical device.

7.5.2.5 Assign Threat Event Frequency and Loss Event Frequency to Scenarios.

We simulate expert elicitation to estimate the frequency with which each risk scenario could be attempted to be exploited within the one-year timeframe identified for this assessment. Our estimates include a minimum frequency, a maximum frequency, a most likely frequency, and a confidence in the estimate. These values will be used to calculate a beta PERT distribution of frequency. The formula for Threat event frequency is shown below.

Table 23. Case Study Sample Risk Scenarios.

Scenario	Asset	Target Device	CVE	Threat Community	CIA Effect
1	PHI	PageWriter TC70	2018-14799	Insider	Confidentiality
2	PHI	PageWriter TC70	2018-14799	Outsider	Confidentiality
3	PHI	PageWriter TC70	2018-14799	Trusted or privileged Insider	Confidentiality
4	PHI	PageWriter TC70	2018-14799	User (error)	Confidentiality
5	PHI	PageWriter TC70	2018-14799	Privileged User/Administrator (error)	Confidentiality
6	Patient Safety	PageWriter TC70	2018-14799	Insider	Integrity
7	Patient Safety	PageWriter TC70	2018-14799	Outsider	Integrity
8	Patient Safety	PageWriter TC70	2018-14799	Trusted or privileged Insider	Integrity
9	Patient Safety	PageWriter TC70	2018-14799	User (error)	Integrity
10	Patient Safety	PageWriter TC70	2018-14799	Privileged User/Administrator (error)	Integrity
11	Business Revenue	PageWriter TC70	2018-14799	Insider	Availability
12	Business Revenue	PageWriter TC70	2018-14799	Outsider	Availability
13	Business Revenue	PageWriter TC70	2018-14799	Trusted or privileged Insider	Availability
14	Business Revenue	PageWriter TC70	2018-14799	User (error)	Availability
15	Business Revenue	PageWriter TC70	2018-14799	Privileged User/Administrator (err or)	Availability
…					
32	PHI	i-STAT 1	None	Insider	Confidentiality
33	PHI	i-STAT 1	None	Outsider	Confidentiality
34	PHI	i-STAT 1	None	Trusted or privileged Insider	Confidentiality
35	PHI	i-STAT 1	None	Cybercriminal organization	Confidentiality
36	PHI	i-STAT 1	None	Rogue Nation	Confidentiality

$$Threat\ Event\ Frequency\ (TEF) = \frac{Min\ TEF + (4 * Most\ Likely\ TEF) + Max\ (TEF}{6}$$

Loss event frequency is calculated by multiplying the threat source capability by the threat event frequency as shown below. Loss event frequency, as distinguished from

threat event frequency, is the frequency with which we expect the threat source to successfully exploit the risk scenario resulting in a negative impact to the organization. This value would be less than or equal to the threat event frequency.

*Loss Event Frequency = Threat event frequency * Threat Actor Capability*

In cases where there is an identified CVE in the risk scenario, we make use of components of the CVSS score to help us understand the severity of the vulnerability and therefore the frequency with which exploitation could occur. The exploitability subscore of the CVSS is a value between 0.12 and 3.9 that describes the characteristics of the vulnerability that could lead to successful exploitation. We calculate the percentage of the exploitability subscore on the range of 0.12 and 3.9. We refer to this metric as the vulnerability metric and use it to modify the capability with which we would expect the threat source to be successful in exploiting the scenario. The calculation for the loss frequency multiplier is described in our previous work where we presented the framework [171] and summarized here.

$$\text{Vulnerability} = \frac{(CVE\ Expoitablity\ sub\ score - 0.12)}{3.9 - 0.12} x \frac{Min\ TAC + (4\ x\ Most\ Likely\ TAC) + Max\ TAC}{6}$$

$$\boxed{\text{Vulnerability} = \frac{(CVE\ Expoitablity\ sub\ score - 0.12)}{3.9 - 0.12} x \frac{Min\ TAC + (4\ x\ Most\ Likely\ TAC) + Max\ TAC}{6}}$$

The modified calculation for the loss event frequency is shown here.

*Loss Event Frequency = Threat event frequency * vulnerability*

7.5.2.6 Assign Single Loss Event Magnitude Estimate to Scenarios.

Following guidance in the FAIR [97] framework, for each risk scenario an estimate of a single loss event magnitude is made. We estimate these values based on a number of factors including characteristics of the medical device, including the FDA

medical device classification [245], [246], the estimated value of the asset that may be compromised, by reviewing HIPAA regulations for data exposure financial penalties, and reviewing research and media sources related to the cost of a data breach [231], [247] in healthcare and other industries. Estimates were made about the number of medical records stored in the hospital database based on the total number of beds in the hospital, the total patient days, the total number of hospital discharges reported. The number of employee records and PII stored in the human resource system is estimated based on number of current employees accounting for an estimate in employee turnover and estimating the storage of historical records on former employees. The daily revenue is estimated based on reported total annual revenue [248]. Estimates of the magnitude of business revenue impact is made by multiplying the daily revenue impact by an estimate of the number of days it could take to recover from the exposure event. The estimates made here simulate what could be elicited from experts in the organization.

The estimates of single loss event magnitude include a minimum loss, and maximum loss, and a most likely loss for each risk scenario. In addition, the confidence of the estimation – represented as a percentage - is documented.

In addition to the estimation of loss magnitude, in risk scenarios where there is an identified CVE a loss magnitude multiplier is calculated using a component of the CVSS. While the CVSS score [249] identified in each CVE is intended to represent the severity of a vulnerability not its risk, some of the metrics that makeup the base score can be useful in considering the magnitude of impact. Of relevance to estimating the magnitude of a loss event, are the impact metrics of confidentiality, integrity, and availability [33]. The possible values for each of these is ‘high’, ‘low’, or ‘none’. We choose a loss

magnitude multiplier of 1.05 if the impact metric value is ‘high’ and a multiplier of 1.0 for values of ‘low’ or ‘none’. Our rationale is that the expert estimation is sufficient for anything that is not characterized as a high impact. Each risk scenario contains only one CIA impact, so there is only one multiplier for each scenario. Table 24 shows the loss magnitude multipliers.

Table 24. Loss Magnitude Multiplier.

CVE CIA Impact value	Loss Magnitude Multiplier
If CVE CIA Impact = Low	1.0
If CVE CIA Impact = High	1.05
If CVE CIA Impact = None	1.0
If no CVE or known exploit	1.0

Our calculation for single Loss Magnitude uses a PERT distribution of the estimated loss magnitude modified by the Loss Magnitude Multiplier.

Single Loss Magnitude

$$= Loss\ Magnitude\ Multiplier\ x\ \frac{Min\ Single\ Loss\ Mag\ Est. + (4 * Most\ Likely\ Single\ Loss\ Mag\ Est.) + Max\ Single\ Loss\ Mag\ Est.}{6}$$

7.5.2.7 Calculate the Expected Loss Magnitude for each Risk Scenario.

The expected loss magnitude is calculated by multiplying the expected loss event frequency by the expected single loss magnitude. We perform a beta PERT distribution of our estimated values and run Monte Carlo simulations of the results.

Risk = Expected Loss Magnitude = Single Loss Magnitude * Loss Event Frequency

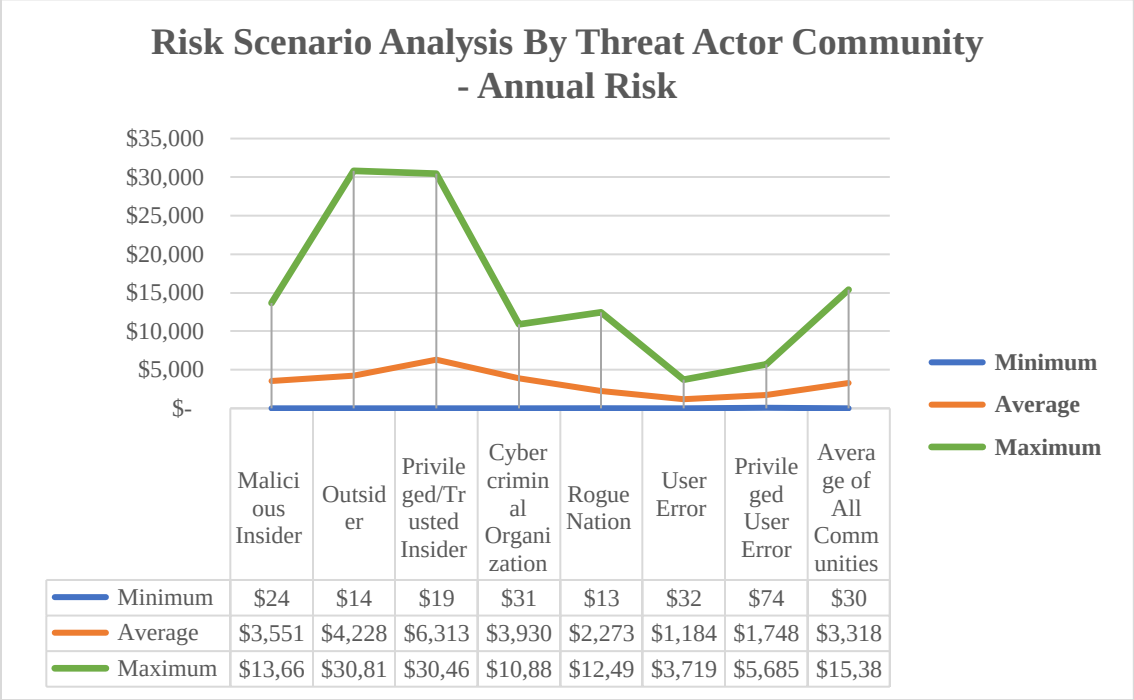
7.6 Discussion

The results of the assessment can be communicated through reporting, sorting, and summarizing the details in a manner that is informative to the organization. Some example reporting is provided here.

Figure 16 shows the minimum, maximum, and average single loss magnitude scenario for each threat actor/community identified in the risk assessment. It reveals that the highest single event risk is posed by the privileged or trusted malicious insider, closely followed by the malicious outsider. In addition, on the far right we see the average minimum, maximum, and average for all threat communities. This average provides a visual illustration of which threat communities are above and below average. The graph provides insights into opportunities for risk mitigation. Interpreting the results and developing an action plan could be supported by drilling down into the details of the risk scenarios. For example, we can find the risk scenarios that are resulting in the highest risk, and the mitigations and resistive controls that are available, or could be made available, to reduce the risk. This graph gives us insight in where to start our investigation.

Figure 17 is a histogram of probability of the risk of the malicious trusted or privileged insider threat community. The graph displays the probability distribution function and the cumulative distribution function. The probability distribution function shows that the annual risk of the malicious insider is a minimum of near $0, a maximum of approximately $32,000, and a most likely risk of approximately $6,400. The cumulative distribution illustrates the confidence we have that the risk falls below the value shown in the graph. For example, we are 90% confident that the risk of a

trusted/privileged insider will be less than approximately $18,000. The histogram can be an informative way of explaining the imprecise nature of risk assessment while reducing uncertainty about risk.



	Malicious Insider	Outsider	Privileged/Trusted Insider	Cyber criminal Organization	Rogue Nation	User Error	Privileged User Error	Average of All Communities
Minimum	$24	$14	$19	$31	$13	$32	$74	$30
Average	$3,551	$4,228	$6,313	$3,930	$2,273	$1,184	$1,748	$3,318
Maximum	$13,66	$30,81	$30,46	$10,88	$12,49	$3,719	$5,685	$15,38

Figure 16. Risk Scenario Analysis by Threat Actor/Community.

A histogram of an individual risk scenario is shown in Figure 18. This scenario was chosen because it is one of the highest risk scenarios in our assessment. We can see from this graph that we are 90% confident that our annual risk for this scenario is somewhere between $13,000 and $50,000, with the most likely risk being approximately $30,000.

Figure 19 shows the minimum, maximum, and average risk scenarios for each asset identified in the risk assessment. It shows that our asset at the greatest risk is

business revenue. As in the previous analysis, we can also see the average or all assets, which illustrates which assets have risk scenarios above and below the average. We can then drill down into the scenarios to uncover the details around the risk. The details include the scenarios and the mitigations that may be in place, or could be put in place, to reduce the risk.

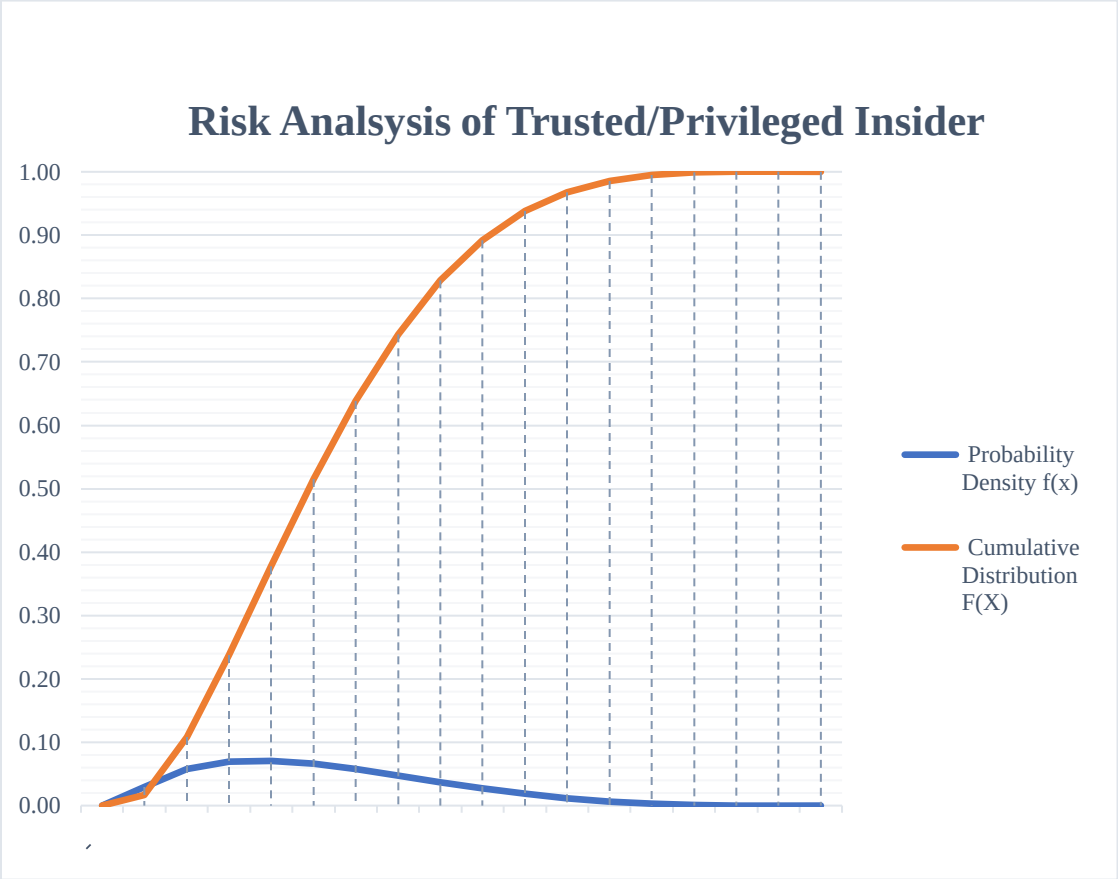


Figure 17. Histogram of Malicious Trusted/Privileged Insider Risk.

Figure 20 shows the minimum, maximum, and average risk scenario for each medical device. In addition, an average of all devices is displayed. We can see from this

graph that our device with the most risk is the infusion pump. In fact, the risk of the infusion pump is so much greater than the other devices that it is the only device above the average risk. This information could support investigating the details that could provide insight into the reason for the large difference in this device in comparison to the other devices.

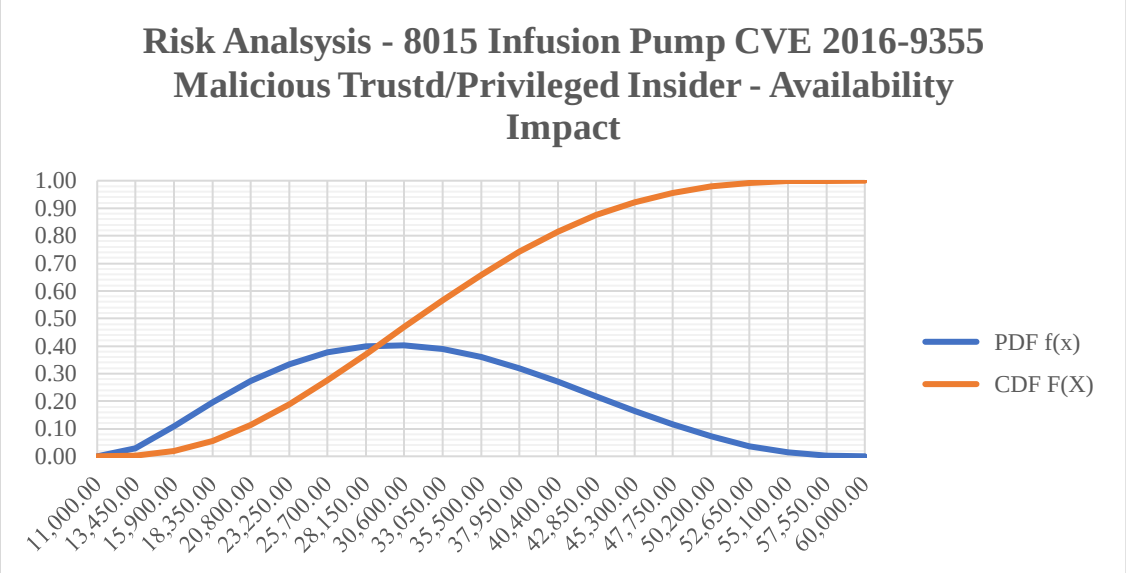
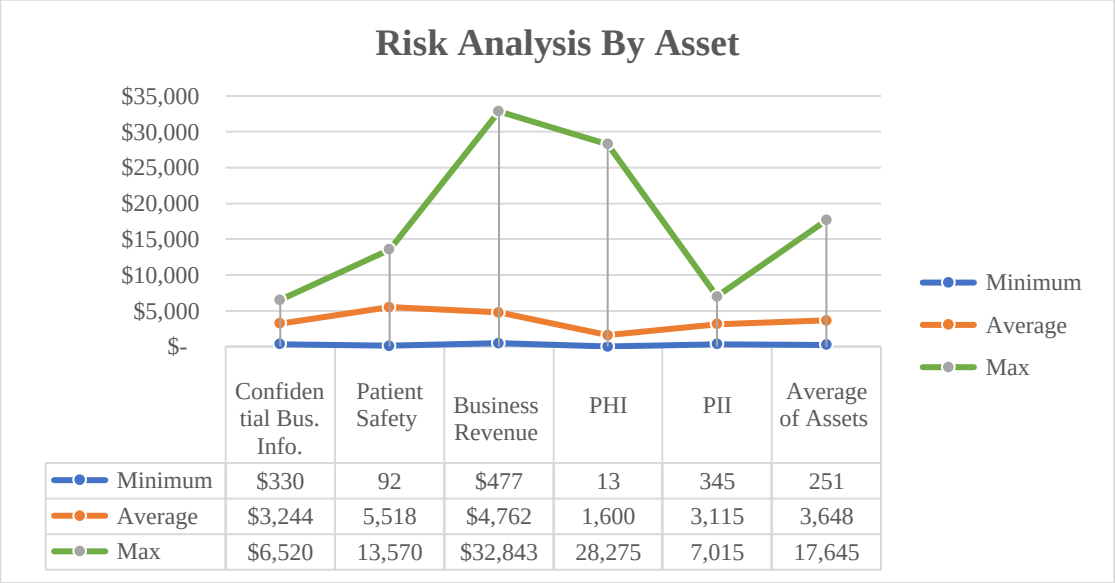


Figure 18. Risk Analysis of Malicious Insider in Individual Scenario.

Figure 21 shows the average minimum, maximum, and most likely Single Loss Magnitude (SLM), and the annual risk for each CVE. In addition, the average loss event frequency for each is shown. This analysis would support a deeper investigation into risk scenarios. In this graph we can see that the maximum single loss magnitude is rather uniform across all CVEs. We can also see that there is much more variety in the most likely single loss magnitude and in the annual risk. The graph shows the average loss event frequency of all the scenarios associated with each CVE, and from this we can see

that two of them are notably higher than the others. In analyzing the details of all the CVEs, the explanation for this higher frequency is the extreme exploitability associated with these two CVEs in combination with the low complexity of the attack required to exploit them. This analysis could support operational decisions about prioritizing patching or otherwise mitigating the vulnerabilities described in CVEs. It could also support managerial decisions regarding investments in mitigations or capital investments in devices replacements.

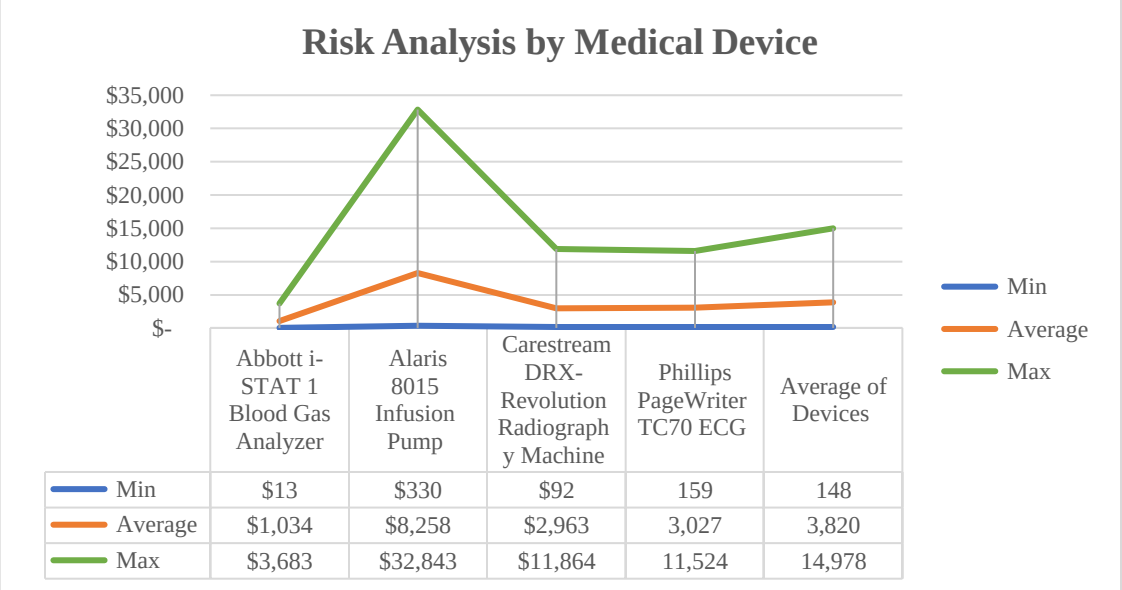


	Confidential Bus. Info.	Patient Safety	Business Revenue	PHI	PII	Average of Assets
Minimum	$330	92	$477	13	345	251
Average	$3,244	5,518	$4,762	1,600	3,115	3,648
Max	$6,520	13,570	$32,843	28,275	7,015	17,645

Figure 19. Risk Analysis by Asset.

Table 25. Sample of Individual Device/CVE Risk Analysis is an analysis of a subset of the risk scenarios associated with CVE 2016-8375 that could impact the organization through the target medical device 8015 PC Unit with internal flash memory. The exploitability of this CVE is 10%, which we calculate based upon the exploitability

subscore of the CVSS score as described in section 4.2.5 of this paper. The risk scenarios are grouped into primary effects and secondary effects, with the primary effect being the risk that can be incurred if the CVE is exploited, and the secondary effects being the subsequent risks that be incurred after the primary risk is incurred.

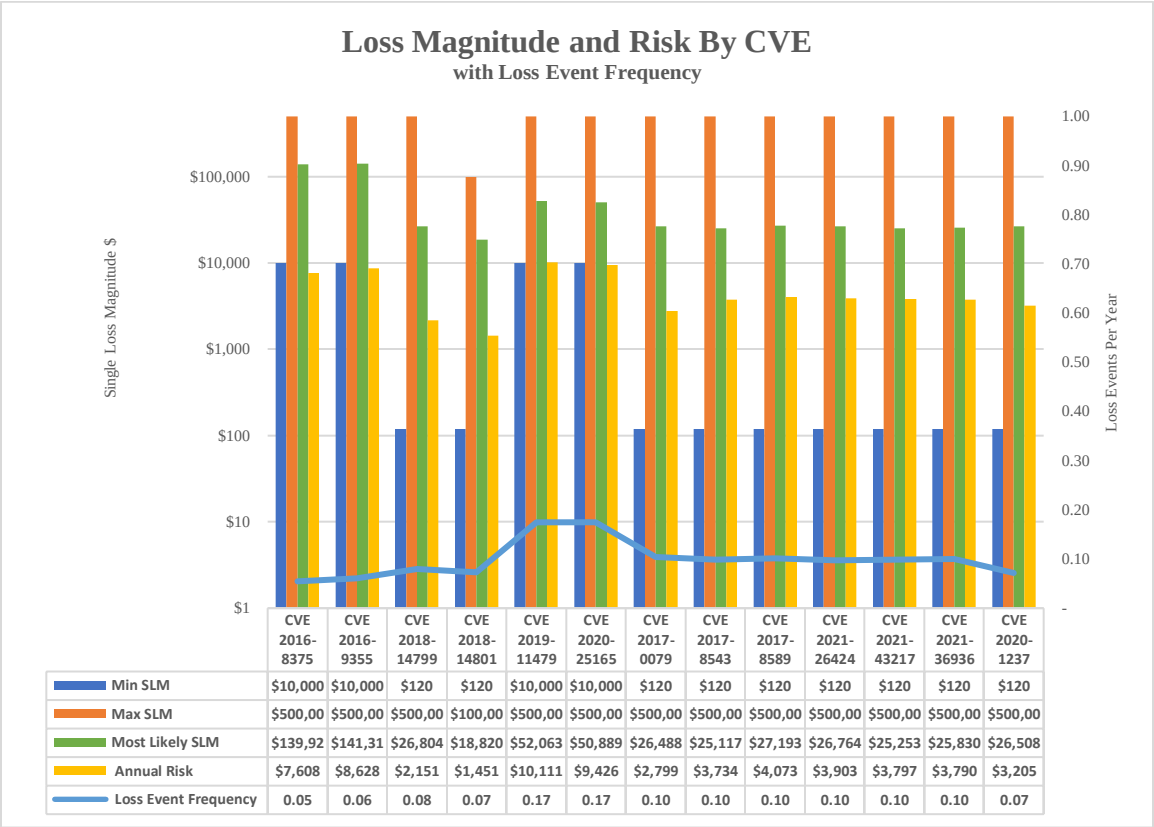


	Abbott i-STAT 1 Blood Gas Analyzer	Alaris 8015 Infusion Pump	Carestream DRX-Revolution Radiography Machine	Phillips PageWriter TC70 ECG	Average of Devices
Min	$13	$330	$92	159	148
Average	$1,034	$8,258	$2,963	3,027	3,820
Max	$3,683	$32,843	$11,864	11,524	14,978

Figure 20. Risk Analysis by Medical Device.

The CVE/asset combination in Table 25 was chosen as an example because it has some risk scenarios that are both infrequent due to low threat activity and have no resistive controls in place. Awareness of this type of scenario is important because, while they may get overlooked in summarization, the cost of an infrequent exposure may drive different prioritization about mitigations. In the FAIR framework, these are referred to as an unstable conditions [97]. Examples of unstable conditions in Table 25 include all three

of the primary effects. In these examples, the frequency is approximately once in 10 years making the annual loss exposure low in comparison to the single loss magnitude.



	CVE 2016-8375	CVE 2016-9355	CVE 2018-14799	CVE 2018-14801	CVE 2019-11479	CVE 2020-25165	CVE 2017-0079	CVE 2017-8543	CVE 2017-8589	CVE 2021-26424	CVE 2021-43217	CVE 2021-36936	CVE 2020-1237
Min SLM	$10,000	$10,000	$120	$120	$10,000	$10,000	$120	$120	$120	$120	$120	$120	$120
Max SLM	$500,00	$500,00	$500,00	$100,00	$500,00	$500,00	$500,00	$500,00	$500,00	$500,00	$500,00	$500,00	$500,00
Most Likely SLM	$139,92	$141,31	$26,804	$18,820	$52,063	$50,889	$26,488	$25,117	$27,193	$26,764	$25,253	$25,830	$26,508
Annual Risk	$7,608	$8,628	$2,151	$1,451	$10,111	$9,426	$2,799	$3,734	$4,073	$3,903	$3,797	$3,790	$3,205
Loss Event Frequency	0.05	0.06	0.08	0.07	0.17	0.17	0.10	0.10	0.10	0.10	0.10	0.10	0.07

Figure 21. Risk Average and Loss Event Frequency by CVE.

In addition to scenarios that represent unstable conditions, there are also scenarios in Table 25 that are expected to occur very infrequently and have only one resistive control in place. For example, the secondary effect scenarios from the malicious insider are reliant on the VLAN for prevention. These are referred to as fragile conditions in FAIR[97] due to them having only one resistive control in place. Understanding the

potential of both unstable and fragile condition scenarios can lead to more informed decisions about preventive controls that may reduce risk to an acceptable level.

Table 25. Sample of Individual Device/CVE Risk Analysis.

CVE Risk Analysis **Target Device: Infusion Pump - 8015 PC Unit with internal flash memory** **CVE 2016-8375**															
CVE Exploitability:	10%														
								Single Loss Magnitude							
	Threat Actor	**Assets**	**CIA Effect**	**Threat Actor Capability (TAC)**	**CVE Vulnerability TAC*(1+Exp)**	**TEF**	**LEF**	**Min**	**Max**	**Most Likely**	**Risk**	**Controls in place**	**Potential Mitigations**	**Notes**
Primary Effect	Malicious Insider	Conf. Bus. Info	Confidentiality	0.50	0.55	0.10	0.06	$ 10,000	$ 100,000	$ 50,000	$2,796		employment screening/ physical security	Cost of resetting credentials for all machines
	Malicious Outsider	Conf. Bus. Info	Confidentiality	0.55	0.61	0.11	0.07	$ 10,000	$ 100,000	$ 50,000	$3,367		physical security	Cost of resetting credentials for all machines
	Trusted or privileged Insider	Conf. Bus. Info	Confidentiality	0.98	1.08	0.10	0.11	$ 10,000	$ 100,000	$ 50,000	$5,352		employment screening/ physical security	Cost of resetting credentials for all machines
`Secondary Effect	Malicious Insider	PII	Confidentiality	0.50	0.55	0.08	0.05	$ 10,000	$ 250,000	$ 50,000	$2,319	VLAN	logging & response/ employment screening	
		PHI	Confidentiality	0.49	0.54	0.08	0.05	$ 10,000	$ 250,000	$ 225,000	$10,305	VLAN	logging & response/ employment screening	This threat agent would be a little less likely to be able to carry out this secondary threat
		Business Revenue	Availability	0.50	0.55	0.08	0.05	$ 100,000	$ 500,000	$ 250,000	$11,561	VLAN	logging & response/ employment screening	

7.7 Conclusions and Future Directions

The framework presented here provides a method for quantifying risk, which to our knowledge is novel in the context of medical devices. We propose that a reduction in the uncertainty about the riskiness of the cybersecurity status of medical devices can be achieved using this framework. The example reports we provide here demonstrate how the results of the risk assessment can be communicated. Communication should include analyzing the results and questioning the inputs with the goal of improving the accuracy of the assessment. Future assessments will benefit from the knowledge learned in previous assessments.

The process of conducting this risk assessment was both tedious and time intensive. So much so that we had to reduce the number of medical devices down to a small fraction of the total dataset to complete the assessment. We conclude that the manual process is impractical for conducting a risk assessment of the full medical device inventory of a healthcare organization. Automating the methodology used in this case study to include an automated data interface of vulnerability information from the National Vulnerability Database should be conducted to make this scalable to the full medical device inventory of a healthcare organization.

Further work to improve the risk assessment is to develop a process to quantify mitigations or resistive controls that can reduce the loss magnitude. This would include a combination of controls and mitigation that are already in place and those that could be implemented to reduce risk. This may be done following the same strategy as has been used here to estimate the risk.

Appendix B – Comparative Analysis provides further analysis of the risk results. Sample analyses that could support risk communication are included. In addition, a comparison or our quantified risk to the qualitative risk score that was provided in the dataset received from our partnering organization is provided and a comparison of our risk to the CVSS score.

7.8 Appendix A

Table 26. Vulnerabilities Published in NVD for Device.

Type	Model Description	Manufacturer	CVE	Summary
Blood Gas Analyzer	i-STAT 1	Abbott	none found	
Digital Radiography	DRX-Revolution	Carestream	2017-0079	local users can gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability" – exemplar of many found
Digital Radiography	DRX-Revolution	Carestream	2017-8543	local users can gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability" – exemplar of many found
Digital Radiography	DRX-Revolution	Carestream	2017-8589	remote code execution vulnerability due to the way that Windows Search handles objects in memory, aka "Windows Search Remote Code Execution Vulnerability– exemplar of many found
Digital Radiography	DRX-Revolution	Carestream	2021-26424	Windows TCP/IP Remote Code Execution Vulnerability – exemplar of many found
Infusion Pump	8015 PC Unit firmware v. 9.33.1.2	Alaris	2016-8375	A unauthorized user with physical access may be able to obtain unencrypted wireless network authentication credentials and other sensitive technical data by disassembling the PC unit and accessing the device's flash memory. version 9.7 and the 8000 store network authentication credential and other sensitive technical data is stored on internal flash memory. Accessing the memory would require special tools and would increase the likelihood of detection.
Infusion Pump	8015 PC Unit firmware v. 9.33.1.2	Alaris	2016-9355	A unauthorized user with physical access may be ble to obtain unencrypted wireless network authentication credentials and other sensitive technlcal data by disassembling the PC unit and accessing the device's flash memory. Versions 9.5 and prior versions store network authentication credential and other sensitive technical data is stored on removable flash memory. Being able to remove the flash memory reduces the risk of detection.

Table 26. cont.

Type	Model Description	Manufacturer	CVE	Summary
Infusion Pump	8015 PC Unit firmware v. 9.33.1.2	Alaris	2019-11479	Jonathan Looney discovered that the Linux kernel default MSS is hard-coded to 48 bytes. This allows a remote peer to fragment TCP resend queues significantly more than if a larger MSS were enforced. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commits 967c05aee439e6e5d7d805e195b3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5cb4654b9fc363.
Infusion Pump	8015 PC Unit firmware v. 9.33.1.2	Alaris	2020-25165	Model 8015, Versions 9.33.1 and earlier are vulnerable to a network session authentication vulnerability within the authentication process between specific versions of the PC unit and the BD Alaris Systems Manager. Attack could result in DoS on PC Unite by modifying configuration headers of data in transit.
Infusion Pump Gateway	Alaris Systems Manager	Alaris	2020-25165	A network session authentication vulnerability within the authentication process between specified versions of the BD Alaris PC Unit and the BD Alaris Systems Manager.an attacker could perform a denial-of-service attack on the BD Alaris PC Unit by modifying the configuration headers of data in transit. A denial-of-service attack could lead to a drop in the wireless capability of the BD Alaris PC Unit, resulting in manual operation of the PC Unit - in versions 4.33 and earlier
ECG	PageWriter TC70	Philips	2018-14799	improper input validation - the PageWriter device does not sanitize data entered by user which can lead to buffer overflow or format string vulnerabilities.
ECG	PageWriter TC70	Philips	2018-14801	hard-coded credentials - attacker with both the superuser password and physical access can enter the superuser password that can be used to access and modify all settings on the device, as well as allow the user to reset existing passwords.
ECG	PageWriter TC70	Philips	2017-0079	local users can gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability" – exemplar of many found

Table 26. cont.

Type	Model Description	Manufacturer	CVE	Summary
ECG	PageWriter TC70	Philips	2017-8543	local users can gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability" – exemplar of many found
ECG	PageWriter TC70	Philips	2017-8589	remote code execution vulnerability due to the way that Windows Search handles objects in memory, aka "Windows Search Remote Code Execution Vulnerability" – exemplar of many found
ECG	PageWriter TC70	Philips	2021-26424	Windows TCP/IP Remote Code Execution Vulnerability – exemplar of many found

Table 27. Threat Agent Library.

Threat Agent	Insider	Outsider	Trusted or Privileged Insider	Established Cybercriminal Organization	Rogue Nation	User (error)	Privileged User/Administrator (error)
Motive	Vindication for personal gain	Personal Gain or ideology	Vindication for personal gain	Financial or PHI	Financial or PHI	unmotivated Error	unmotivated Error
Primary Intent	Gain retribution or to acquire money	Financial gain or to damage organization's reputation	Gain retribution or to acquire money	Data gathering and/or disruption of services	Data gathering and/or disruption of services	goodwill	goodwill
Sponsorship	None. In rare cases, collusion with other bad actors		None. In rare cases, collusion with other bad actors	unknown	Nation State	none	none
Preferred Target	High value targets for retribution; or easy yet hidden financial gains	High value targets for reputation damage; or easy financial gains	High value targets for retribution; or easy yet hidden financial gains	Easy financial gains via remote means	Entities with financial resources or high value assets or IP	Systems they have access to	Systems they have access to
Preferred Targets	Targets to which the attacker already has access	Targets with easy access	Targets to which the attacker already has access	Entities with financial resources or high value assets	Entities with financial resources or high value assets	no preference	no preference
Capability	Skills vary. Likely limited access to systems and limited skills, but some may be more skilled. Usually not well-versed in hacking	Varies widely	Skills vary. Usually well-versed in target systems; could have high computer skills, yet not well-versed in hacking	Well-funded trained and skilled	Highly funded trained and skilled	Low to high depending on the system	Usually high - depends on the system
Personal Risk Tolerance	Varies	Low to medium	Low	Very high	Very high	Low to medium	Low
Concern for Collateral Damage	Varies	Low to medium	Low to medium	Medium	Medium	High	High

7.9 Appendix B - Comparative Analysis

After conducting the risk assessment, we sought methods to compare our results to other available information. We found two measures for comparison. The first is the 'Risk Score' provided in the data we received from our partnering healthcare organization. The second is a comparison to the CVSS score. While the CVSS score is intended to communicate severity and not risk, we think that analyzing how these two things differ may be insightful.

7.9.1 Comparing our Risk To our Partnering Healthcare Organization Risk Score

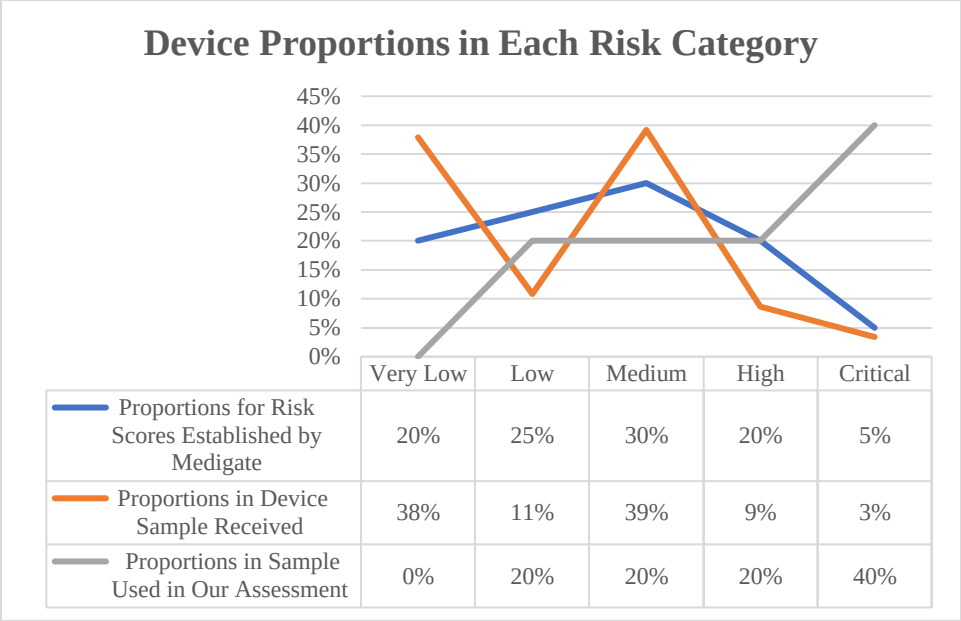
There is a risk score associated with each medical device in the data received from our partnering organization. The source of the risk score is Medigate [236], a cybersecurity platform for medical device inventory and vulnerability and risk management that is used by our partnering facility. According to Medigate documentation [250], the risk score follows industry standards such as NIST SP 800-30 and AAMI TIR57 [251] information security risk management and uses the components of likelihood and severity of impact to arrive at the score. Their factors and considerations are similar to the factors described our framework. Their resulting risk score is reported as one of five risk categories: very low, low, medium, high, and critical. They established ranges for each category to create distribution that facilitates prioritization and action. Medigate's estimated proportion of devices is shown in Table 28. It is noted here that Medigate assigns risk scores to medical devices, and we assign risk to individual risk scenarios.

Table 28. Medigate Risk Score Proportions.

Risk Category	Estimated Proportion of Devices
Very Low	20 %
Low	25 %
Medium	30 %
High	20%
Critical	5%

An analysis was conducted to see how the dataset received from our partnering organization compared with the general proportions in Table 28. We looked at two data references. The first was the entire dataset of 3,520 devices that we received, and the second was the sample of assets we selected from that dataset for our risk assessment. Figure 22 shows our comparison. The general proportions established by Medigate place the largest percentage of devices at medium risk, and our full dataset supports that largest proportion. There is a difference in the percentage of very low and low risk devices. It is noted that the dataset we received was a subset of the organization's full medical device inventory. When we look at the percentages of our sample, we see a pattern that is not consistent with either of the other two proportions. Two of the devices were critical risk devices. However, we did not select for risk score, and the small number of medical devices in our sample is not conducive to a percentage analysis.

Next, we sought to equate our quantified values to the risk scores of the devices in our sample data so that we could make a comparison. We opted for risk ranges in line with the general proportions established by Medigate as show in Table 28. We perform ed a PERT distribution of our risks as shown in Figure 23 for the purpose of establishing ranges for risk.



	Very Low	Low	Medium	High	Critical
Proportions for Risk Scores Established by Medigate	20%	25%	30%	20%	5%
Proportions in Device Sample Received	38%	11%	39%	9%	3%
Proportions in Sample Used in Our Assessment	0%	20%	20%	20%	40%

Figure 22. Comparison of Proportions in Each Risk Category.

From the PERT distribution, we identified the values in each of the proportion ranges established by Medigate. Table 29 shows the ranges for the proportions. We use these ranges to assign the qualitative risk score to each risk scenario.

Once the qualitative risk scores were assigned to each of our risk scenarios according to the ranges in Table 29, we compare them to the risk scores that were assigned to the devices by our partnering organization. Figure 24 shows the comparison in quantities and percentages. There is a wide variance in the two risk scores. One explanation for this is that the risk scores provided in our sample data were associated with the device, while ours are associated with the risk scenario. We can also see that we arrived at a total of seven scenarios that are either high or critical. The conclusion that can be drawn from this analysis is that assessing risk scenarios instead of devices may give us more detailed information upon which to establish risk mitigation priorities.

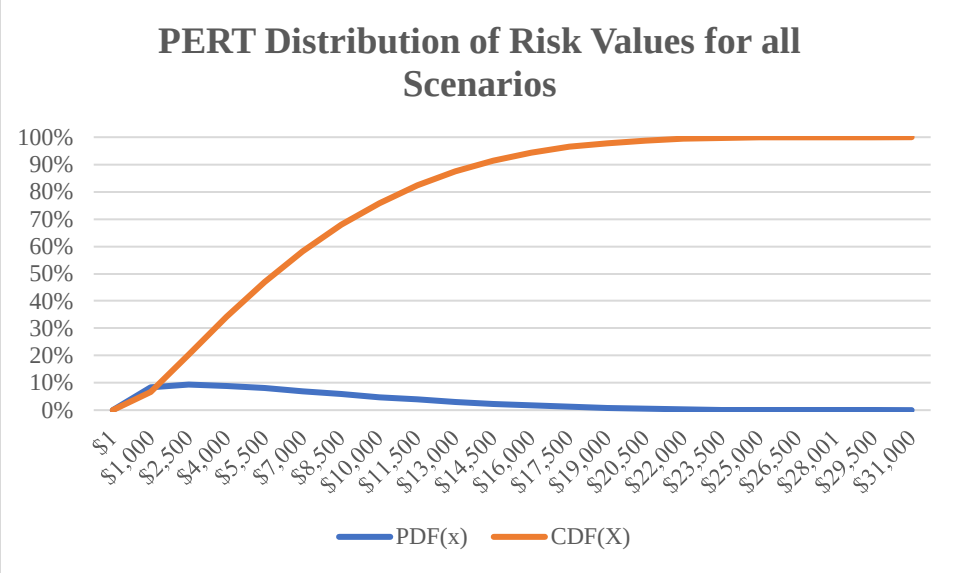
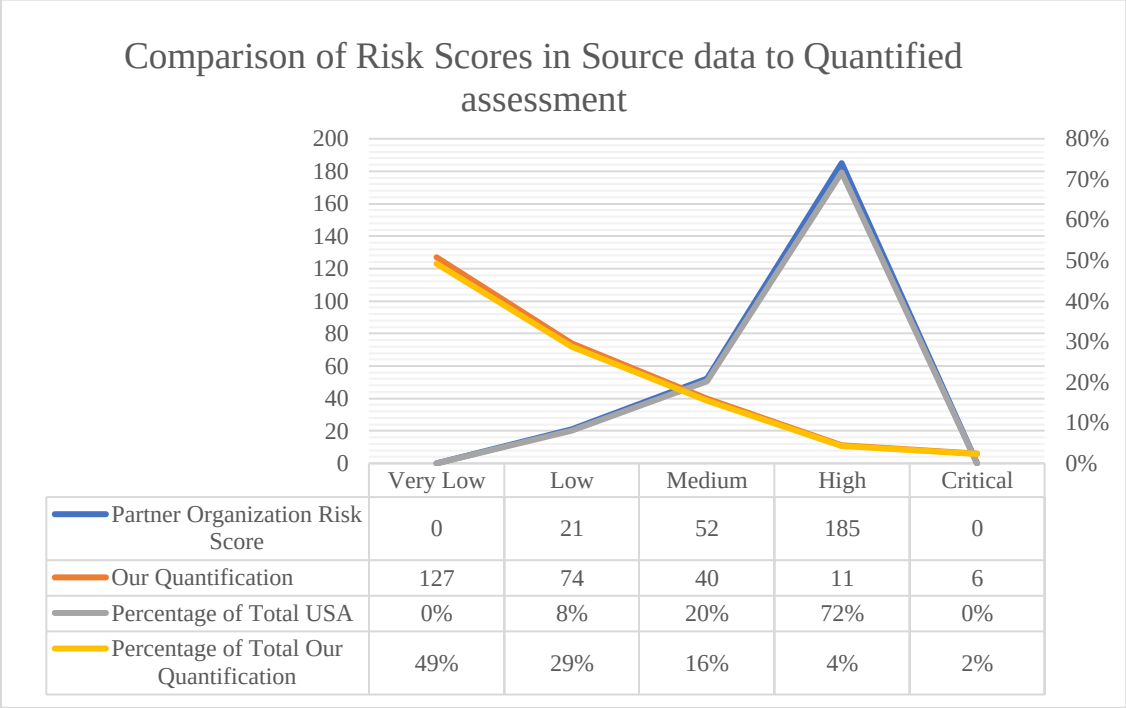


Figure 23. PERT Distribution of all Risk Scenarios.

Table 29. Risk Score Ranges Using Medigate Proportions.

Qualitative Risk Score	**Min**	**Max**	**Percentile**
Very Low	$ 1	$ 2,500	20%
Low	$ 2,501	$ 5,400	25%
Medium	$ 5,401	$ 10,000	30%
High	$ 10,001	$ 18,000	20%
Critical	$ 18,001	$ 32,000	5%

Figure 24. Comparison of Risk Scores to Quantified Assessment.



	Very Low	Low	Medium	High	Critical
Partner Organization Risk Score	0	21	52	185	0
Our Quantification	127	74	40	11	6
Percentage of Total USA	0%	8%	20%	72%	0%
Percentage of Total Our Quantification	49%	29%	16%	4%	2%

7.9.2 Comparing our Risk to CVSS Severity

NVD specifies that CVSS is not a measure of risk. Accordingly, we hypothesize that our risk would not correlate with the CVSS score associated with the CVEs identified in our risk scenarios. To test this hypothesis, we compared the two. The process of comparing our risk scenarios to the CVSS score included developing a methodology for converting our quantified risk to a unit of measure equivalent to CVSS. While the CVSS score is a numeric value ranging from 1 to 9.8, NVD provides qualitative measures for ranges of numeric the CVSS score [252]. **Error! Reference s ource not found.** shows the qualitative ratings and score ranges for each rating.

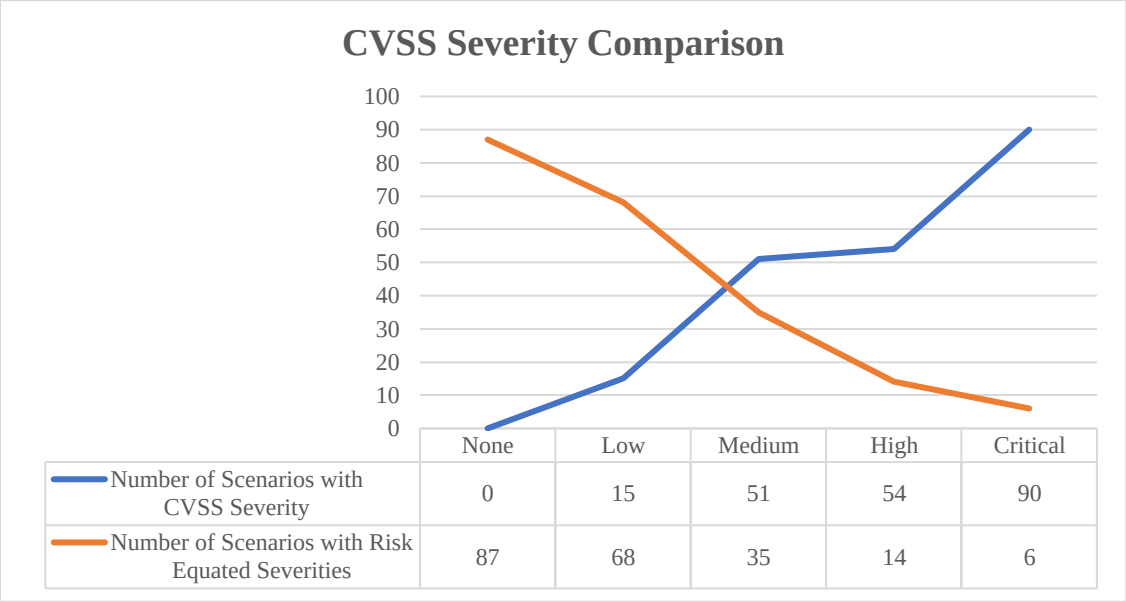
Table 30. CVSS Scores to Qualitative Ratings

CVSS v3.0 Ratings		
	Numeric Base Score	
Qualitative Severity	Min	Max
None	0	0
Low	0.1	3.9
Medium	4	6.9
High	7	8.9
Critical	9	10

To compare our quantified risk to CVSS we opted to convert our quantified risk to the qualitative ratings established by NVD. To do this, we relied upon the qualitative ratings we developed for each scenario when comparing risk to our partnering organization's risk score. The qualitative ratings provided by Medigate for that analysis are very similar to the CVSS qualitative ratings, with the only difference being in the lowest risk category. Where Medigate uses 'Very Low', NVD uses 'None'. We used the qualitative ratings we established in the comparison of our risk to our partner's risk score, shown in Table 29, except for changing the 'Very Low' measure to 'None' in order to match the values established by NVD.

In addition to equating our quantified risk to qualitative ratings, for this comparison we also excluded the risk scenarios that did not have an associated CVE. In total, 48 risk scenarios did not have an associated CVE and were removed from the 258 total risk scenarios, resulting in 210 risk scenarios that had an associated CVE.

Figure 25 shows the comparison between the CVSS score and our quantified risk using the qualitative ratings we describe above. The graphs shows that our risk and the CVSS from associated CVEs are not congruent. A detailed analysis showed that while there were some scenarios where the scores equated, in most there is not parity. This analysis supports the hypothesis that our quantified risk does not match the CVSS and confirms that CVSS is not a measure of risk in our risk scenarios.



	None	Low	Medium	High	Critical
Number of Scenarios with CVSS Severity	0	15	51	54	90
Number of Scenarios with Risk Equated Severities	87	68	35	14	6

Figure 25. Comparison or Risk to CVSS Score.

CHAPTER VIII

FUTURE DIRECTIONS AND MAJOR CONTRIBUTIONS

8.1 Future Directions

Future directions in this research can include automating the risk assessment. Automating the framework would expand opportunities to apply it to a larger number of medical devices. Another future direction could be applying the risk framework in domains other than medical devices. Suitable domains would be those in which risk is consequential and there is a lack of historical data on which to base risk. Each of these directions is described here.

8.1.2 Automating the Risk Assessment Process

In Chapter VII, the risk assessment framework was applied using a subset of medical device data received from a partnering healthcare organization. The process of manually applying the framework was so time intensive as to make it impractical to apply to the full inventory of medical device inventory. This is a barrier to its broad application in a real-world setting. Automating the process would remove this barrier and provide the possibility of using the framework to reduce the uncertainty of the risk posed by networked medical devices in a healthcare organization. Some work has been done to design the database schema necessary to accomplish this. Future research could

operationalize this through a database driven application to reduce the manual labor involved.

8.1.3 Applying the Risk Assessment in other Domains

The framework proposed in this research could be adopted in domains other than healthcare medical devices. Other domains with computerized devices on trusted networks could benefit from cybersecurity risk assessment. Examples that may be considered include manufacturing facilities and industrial control systems. The sources of vulnerability information would have to be explored to determine if there are domain-specific sources of information that may not be included in the current framework.

8.2 Major Contributions

This dissertation made several contributions that may help reduce uncertainty about the risk posed by networked medical devices. First, we identified factors that influence the cybersecurity risk assessment of medical devices, and we demonstrated that it is possible to identify through open-source investigation threats and vulnerabilities that present risks in networked medical devices.

Second, a framework was developed that provides a method for identifying and quantifying risk, which to our knowledge is novel in the context of medical devices. The framework uses industry standards for identifying risks and expert elicitation for predicting the impact that may be experienced by the organization. The process of calibrating experts to be better at prediction is well established in the literature, and when used to prepare experts, improves the accuracy of their predictions. We propose that a reduction in uncertainty about the riskiness of the cybersecurity status of medical devices

can be achieved using this framework. Furthermore, we propose that presenting risk in monetary units is an improvement over using qualitative scales to measure risk. Monetary units can be superior to qualitative measures in the communicating risk by providing more consistency in the perception of risk, and risk can then be compared objectively to the organizations risk appetite.

Finally, this dissertation presented risk reporting that demonstrates how quantified risk may be communicated to operational and managerial levels of an organization. The prioritization of vulnerabilities and risk scenarios can provide the operational level with a tool to prioritize limited resources toward most effectively reducing risk. At the managerial level, reporting risk can provide insights into risk that can lead to effective investment in resistive controls and other mitigations.

APPENDIX

Copyright Permissions

Paper One was published in the AMCIS 2016 Proceedings [253]. The copyright agreement reserves the author's right to use, free of charge, all or part of the published material in future works of their own. In addition, the author maintains the right to use the material in subsequent compilations of their own.

Paper Two was published in the Proceeding of the 18th International Conference on Cyber Warfare and Security [254]. These conference proceedings are open access, meaning that the information may be used by any persons without requiring permission of the publisher or the author.

REFERENCES

[1] "The Cost of Malicious Cyber Activity to the U.S. Economy," The Council of Economic Advisers - Executive Office of the President of the United States, Feb. 2018. [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

[2] M. Reel and J. Robertson, "It's Way Too Easy to Hack the Hospital," *Bloomberg.com*, Nov. 2015. http://www.bloomberg.com/features/2015-hospital-hack/ (accessed Apr. 17, 2016).

[3] J. Finkle, "U.S. government probes medical devices for possible cyber flaws | Reuters," *reuters.com/Technology*, Oct. 22, 2014. http://www.reuters.com/article/2014/10/22/us-cybersecurity-medicaldevices-insight-idUSKCN0IB0DQ20141022 (accessed Oct. 08, 2015).

[4] "HITECH Act Enforcement Interim Final Rule," *U. S. Department of Health & Human Services*. http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html (accessed Oct. 29, 2015).

[5] "Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions," Federal Bureau of Investigation, FBI Cyber Division Bulletin, May 2014. Accessed:

Sep. 20, 2015. [Online]. Available: https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf

[6] "Criminal Attacks Are Now Leading Cause of Data Breach in Healthcare, According to New Ponemon Study - News and Press Releases," May 07, 2015. http://www.ponemon.org/news-2/66 (accessed Oct. 08, 2015).

[7] "Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data," Ponemon Institute LLC, Research Report, May 2016.

[8] B. Mastroianni, "Dangerous escalation in ransomware attacks," Feb. 19, 2016. https://www.cbsnews.com/news/ransomware-hollywood-presbyterian-hospital-hacked-for-ransom/ (accessed Feb. 23, 2016).

[9] KPMG, LLP, "Health Care and Cyber Security: Increasing Threats Require Increased Capabilities," KPMG, LLP, Research Report, 2015. Accessed: Mar. 03, 2018. [Online]. Available: https://advisory.kpmg.us/content/dam/kpmg-advisory/PDFs/ManagementConsulting/2015/KPMG-2015-Cyber-Healthcare-Survey.pdf

[10] *HIPAA Administrative Simplification*. 2013. Accessed: Nov. 21, 2015. [Online]. Available: http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/

[11] "Health IT Legislation | Policy Researchers & Implementers | HealthIT.gov," *HealthIT.gov*. https://www.healthit.gov/policy-researchers-implementers/health-it-legislation (accessed Oct. 19, 2015).

[12] "General Data Protection Regulation (GDPR) Compliance Guidelines," *GDPR.eu*. https://gdpr.eu/ (accessed Mar. 06, 2023).

[13] "National Health Expenditure Data," *Centers for Medicare & Medicaid Services*, Jan. 08, 2018. https://www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/NationalHealthExpendData/NationalHealthAccountsHistorical.html (accessed Mar. 03, 2018).

[14] "Fast Facts on U.S. Hospitals, 2018 | AHA." Feb. 2018. Accessed: Jun. 20, 2019. [Online]. Available: https://www.aha.org/statistics/fast-facts-us-hospitals

[15] "Health IT Quick Stats," *The Office of the National Coordinator for Health Information Technology*. https://dashboard.healthit.gov/quickstats/quickstats.php (accessed Mar. 03, 2018).

[16] U. S. Food and Drug Administration, "Safety Alerts for Human Medical Products - Symbiq Infusion System by Hospira: FDA Safety Communication - Cybersecurity Vulnerabilities." https://www.fda.gov/safety/medwatch/safetyinformation/safetyalertsforhumanmedicalproducts/ucm456832.htm (accessed Nov. 29, 2017).

[17] Center for Devices and Radiological Health, "Products and Medical Procedures - Cybersecurity," Feb. 07, 2018. https://www.fda.gov/medicaldevices/productsandmedicalprocedures/ucm373213.htm (accessed Mar. 03, 2018).

[18] "Hospira LifeCare PCA Infusion System Vulnerabilities (Update B) | ICS-CERT," *Department of Homeland Security ICS-CERT*, Jun. 10, 2015. https://ics-cert.us-cert.gov/advisories/ICSA-15-125-01B (accessed Jul. 22, 2018).

[19] TrapX Labs, “MEDJACK (Medical Device Hijack),” TrapX Security, Inc., May 2015.

[20] U. S. Food and Drug Administration, “Historical Case Studies of Product Regulation - Medical Device & Radiological Health Regulations Come of Age,” *U. S. Food and Drug Administration*. https://www.fda.gov/about-fda/history-fdas-fight-consumer-protection-and-public-health (accessed Mar. 03, 2018).

[21] P. Rogers, *H.R.11124 - 94th Congress (1975-1976): Medical Device Amendments*. 1976. Accessed: Mar. 03, 2018. [Online]. Available: https://www.congress.gov/bill/94th-congress/house-bill/11124

[22] H. Waxman, *H.R.3095 - 101st Congress (1989-1990): Safe Medical Devices Act of 1990*. 1990. Accessed: Jul. 07, 2017. [Online]. Available: https://www.congress.gov/bill/101st-congress/house-bill/3095

[23] “EU General Protection Regulation (GDPR) – Information Portal.” https://eugdpr.org/ (accessed Oct. 03, 2018).

[24] “The Joint Commission,” 2015. http://www.jointcommission.org/ (accessed Nov. 20, 2015).

[25] “NIST | National Institute of Standards and Technology,” *NIST*. https://www.nist.gov (accessed Mar. 04, 2018).

[26] “ISO - International Organization for Standardization,” *ISO*. http://www.iso.org/ (accessed Jul. 22, 2019).

[27] “HITRUST Alliance,” *HITRUST*. https://hitrustalliance.net/ (accessed Sep. 19, 2019).

[28] “Center for Internet Security (CIS),” *CIS*. https://www.cisecurity.org/ (accessed May 22, 2020).

[29] “ISACA.” http://www.isaca.org/ (accessed Jun. 26, 2018).

[30] “NEMA,” *National Electrical Manufacturers Association (NEMA)*. https://www.nema.org/ (accessed Mar. 04, 2022).

[31] “CAPEC - Common Attack Pattern Enumeration and Classification (CAPEC),” *The MITRE Corporation*. https://capec.mitre.org/ (accessed Mar. 04, 2018).

[32] “The MITRE Corporation,” *The MITRE Corporation*, 2015. http://www.mitre.org/ (accessed Nov. 28, 2015).

[33] NIST- NVD, “National Vulnerability Database,” *government*. https://nvd.nist.gov/ (accessed Nov. 20, 2017).

[34] “OVAL - Open Vulnerability and Assessment Language,” *Center for Internet Security*. https://oval.cisecurity.org/ (accessed Mar. 04, 2018).

[35] NIST - SCAP, “Security Content Automation Protocol | CSRC,” *NIST*. https://csrc.nist.gov/projects/security-content-automation-protocol/ (accessed Mar. 04, 2018).

[36] NIST - CPE, “Common Platform Enumeration,” *National Institute of Standards and Technology (NIST)*. https://csrc.nist.gov/Projects/Security-Content-Automation-Protocol/Specifications/cpe (accessed Mar. 04, 2018).

[37] “MITA Releases National Standard for Medical Device Security,” *Medical Imaging & Technology Alliance (MITA)*, Oct. 09, 2019. https://www.medicalimaging.org/mita-news/view/mita-releases-national-standard-for-medical-device-security (accessed Mar. 04, 2022).

[38] “ANSI/NEMA HN 1-2019 - American National Standard— Manufacturer Disclosure Statement for Medical Device Security.” National Electrical Manufacturers Association (NEMA), 2019.

[39] “MITA,” *Medical Imaging & Technoloyg Alliance (MITA)*. https://www.medicalimaging.org (accessed Mar. 04, 2022).

[40] K. A. Seale, “Integrating Relational Data Frameworks into Risk Assessment of Networked Medical Devices,” University of South Alabama, Mobile, AL, 2017. Accessed: Oct. 09, 2017. [Online]. Available: https://search.proquest.com/openview/ca5b92590543e88ce0cf2c92986e3269/1?pq-origsite=gscholar&cbl=18750&diss=y

[41] J. H. Pardue, S. Purawat, and J. P. Landry, “A Database-driven Model for Risk Assessment,” in *Twentieth Americas Conference on Information Systems*, Savannah, GA, 2014.

[42] J. Cerkovnik, “Managing Vulnerabilities and Risk in Networked Medical Devices,” Graduate, University of South Alabama, Mobile, AL, 2015.

[43] B. Hodges, “Attack Modeling and Mitigation Strategies for Risk Based Analysis of Networked Medical Devices,” Master’s Thesis, University of South Alabama, Mobile, AL.

[44] F. O. of the Commissioner, “Federal Food, Drug, and Cosmetic Act (FD&C Act),” *FDA*, Nov. 03, 2018. http://www.fda.gov/regulatory-information/laws-enforced-fda/federal-food-drug-and-cosmetic-act-fdc-act (accessed Jun. 24, 2019).

[45] O. of the Commissioner, “21st Century Cures Act,” *FDA*, Feb. 08, 2019. http://www.fda.gov/regulatory-information/selected-amendments-fdc-act/21st-century-cures-act (accessed Jun. 24, 2019).

[46] Center for Devices and Radiological Health, “Changes to Existing Medical Software Policies Resulting from Section 3060 of the 21st Century Cures Act,” *U.S. Food and Drug Administration*, May 14, 2019. http://www.fda.gov/regulatory-information/search-fda-guidance-documents/changes-existing-medical-software-policies-resulting-section-3060-21st-century-cures-act (accessed Jun. 24, 2019).

[47] Center for Devices and Radiological Health, “Overview of Medical Device Regulation - Code of Federal Regulations (CFR),” *U. S. Food and Drug Administration*, Oct. 31, 2014. https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ucm134499.htm (accessed Jul. 06, 2017).

[48] FDA, “Overview of Medical Device Classification and Reclassification,” *US Food Drug Adm.*, Nov. 2018, Accessed: Jun. 24, 2019. [Online]. Available: http://www.fda.gov/about-fda/cdrh-transparency/overview-medical-device-classification-and-reclassification

[49] “Cisco Medical NAC, Identifying, Classifying, and Segmenting Clinical Healthcare Devices.” Cisco, May 2016. Accessed: Sep. 23, 2018. [Online]. Available: https://www.cisco.com/c/dam/en/us/products/collateral/security/medical-nac-white-paper.pdf

[50] “Common Vulnerability Scoring System v3.0.” Forum of Incident Response and Security Teams (FIRST), Jun. 10, 2015. Accessed: Mar. 20, 2016. [Online]. Available: https://www.first.org/cvss

[51] “Press Announcements - FDA outlines cybersecurity recommendations for medical device manufacturers,” Jan. 15, 2016. http://www.fda.gov/newsevents/newsroom/pressannouncements/ucm481968.htm (accessed Apr. 24, 2016).

[52] “CVSS v3.0 Specification Document.” Accessed: Jul. 03, 2018. [Online]. Available: https://www.first.org/cvss/v3.0/specification-document

[53] “U. S. Department of Homeland Security,” *Department of Homeland Security*. https://www.dhs.gov/ (accessed Jun. 24, 2019).

[54] “The Cybersecurity and Infrastructure Security Agency (CISA).” https://www.us-cert.gov/about-us (accessed Oct. 18, 2015).

[55] “Attorney General Sessions Announces New Cybersecurity Task Force.” U. S. Department of Justice, Feb. 20, 2018. Accessed: Jul. 18, 2018. [Online]. Available: https://www.justice.gov/opa/press-release/file/1035457/download

[56] “Report of the Attorney General’s Cyber Digital Task Force,” U. S. Department of Justice, Washington, DC, Jul. 2018.

[57] “FBI Mission & Priorities,” *Federal Bureau of Investigation*. https://www.fbi.gov/about/mission (accessed Jul. 25, 2018).

[58] R. Ross, “Guide for Conducting Risk Assessments - Special Publication (NIST SP) - 800-30 Rev 1,” National Institute of Standards and Technology, Gaithersburg,

MD, NIST Special Publication 800–30 Rev 1, Sep. 2012. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

[59] NIST - CF, “Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.” National Institute of Standards and Technology, Apr. 16, 2018. Accessed: Jun. 25, 2019. [Online]. Available: http://www.nist.gov/cyberframework/framework

[60] “ISO/IEC 27000:2018 - Information technology -- Security techniques -- Information security management systems,” *International Organization for Standardization (ISO)*. http://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/39/73906.html (accessed Jul. 22, 2019).

[61] T. A. Allen, “NIST Information Technology Laboratory,” *NIST*, Apr. 28, 2015. https://www.nist.gov/itl (accessed Jul. 21, 2019).

[62] *The Cybersecurity Enhancement Act of 2014 (S.1353 - 113th Congress)*, vol. 113th Congress. 2014. Accessed: Jul. 22, 2019. [Online]. Available: https://www.congress.gov/bill/113th-congress/senate-bill/1353/text

[63] “ANSI-American National Standards Institute.” https://www.ansi.org/ (accessed Mar. 19, 2020).

[64] “NIAP: National Informaiton Assurance Partnership.” https://www.niap-ccevs.org/index.cfm (accessed Jul. 16, 2019).

[65] “Common Criteria.” https://www.commoncriteriaportal.org/ (accessed Jul. 17, 2019).

[66] HITRUST Alliance, “HITRUST CSF, Version 9.2.” HITRUST Alliance, Jan. 2019. [Online]. Available: https://hitrustalliance.net/csf-rmf-related-documents/

[67] CIS, “CIS Critical Security Controls v7.1.” Center for Internet Security, Apr. 2019. [Online]. Available: https://www.cisecurity.org/controls/

[68] “CIS RAM Version 1.0 Center for Internet Security® Risk Assessment Method.” Center for Internet Security, Apr. 2018.

[69] “COBIT 5: A Business Framework for the Governance and Management of Enterprise IT.” http://www.isaca.org/cobit/pages/default.aspx (accessed Jun. 26, 2018).

[70] “Risk IT Resources,” *ISACA*. https://www.isaca.org/resources/it-risk (accessed Aug. 30, 2020).

[71] HIMSS, “2018 HIMSS Cybersecurity Survey,” HIMSS North America, Chicago, IL, 2018.

[72] Joint Task Force, “Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,” National Institute of Standards and Technology, NIST Special Publication 800–37 Rev. 2, Oct. 2018. Accessed: Nov. 04, 2018. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

[73] “Privacy Act of 1974,” Jun. 16, 2014. https://www.justice.gov/opcl/privacy-act-1974 (accessed Nov. 07, 2018).

[74] T. Carper, *S.2521 - 113th Congress (2013-2014): Federal Information Security Modernization Act of 2014 (FISMA)*. 2014. Accessed: Nov. 07, 2018. [Online]. Available: https://www.congress.gov/bill/113th-congress/senate-bill/2521

[75] "Office of Management and Budget (OMB)," *The White House*. https://www.whitehouse.gov/omb/ (accessed Nov. 07, 2018).

[76] NIST, "Federal Information Processing Standards Publications (FIPS PUBS)," Feb. 24, 2010. https://www.nist.gov/itl/publications-0/federal-information-processing-standards-fips (accessed Mar. 08, 2023).

[77] "FIPS PUB 199 Standards for Security Categorization of Federal Information and Information Systems." National Institute of Standards and Technology, Feb. 2004. [Online]. Available: https://csrc.nist.gov/csrc/media/publications/fips/199/final/documents/fips-pub-199-final.pdf

[78] Joint Task Force, "Security and Privacy Controls for Information Systems and Organizations," National Institute of Standards and Technology, NIST Special Publication 800–53, Aug. 2017.

[79] Joint Task Force, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans," National Institute of Standards and Technology, NIST Special Publication 800-53Ar4, Dec. 2014. doi: 10.6028/NIST.SP.800-53Ar4.

[80] National Institute of Standards and Technology, "Standards for security categorization of federal information and information systems," National Institute of Standards and Technology, Gaithersburg, MD, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION NIST FIPS 199, Feb. 2004. doi: 10.6028/NIST.FIPS.199.

[81] Joint Task Force Transformation Initiative, “Managing Information Security Risk : Organization, Mission, and Information System View,” National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication 800–39, 2011. doi: 10.6028/NIST.SP.800-39.

[82] J. M. Boyens, C. Paulsen, R. Moorthy, and N. Bartol, “Supply Chain Risk Management Practices for Federal Information Systems and Organizations,” National Institute of Standards and Technology, NIST Special Publication 800–161, Apr. 2015. doi: 10.6028/NIST.SP.800-161.

[83] *H.R.3162 - 107th Congress (2001-2002): Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001*. 2001. Accessed: Jun. 26, 2019. [Online]. Available: https://www.congress.gov/bill/107th-congress/house-bill/3162

[84] “Critical Infrastructure Sectors | Homeland Security,” *Department of Homeland Security (DHS)*, Oct. 27, 2015. http://www.dhs.gov/critical-infrastructure-sectors (accessed Dec. 02, 2015).

[85] “An Overview of ISO/IEC 27000 family of Information Security Management System Standards.” Innovation and Technology Commission of the Government of the Hong Kong, Nov. 2017. [Online]. Available: www.infocloud.gov.hk

[86] “NIST Special Publication 800 Series,” *National Institute of Standards and Technology (NIST)*. https://csrc.nist.gov/publications/sp800 (accessed Sep. 20, 2019).

[87] 14:00-17:00, “ISO 27799:2008,” *ISO*. http://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/04/12/41298.html (accessed Sep. 20, 2019).

[88] “Privacy and Security Standards - Centers for Medicare & Medicaid Services (CMS),” *HHS, CMS*, Apr. 02, 2013. https://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/PrivacyandSecurityStandards.html (accessed Nov. 26, 2015).

[89] “PCI Security Standards Council.” https://www.pcisecuritystandards.org/ (accessed Sep. 20, 2019).

[90] I. T. L. Computer Security Division, “NIST 800-53 Overlay Overview - Risk Management | CSRC,” *CSRC | NIST*, Nov. 30, 2016. https://csrc.nist.gov/Projects/Risk-Management/scor/Overlay-Overview (accessed Sep. 24, 2019).

[91] “HALOCK,” *HALOCK*. https://www.halock.com/ (accessed Aug. 30, 2020).

[92] 14:00-17:00, “ISO/IEC 27005:2018,” *ISO*. https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/52/75281.html (accessed Aug. 29, 2020).

[93] G. Stoneburner, A. Goguen, and A. Feringa, “Risk Management Guide for Information Technology Systems,” National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication SP 800-30, Jul. 2002. Accessed: Jun. 14, 2018. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-30/archive/2002-07-01

[94] "DoCRA – Duty of Care Risk Analysis Standard." https://www.docra.org/ (accessed Aug. 30, 2020).

[95] R. S. Kaplan and D. P. Norton, *The Balanced Scorecard: Translating Strategy into Action*. Harvard Business Review Press, 1996. [Online]. Available: https://books.google.com/books?id=0tjRLqFH830C

[96] "Conducting an IT Security Risk Assessment." ISACA, 2020.

[97] J. Freund and J. Jones, *Measuring and managing information risk: a FAIR approach*. Butterworth-Heinemann, 2014.

[98] T. R. Peltier, *Information Security Risk Analysis, 3rd*, Third Edition. New York, NY, USA: Auerbach Publications, 2010.

[99] D. Landoll, *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments*, 2nd ed. Boca Raton, FL, USA: CRC Press, Inc., 2011.

[100] S. Kaplan and B. J. Garrick, "On The Quantitative Definition of Risk," *Risk Anal.*, vol. 1, no. 1, pp. 11–27, 1981, doi: 10.1111/j.1539-6924.1981.tb01350.x.

[101] "Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants." U. S. Nuclear Regulatory Commission, Oct. 1975.

[102] B. J. Garrick and S. Kaplan, *Cost-benefit estimate of transporting spent nuclear fuel by special trains*. United States: American Nuclear Society, Inc, 1978. [Online]. Available: http://inis.iaea.org/search/search.aspx?orig_q=RN:10487871

[103] "The Actuary's Role in Risk Management." The Society of Actuaries, Oct. 17, 1999. Accessed: Mar. 07, 2018. [Online]. Available:

https://www.soa.org/library/proceedings/record-of-the-society-of-actuaries/1990-99/1999/january/rsa99v25n3126pd.pdf

[104] "Overview of Enterprise Risk Management." Casualty Actuarial Society, May 2003.

[105] W. Meyer, "Quantifying risk," presented at the PMI Global Congress 2015 - EMEA, London, England, Oct. 2015. Accessed: Nov. 15, 2018. [Online]. Available: https://www.pmi.org/learning/library/quantitative-risk-assessment-methods-9929

[106] C. Starr, "Social benefit versus technological risk," *Read. Environ. Impact*, vol. 165, p. 78, 1974.

[107] L. Anthony (Tony) Cox Jr, "What's Wrong with Risk Matrices?," *Risk Anal.*, vol. 28, no. 2, pp. 497–512, 2008, doi: https://doi.org/10.1111/j.1539-6924.2008.01030.x.

[108] D. W. Hubbard and R. Seiersen, *How to Measure Anything in Cybersecurity Risk*. Hoboken, NJ: John Wiley & Sons, Inc., 2016.

[109] C. E. Shannon, "A mathematical theory of communication," *Bell Syst Tech J*, vol. 27, pp. 379–423, 1948.

[110] Rev. T. Bayes, "An essay toward solving a problem in the doctrine of chances," *Phil Trans Roy Soc Lond*, vol. 53, pp. 370–418, 1764, doi: 10.1098/rstl.1763.0053.

[111] M. Beynon, B. Curry, and P. Morgan, "The Dempster–Shafer theory of evidence: an alternative approach to multicriteria decision modelling," *Omega*, vol. 28, no. 1, pp. 37–50, 2000.

[112] A. P. Dempster, “Upper and lower probabilities induced by a multivalued mapping,” in *Classic works of the Dempster-Shafer theory of belief functions*, Springer, 2008, pp. 57–72.

[113] L. A. Wasserman, “Belief functions and statistical inference,” *Can. J. Stat.*, vol. 18, no. 3, pp. 183–196, 1990.

[114] T. Denœux, “40 years of Dempster–Shafer theory,” *Int. J. Approx. Reason.*, vol. 79, pp. 1–6, 2016, doi: https://doi.org/10.1016/j.ijar.2016.07.010.

[115] H. T. Nguyen, “On random sets and belief functions,” in *Classic Works of the Dempster-Shafer Theory of Belief Functions*, Springer, 2008, pp. 105–116.

[116] T. L. Saaty, “How to make a decision: the analytic hierarchy process,” *Eur. J. Oper. Res.*, vol. 48, no. 1, pp. 9–26, 1990.

[117] J. Mun, *Modeling risk: Applying Monte Carlo simulation, real options analysis, forecasting, and optimization techniques*, vol. 347. John Wiley & Sons, 2006.

[118] H. Gould, J. Tobochnik, and W. Christian, *An introduction to computer simulation methods*, vol. 1. Addison-Wesley New York, 1988.

[119] P. E. Meehl, *Clinical versus statistical prediction: A theoretical analysis and a review of the evidence*. University of Minnesota Press, 1954. Accessed: Jun. 02, 2020. [Online]. Available: https://doi.org/10.1037/11281-000

[120] W. M. Grove, D. H. Zald, B. S. Lebow, B. E. Snitz, and C. Nelson, “Clinical versus mechanical prediction: A meta-analysis,” *Psychol. Assess.*, vol. 12, no. 1, pp. 19–30, Mar. 2000, doi: 10.1037/1040-3590.12.1.19.

[121] Orley Ashenfelter, “Predicting the Quality and Prices of Bordeaux Wine,” *Econ. J.*, vol. 118, no. 529, pp. F174–F184, Jun. 2008, doi: https://doi.org/10.1111/j.1468-0297.2008.02148.x.

[122] C. W. J. Granger and O. Morgenstern, *Predictability of stock market prices*. Heath Lexington Books, 1970.

[123] R. M. Dawes, D. Faust, and P. E. Meehl, “Clinical Versus Actuarial Judgment,” *Science*, vol. 243, pp. 1668–1674, Mar. 1989.

[124] D. Kahneman and A. Tversky, “On the psychology of prediction,” *Psychol. Rev.*, vol. 80, no. 4, p. 237, 1973.

[125] D. KAHNEMAN and G. KLEIN, “Conditions for Intuitive Expertise: A Failure to Disagree,” *Am. Psychol.*, vol. 64, no. 6, pp. 515–526, 2009.

[126] A. D. De Groot and A. de Groot, “Thought and choice in chess (Vol. 4),” *Mouton Gruyter*, 1978.

[127] G. A. Klein, J. Orasanu, R. Calderwood, and C. E. Zsambok, Eds., “Decision making in action: Models and methods.,” *Decis. Mak. Action Models Methods*, pp. xi, 480–xi, 480, 1993.

[128] B. Crandall and K. Getchell-Reiter, “Critical decision method: a technique for eliciting concrete assessment indicators from the intuition of NICU nurses.,” *Adv. Nurs. Sci.*, 1993.

[129] W. Fogarty, “Formal investigation into the circumstances surrounding the downing of a commercial airliner by the USS Vincennes,” *Memo. Command. Chief*, 1988.

[130] S. C. Collyer and G. S. Malecki, “Tactical decision making under stress: History and overview.,” 1998.

[131] A. Tversky and D. Kahneman, “Belief in the law of small numbers.,” *Psychol. Bull.*, vol. 76, no. 2, p. 105, 1971.

[132] S. Lichtenstein, B. Fischhoff, and L. D. Phillips, “Calibration of probabilities: The state of the art to 1980,” DECISION RESEARCH EUGENE OR, 1981.

[133] S. Lichtenstein and B. Fischhoff, “Training for calibration,” *Organ. Behav. Hum. Perform.*, vol. 26, no. 2, pp. 149–171, 1980.

[134] J. E. Sieber, “Effects of decision importance on ability to generate warranted subjective uncertainty.,” *J. Pers. Soc. Psychol.*, vol. 30, no. 5, p. 688, 1974.

[135] A. Koriat, S. Lichtenstein, and B. Fischhoff, “Reasons for confidence.,” *J. Exp. Psychol. [Hum. Learn.]*, vol. 6, no. 2, p. 107, 1980.

[136] G. Wright and A. Wisudha, “Differences in calibration for past and future events,” in *Seventh Research Conference on Subjective Probability, Utility and Decision Making, Goteborg, Sweden*, 1979.

[137] M. G. International, “Casualty Actuarial Society.” https://www.casact.org/ (accessed Jul. 28, 2020).

[138] “Committee of Sponsoring Organizations of the Treadway Commisson (COSO).” https://www.coso.org/Pages/default.aspx (accessed May 28, 2020).

[139] “COSO Enterprise Risk Management — Integrated Framework.” Committee of Sponsoring Organizations of the Treadway Commission, 2004. Accessed: Aug. 28, 2020. [Online]. Available: https://www.coso.org/Pages/erm-integratedframework.aspx

[140] "Enterprise Risk Management — Integrated Framework; Executive Summary." Committee of Sponsoring Organizations of the Treadway Commission, Sep. 2004. [Online]. Available: https://www.coso.org/Documents/COSO-ERM-Executive-Summary.pdf

[141] Deloitte, "Managing Cyber Risk in the Digital Age." The Committee of Sponsoring Organizations of the Treadway Commission (COSO), Nov. 2019.

[142] "System and Organization Controls (SOC) for Cybersecurity," *AICPA*. https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpacybersecurityinitiative.html (accessed Jul. 28, 2020).

[143] "ASHRM: Homepage | ASHRM." https://www.ashrm.org/ (accessed Jul. 28, 2020).

[144] "ASHRM Enterprise Risk Management (ERM) Resources." https://www.ashrm.org/resources/erm-resources (accessed Jul. 28, 2020).

[145] "Understanding risk assessment practices at manufacturing companies," Deloitte & Touche LLP, Mar. 2015.

[146] L. J. Hoffman, E. H. Michelman, and D. P. Clements, "SECURATE: a security evaluation and analysis system using fuzzy metrics," in *AFIPS National Computer Conference Proceedings 47*, Arlington, VA, 1978, pp. 531–540.

[147] M. E. Whitman, "Enemy at the Gate: Threats to Information Security," *Commun ACM*, vol. 46, no. 8, pp. 91–95, Aug. 2003, doi: 10.1145/859670.859675.

[148] C. Schou and D. P. Shoemaker, *Information Assurance for the Enterprise: A Roadmap to Information Security*, 1st ed. New York, NY, USA: McGraw-Hill, Inc., 2007.

[149] H. Pardue, J. Landry, and Yasinsac, Alec, “E-Voting Risk Assessment: A Threat Tree for Direct Recording Electronic Systems,” *Int J Inf Sec Priv*, vol. 5, no. 3, pp. 19–35, Jul. 2011, doi: 10.4018/jisp.2011070102.

[150] H. Pardue, J. Landry, and A. Yasinsac, “A Risk Assessment Model for Voting Systems using Threat Trees and Monte Carlo Simulation,” in *2009 First International Workshop on Requirements Engineering for e-Voting Systems*, Aug. 2009, pp. 55–60. doi: 10.1109/RE-VOTE.2009.1.

[151] B. Schneier, “Attack Trees,” *Dr Dobbs J. Softw. Tools*, vol. 24, no. 12, pp. 21–29, Dec. 1999.

[152] “Unified Modeling Language.” http://www.uml.org/ (accessed Jun. 22, 2018).

[153] Joint Task Force Transformational Initiative Interagency Working Group, “Security and Privacy Controls for Federal Information Systems and Organizations,” National Institute of Standards and Technology, Special Publication NIST SP 800-53r4, Apr. 2013. doi: 10.6028/NIST.SP.800-53r4.

[154] T. R. Peltier, *Information Security Risk Analysis, 2nd*, Second Edition. Boca Raton, FL: Auerbach Publications, Taylor & Francis Group.

[155] “The STRIDE Threat Model,” *Microsoft Corporation*. https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx (accessed Mar. 30, 2017).

[156] “OWASP Risk Rating Methodology - OWASP,” *Open Web Application Security Project (OWASP)*, May 30, 2016. https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology#The_OWASP_Risk_Rating_Methodology (accessed Mar. 08, 2018).

[157] "Risk Management Framework (RMF) Overview - Risk Management | CSRC," *National Institute of Standards and Technology (NIST)*, Nov. 30, 2016. https://csrc.nist.gov/projects/risk-management/risk-management-framework-(RMF)-Overview (accessed Mar. 08, 2018).

[158] "CVSS v2 Complete Documentation," *FIRST — Forum of Incident Response and Security Teams*. https://www.first.org/cvss/v2/guide (accessed May 15, 2020).

[159] "CVE - Common Vulnerabilities and Exposures," *MITRE*. https://cve.mitre.org/ (accessed Jun. 27, 2018).

[160] "CWE - Common Weakness Enumeration," *MITRE*. https://cwe.mitre.org/index.html (accessed Jun. 27, 2018).

[161] Center for Devices and Radiological Health, "MAUDE - Manufacturer and User Facility Device Experience," *U. S. Food and Drug Administration*, Sep. 30, 2015. https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfmaude/search.cfm#fn1 (accessed Oct. 14, 2015).

[162] Center for Devices and Radiological Health, "MedSun: Medical Product Safety Network," *U. S. Food and Drug Administration*, Sep. 19, 2016. http://www.fda.gov/MedicalDevices/Safety/MedSunMedicalProductSafetyNetwork/ (accessed Nov. 16, 2016).

[163] Center for Devices and Radiological Health, "510(k) Clearances," *U. S. Food and Drug Administration*. https://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/DeviceApprovalsandClearances/510kClearances/ (accessed Jun. 21, 2017).

[164] Center for Devices and Radiological Health, “Medical Device Recalls.” https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfRES/res.cfm (accessed Jun. 21, 2017).

[165] “Shodan.” https://www.shodan.io/ (accessed May 18, 2020).

[166] “Professional | Joval Continuous Monitoring.” https://jovalcm.com/professional-edition/ (accessed May 22, 2020).

[167] Brant Cheikes, David A. Waltermire, and Karen A. Scarfone, “Common Platform Enumeration (CPE): Naming Specification Version 2.3,” National Institute of Standards and Technology, NIST Pubs 7695, Aug. 2011. [Online]. Available: https://www.nist.gov/publications/common-platform-enumeration-naming-specification-version-23

[168] “NVD - Official CPE Dictionary,” *National Institute of Standards and Technology (NIST)*. https://nvd.nist.gov/products/cpe (accessed Mar. 04, 2018).

[169] “NVD - XML Vulnerability Feed Retirement.” https://nvd.nist.gov/General/News/XML-Vulnerability-Feed-Retirement (accessed May 28, 2020).

[170] M. Van Devender, W. B. Glisson, M. Campbell, and M. Finan, “Identifying Opportunities to Compromise Medical Environments,” in *Proceedings of the Americas Conference on Information Systems (AMCIS 2016)*, San Diego, CA, Aug. 2016.

[171] M. Van Devender and J. T. McDonald, “A Quantitative Risk Assessment Framework for the Cybersecurity of Networked Medical Devices,” in *Proceedings*

of the 18th International Conference on Cyber Warfare and Security, Towson, MD, Mar. 2023.

[172] J. McMillan, W. Glisson, and M. Bromby, "Investigating the increase in mobile phone evidence in criminal activities. System Sciences (HICSS)," in *2013 46th Hawaii International Conference on*, 2013.

[173] K. J. Berman, W. B. Glisson, and L. M. Glisson, "Investigating the impact of global positioning system evidence," in *2015 48th Hawaii International Conference on System Sciences*, 2015, pp. 5234–5243.

[174] "FBI Cyber Division Bulletin: Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions | Public Intelligence," May 06, 2014. https://publicintelligence.net/fbi-health-care-cyber-intrusions/ (accessed Sep. 08, 2022).

[175] Cooper, Michol A.; Ibrahim, Andrew; Lyu, Heather; Makary, Martin A., "Underreporting of robotic surgery complications," *J. Healthc. Qual.*, vol. 37, no. 2, pp. 133–138, Apr. 2015, doi: 10.1111/jhq.12036.

[176] "Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-The-Shelf (OTS) Software," *U. S. Food and Drug Administration*, Jul. 28, 2015. http://www.fda.gov/RegulatoryInformation/Guidances/ucm070634.htm (accessed Nov. 13, 2015).

[177] W. B. Glisson, T. Andel, T. McDonald, M. Jacobs, M. Campbell, and J. Mayr, "Compromising a Medical Mannequin.," 2015, [Online]. Available:

https://libproxy.usouthal.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsarx&AN=1509.00065&site=eds-live

[178] K. Malasri and L. Wang, "Securing wireless implantable devices for healthcare: Ideas and challenges," *Commun. Mag. IEEE*, vol. 47, no. 7, pp. 74–80, Jul. 2009, doi: 10.1109/MCOM.2009.5183475.

[179] M. Rushanan, A. D. Rubin, D. F. Kune, and C. M. Swanson, "SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks," in *Security and Privacy (SP), 2014 IEEE Symposium on*, May 2014, pp. 524–539. doi: 10.1109/SP.2014.40.

[180] C. Camara, P. Peris-Lopez, and J. E. Tapiador, "Security and privacy issues in implantable medical devices: A comprehensive survey," *J. Biomed. Inform.*, vol. 55, pp. 272–289, 2015, doi: http://dx.doi.org/10.1016/j.jbi.2015.04.007.

[181] Li, Chunxiao, Zhang, Meng, Raghunathan, Anand, and Jha, Niraj K., "Attacking and Defending a Diabetes Therapy System," in *Security and Privacy for Implantable Medical Devices*, Burleson, Wayne and Carrara, Sandro, Eds. Springer New York, 2014, pp. 175–193.

[182] T. Bonaci, J. Herron, T. Yusuf, J. Yan, T. Kohno, and H. J. Chizeck, "To Make a Robot Secure: An Experimental Analysis of Cyber Security Threats Against Teleoperated Surgical Robots," Apr. 2015, [Online]. Available: https://libproxy.usouthal.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsarx&AN=1504.04339&site=eds-live

[183] Lee, Gregory S. and B. Thuraisingham, “Cyberphysical systems security applied to telesurgical robotics,” *Comput. Stand. Interfaces*, vol. 34, pp. 225–229, 2012, doi: 10.1016/j.csi.2011.09.001.

[184] K. K. Venkatasubramanian, E. Y. Vasserman, O. Sokolsky, and I. Lee, “Security and Interoperable Medical Device Systems: Part 1,” *IEEE Secur. Priv.*, vol. 10, no. 5, pp. 61–63, 2012, doi: 10.1109/MSP.2012.128.

[185] “LexisNexis® Legal Research & Practical Guidance,” *LexisNexis*, Oct. 15, 2015. http://www.lexisnexis.com/en-us/legal-research-and-transactions/default.page (accessed Oct. 17, 2015).

[186] Administrative Office of the U. S. Courts, “Public Access to Court Electronic Records,” *PACER*. https://www.pacer.gov/ (accessed Oct. 17, 2015).

[187] Oates, Briony J., *Researching Information Systems and Computing*. SAGE Publications, Ltd, 2007.

[188] R. K. Yin, *Case study research: Design and methods*, vol. 5. sage, 2009.

[189] H. Alemzadeh, D. Chen, A. Lewis, Z. Kalbarczyk, and R. K. Iyer, “Systems-theoretic Safety Assessment of Robotic Telesurgical Systems,” *CoRR*, vol. abs/1504.07135, 2015, [Online]. Available: http://arxiv.org/abs/1504.07135

[190] “Intuitive Surgical Announces Preliminary Fourth Quarter and Full Year 2015 Results,” *Intuitive Surgical*, Jan. 13, 2016. http://investor.intuitivesurgical.com/mobile.view?c=122359&v=203&d=1&id=2128884 (accessed Feb. 24, 2016).

[191] S. McKeown, D. Maxwell, L. Azzopardi, and W. B. Glisson, “Investigating people: A qualitative analysis of the search behaviours of open-source intelligence

analysts," in *Proceedings of the 5th Information Interaction in Context Symposium*, 2014, pp. 175–184.

[192] U. S. Food and Drug Administration, "FDA, Medical Devices, Overview of Device Regulation," *FDA*. http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ (accessed Oct. 02, 2015).

[193] "Intuitive Surgical - da Vinci Surgical System," *Intuitive Surgical, Inc.*, 2015. http://www.intuitivesurgical.com/products/davinci_surgical_system/ (accessed Oct. 18, 2015).

[194] "Robotic Surgery: The da Vinci Surgical System," *University of Southern California, Cardiothoracic Surgery*. http://www.cts.usc.edu/rsi-davincisystem.html (accessed Nov. 04, 2015).

[195] "Intuitive Surgical - OnSite for the da Vinci Surgical System," *Intuitive Surgical, Inc.*, May 2015. http://www.intuitivesurgical.com/support/onsite.html (accessed Oct. 06, 2015).

[196] "Stryker Corporation," *Stryker Corporation*. http://www.stryker.com/en-us/index.htm (accessed Feb. 25, 2016).

[197] W. H. L. Chang, S. Hameed, A. A. Mahadik, K. A. Javadekar, and O. F. Abello, "Multi-function image and video capture device for use in an endoscopic camera system," Sep. 2004 [Online]. Available: http://www.google.com/patents/US6791601

[198] D. Kushner, "The Real Story of Stuxnet," *IEEE Spectrum: Technology, Engineering, and Science News*, Feb. 26, 2013.

http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet (accessed Nov. 29, 2016).

[199] D. Goodin, “This thumbdrive hacks computers. ‘BadUSB’ exploit makes devices turn ‘evil,’” *Ars Technica*, Jul. 31, 2014. http://arstechnica.com/security/2014/07/this-thumbdrive-hacks-computers-badusb-exploit-makes-devices-turn-evil/ (accessed Nov. 29, 2016).

[200] “Vulnerability Summary for CVE-2004-1038,” *NIST National Vulnerability Database*, Mar. 01, 2005. https://nvd.nist.gov/vuln/detail/CVE-2004-1038 (accessed Sep. 08, 2022).

[201] “IEEE SA - 1394-2008 - IEEE Standard for a High-Performance Serial Bus,” *IEEE*, 2008. https://standards.ieee.org/findstds/standard/1394-2008.html (accessed Feb. 26, 2016).

[202] “Windows XP End of Support April 8th, 2014,” *Microsoft*, 2014. https://www.microsoft.com/en-us/WindowsForBusiness/end-of-xp-support (accessed Nov. 29, 2016).

[203] T. Zhao, W. Zhao, B. D. Hoffman, W. C. Nowlin, and H. Hui, “US Patent 8,971,597 B2, Efficient Vision and Kinematc Data Fusion for Robotic Surgical Instruments and Other Applications,” 8,971,597 B2, Mar. 15, 2015

[204] P. O’Grady, I. McDowall, and B. D. Hoffman, “US Patent 9,019,345 B2, Imaging Mode Blooming Suppression,” 9,019,345 B2, Apr. 2015

[205] Verizon, “2022 Data Breach Investigation Report (DBIR),” *Verizon Enterprise Solutions*, 2022.

https://www.verizon.com/business/resources/reports/2022/dbir/2022-dbir-data-breach-investigations-report.pdf (accessed Jun. 18, 2022).

[206] HIMSS, “2021 HIMSS Healthcare Cybersecurity Survey Report | HIMSS,” Jan. 2022. Accessed: Jun. 03, 2022. [Online]. Available: https://www.himss.org/resources/himss-healthcare-cybersecurity-survey

[207] P. A. Williams and A. J. Woodward, “Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem,” *Med. Devices Auckl. NZ*, vol. 8, p. 305, 2015.

[208] Federal Bureau of Investigation (FBI), “220912 Unpatched and Outdated Medical Devices Provide Cyber Attack Opportunities.” Federal Bureau of Investigation (FBI), Sep. 12, 2022. [Online]. Available: https://www.ic3.gov/Media/News/2022/220912.pdf

[209] R. Hireche, H. Mansouri, and A.-S. K. Pathan, “Security and Privacy Management in Internet of Medical Things (IoMT): A Synthesis,” *J. Cybersecurity Priv.*, vol. 2, no. 3, pp. 640–661, 2022.

[210] US Dept of Homeland Security, “A Lifeline: Patient Safety & Cybersecurity.” U. S. Department of Homeland Security, 2019. Accessed: Aug. 04, 2021. [Online]. Available: https://www.dhs.gov/sites/default/files/publications/ia/ia_vulnerabilities-healthcare-it-systems.pdf

[211] K. Collier, “Baby died because of ransomware attack on hospital, suit says,” *NBC News*. https://www.nbcnews.com/news/baby-died-due-ransomware-attack-hospital-suit-claims-rcna2465 (accessed Jun. 29, 2022).

[212] M. Eddy and N. Perlroth, “Cyber Attack Suspected in German Woman’s Death,” *The New York Times*, Sep. 18, 2020. Accessed: Jun. 29, 2022. [Online]. Available: https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html

[213] I. Lee *et al.*, “Challenges and Research Directions in Medical Cyber Physical Systems,” *Proc. IEEE*, vol. 100, no. 1, pp. 75–90, Jan. 2012, doi: 10.1109/JPROC.2011.2165270.

[214] R. M. Cooke and L. Goossens, “Procedures guide for structured expert judgment,” *EUR(Luxembourg)*, [Online]. Available: https://op.europa.eu/en/publication-detail/-/publication/7faaedf8-d59b-465e-a9c1-23cce34ee2b4

[215] N. R. Ortiz, T. A. Wheeler, R. J. Breeding, S. Hora, M. A. Meyer, and R. L. Kenney, “Use of expert judgement in NUREG-1150,” *Nucl. Eng. Des.*, vol. 126, no. 3, pp. 313–331, 1991.

[216] M. Krisper, J. Dobaj, and G. Macher, “Assessing Risk Estimations for Cyber-Security Using Expert Judgment,” in *Systems, Software and Services Process Improvement*, vol. 1251, M. Yilmaz, J. Niemann, P. Clarke, and R. Messnarz, Eds. Cham: Springer International Publishing, 2020, pp. 120–134. doi: 10.1007/978-3-030-56441-4_9.

[217] L. H. Goossens, R. Cooke, A. R. Hale, and L. Rodić-Wiersma, “Fifteen years of expert judgement at TUDelft,” *Saf. Sci.*, vol. 46, no. 2, pp. 234–244, 2008.

[218] T. G. Martin *et al.*, “Eliciting expert knowledge in conservation science,” *Conserv. Biol.*, vol. 26, no. 1, pp. 29–38, 2012.

[219] ISO, “ISO - Standards,” *ISO*. https://www.iso.org/standards.html (accessed Oct. 11, 2022).

[220] R. Caralli, J. Stevens, L. Young, and W. Wilson, “Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process,” Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, CMU/SEI-2007-TR-012, 2007. [Online]. Available: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=8419

[221] NTIA, “Software Component Transparency,” National Telecommunications and Information Administration, Oct. 2019. [Online]. Available: https://www.ntia.gov/files/ntia/publications/ntia_sbom_healthcare_poc_report_2019_1001.pdf

[222] N. A. Hassan and R. Hijazi, *Open Source Intelligence Methods and Tools*. Springer, 2018.

[223] FIRST, “Common Vulnerability Scoring System v3.1.” FIRST, Jun. 2019. [Online]. Available: https://www.first.org/cvss/v3.1/specification-document

[224] S. Samonas and D. Coss, “The CIA strikes back: Redefining confidentiality, integrity and availability in security.,” *J. Inf. Syst. Secur.*, vol. 10, no. 3, 2014.

[225] NIST, “Predisposing Condition - Glossary | CSRC,” *NIST Computer Security Resource Center*. https://csrc.nist.gov/glossary/term/predisposing_condition (accessed Jul. 17, 2022).

[226] M. Rosenquist, “Prioritizing information security risks with threat agent risk assessment.” Intel Corporation White Paper, 2009.

[227] ThoughtLab, “Cybersecurity Solutions for a Riskier World,” 2022. [Online]. Available: https://thoughtlabgroup.com/wp-content/uploads/2022/05/Cybersecurity-Solutions-for-a-Riskier-World-eBook_FINAL-2-1.pdf

[228] “Executive Order -- Improving Critical Infrastructure Cybersecurity,” *whitehouse.gov*, Feb. 12, 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (accessed Jul. 01, 2022).

[229] “Presidential Policy Directive -- Critical Infrastructure Security and Resilience,” *whitehouse.gov*, Feb. 12, 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (accessed Jul. 01, 2022).

[230] *H. R. 7898 - HIPAA Safe Harbor Law*. 2021. [Online]. Available: https://www.congress.gov/116/plaws/publ321/PLAW-116publ321.pdf

[231] “HIPAA Administrative Simplification Statute and Rules,” *HHS - Office of Civil Rights, Health Information Privacy*. http://www.hhs.gov/ocr/privacy/hipaa/administrative/index.html (accessed Nov. 20, 2015).

[232] NIST, “Framework for Improving Critical Infrastructure Cybersecurity.” National Institute of Standards and Technology, Feb. 12, 2014. Accessed: Oct. 08, 2015. [Online]. Available: http://www.nist.gov/cyberframework/

[233] “NIST Special Publication 800-series General Information,” *NIST*, May 21, 2018. https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information (accessed Jul. 02, 2022).

[234] "2020 HIMSS Cybersecurity Survey," 2021. Accessed: Aug. 03, 2021. [Online]. Available: https://www.himss.org/resources/himss-healthcare-cybersecurity-survey

[235] "Blue Flow by Virta Laboratories, Inc." https://www.virtalabs.com/ (accessed Feb. 06, 2019).

[236] "Medigate," Aug. 04, 2021. https://claroty.com/healthcare-cybersecurity/medigate (accessed Aug. 04, 2021).

[237] "Clearwater Healthcare Cyber Risk Management," *Clearwater*. https://clearwatercompliance.com/ (accessed Aug. 04, 2021).

[238] "Nuvolo Medical Device Cybersecurity." https://www.nuvolo.com/solutions/cybersecurity (accessed Feb. 06, 2019).

[239] S. Sappal and P. Prowse, "A Cybersecurity Vulnerability Management System for Medical Devices," *CMBES Proc.*, vol. 44, May 2021, [Online]. Available: https://proceedings.cmbes.ca/index.php/proceedings/article/view/951

[240] S. Coley and P. Chase, "Rubric for Applying CVSS to Medical Devices." Mitre Corporation, Oct. 27, 2020.

[241] A. A. Ganin *et al.*, "Multicriteria decision framework for cybersecurity risk assessment and management," *Risk Anal.*, vol. 40, no. 1, pp. 183–199, 2020.

[242] "ICS-CERT Advisories | CISA." https://www.cisa.gov/uscert/ics/advisories (accessed Mar. 23, 2023).

[243] "National Cyber Awareness System | CISA." https://us-cert.cisa.gov/ncas (accessed Aug. 05, 2021).

[244] "What is a zero-day exploit?" https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work.html (accessed Jun. 28, 2022).

[245] *Federal Food, Drug, and Cosmetic ACT (FD&C Act)*, vol. 21 CFR. [Online]. Available: https://uscode.house.gov/browse/prelim@title21/chapter9/subchapter5/partA&edition=prelim

[246] *21 C.F.R. § 360c 2002*.

[247] "Cost of a Data Breach Report 2021." IBM Security.

[248] "American Hospital Directory - information about hospitals from public and private data sources including MedPAR, OPPS, hospital cost reports, and other CMS files." https://www.ahd.com/ (accessed Jul. 11, 2022).

[249] "Common Vulnerability Scoring System SIG," *FIRST — Forum of Incident Response and Security Teams*. https://www.first.org/cvss (accessed Jun. 13, 2022).

[250] Medigate, "Calculating Risk for Devices on Healthcare Enterprise Networks." Medigate, Mar. 2021. Accessed: Jul. 02, 2021. [Online]. Available: https://www.medigate.io/calculating-risk-for-devices-on-healthcare-enterprise-networks/

[251] "AAMI," *Default*. https://www.aami.org (accessed Feb. 25, 2023).

[252] "NVD - Vulnerability Metrics," *National Institute of Standards and Technology (NIST)*. https://nvd.nist.gov/vuln-metrics/cvss (accessed Feb. 26, 2023).

[253] "Council Policy Manual Association for Information Systems." Association for Information Systems, Jun. 08, 2014. [Online]. Available: https://cdn.ymaws.com/aisnet.org/resource/resmgr/ais_policy_manual/Council_Policy_Manual_v_23.pdf

[254] “Submissions | International Conference on Cyber Warfare and Security.” https://papers.academic-conferences.org/index.php/iccws/about/submissions (accessed Mar. 14, 2023).

BIOGRAPHICAL SKETCH

Maureen S. Van Devender graduated from the University of South Alabama in Mobile, Alabama with a Bachelor of Science in Computer and Information Sciences in 1991, from Spring Hill College in Mobile, Alabama with a Master in Business Administration in 2002 where she was awarded the Outstanding MBA Graduate Award, and from the University of South Alabama in Mobile, Alabama with a Doctor of Philosophy in Computing in 2023. She has published the conference papers "Identifying Opportunities to Compromise Medical Environments" in "*The Americas Conference on Information Systems*", *AMCIS 2016*, "Understanding De-identification of Healthcare Big Data" in *The Americas Conference on Information Systems, AMCIS 2017, A Quantitative Risk Assessment Framework for the Cybersecurity of Networked Medical Devices, ICCWS 2023,* and was a contributing author on "Attack Modeling and Mitigation Strategies for Risk-Based Analysis of Networked Medical Devices" in *The 53rd Hawaii International Conference on System Sciences, HICSS 2020*.