A Quantitative Risk Assessment Framework for the Cybersecurity of Networked Medical Devices

Maureen S. Van Devender and Jeffrey Todd McDonald
University of South Alabama, Mobile, AL USA

mvandevender@southalabama.edu
jtmcdonald@southalabama.edu

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.

Keywords: Risk assessment framework, medical device security risk, threat/vulnerability/asset (TVA) models

1. Introduction

Cybersecurity incidents are on the rise, and organizations face the challenge of protecting against attacks from an adversary that is increasing in sophistication (Verizon, 2022). Healthcare organizations are experiencing significant security incidents (HIMSS, 2022) (Williams and Woodward, 2015). 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 (TrapX Labs, 2015) (Federal Bureau of Investigation (FBI), 2022). Email phishing attacks are reported as a significant source of cybersecurity exposure (HIMSS, 2022), 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 (Reel and Robertson, 2015). 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 (Hireche *et al.*, 2022).

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 (HIMSS, 2022). 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 (US Dept of Homeland Security, 2019). However, two legal proceedings alleging deaths related to ransomware attacks on hospital networks have been reported (Collier, n.d.; Eddy and Perlroth, 2020).

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 2 provides related work to our approach and section 3 proposes a risk assessment framework for networked medical devices. In section 4 we conclude with the merits and limitations of the proposed framework and discuss future work.

2. Related Work

Lee et al., (Lee *et al.*, 2012) 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 (Kaplan and Garrick, 1981) 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 (Hubbard and Seiersen, 2016). 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 (Cooke and Goossens, n.d.; Ortiz *et al.*, 1991). Krisper, et al. (Krisper *et al.*, 2020) 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 (Lichtenstein and Fischhoff, 1980) 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 (Goossens *et al.*, 2008) and conservation science (Martin *et al.*, 2012). 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.

3. 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 (1) :

$$R_e = F_e I_e \quad (1)$$

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 (HITRUST Alliance, 2019) (CIS, 2019; ISO, n.d.) (Caralli *et al.*, 2007), several sources were selected for their suitability to this context. First, the Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) (NIST - CF, 2018) 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 (HIMSS, 2018) 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 (ISO, n.d.), a prominent risk assessment tool set. Second, the NIST SP 800-30 Guide for Conducting Risk Assessment (Ross, 2012) is used for the stepwise structure it provides. Third, the Factor Analysis of Information Risk (FAIR) (Freund and Jones, 2014) 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, and combining threats, vulnerabilities, and likelihoods to determine risk. Our framework, based on the four-step process of the NIST SP 800-30 Risk Assessment Process is shown in **Figure 1**. A description of the execution of each of the steps in this research follows.

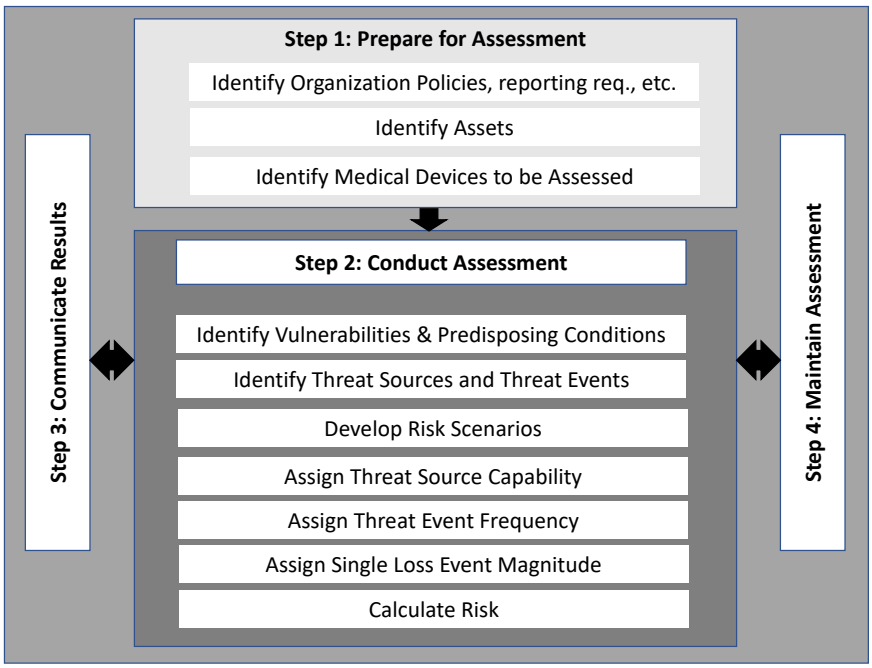

Figure 1: Medical Device Risk Assessment Framework

3.1 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.

3.1.1 Identify Assets

In a medical device risk assessment, it would be logical to consider the medical devices to be the asset. However, Landoll (2011) 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 (Freund and Jones, 2014), 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 (Landoll, 2011).

3.1.2 Identify Target Devices

The OCTAVE Allegro framework (Caralli *et al.*, 2007) 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 (NTIA, 2019). With this limitation, every effort should be made to identify the components of each device.

The Security Content Automation Protocol (SCAP) (NIST - SCAP, n.d.) is a community effort overseen by NIST that contains standardized expressions. Of interest to us in SCAP is Common Platform Enumeration (CPE) (NIST - CPE, n.d.) 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.

3.2 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 (Kaplan and Garrick, 1981) 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.

3.2.1 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) (Hassan and Hijazi, 2018) techniques can be used to identify cybersecurity vulnerabilities that may have been reported by other parties.

Common Vulnerabilities and Exposures (CVEs) (NIST- NVD, n.d.) 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 (NIST - CPE,

n.d.). 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 (FIRST, 2019) 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 (Samonas and Coss, 2014). 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 (NIST, n.d.). Conditions of interest for each device include: whether it contains PHI, the physical security status of the device, the FDA class (FDA, 2018) 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 1** 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 1: 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

3.2.2 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 (Ross, 2012). In this assessment, threats are decomposed into threat sources and threat events.

3.2.3 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 (Ross, 2012). 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 (Freund and Jones, 2014). Threats sources are generalized as: adversarial/malicious and human errors of omission or commission (Ross, 2012). 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 (Ross, 2012). 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.

The FAIR methodology references the work of Intel (Rosenquist, 2009) in the establishment of a threat agent library. **Table 2** shows the attributes that we identify for establishing a threat agent library based on the work presented in the FAIR methodology (Freund and Jones, 2014) 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.

Table 2: Threat Agent Library

Threat Source	Motive	Primary Intent	Sponsorship	Preferred Target characteristics	Preferred targets	Capability	Personal Risk Tolerance	Concern for Collateral Damage
Established Cyber-criminal Organization	Financial or PHI	Data gathering and/or disruption of services	unknown	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)	Unmotivated Error	goodwill	none	Systems they access	no preference	Low to high depending on system	Low to medium	High

3.2.4 *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 (Lichtenstein and Fischhoff, 1980). 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 3: 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

3.2.5 *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.

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 (NIST - CF, 2018). Additional threat events can be obtained from examples provided in NIST SP 800-30 (Ross, 2012). Threat event information may also be gathered from descriptions provided in CVEs discovered in the vulnerability identification process.

3.2.6 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 4** shows a list of example scenarios.

Table 4: 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.

3.2.7 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.

3.2.8 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 (Lichtenstein and Fischhoff, 1980). 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 (2).

$$Threat\ Event\ Frequency\ (TEF) = \frac{Min\ TEF + (4 * Most\ Likely\ TEF) + Max\ (TEF}{6} \quad (2)$$

In addition to the expert elicitation, 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 (NIST- NVD, n.d.) of the CVSS score (FIRST, 2019), discussed in the vulnerability identification step, to further refine the threat 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 (FIRST, 2019). 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 in (3).

$$\text{Vulnerability} = \frac{(CVE\ Expoitablity\ sub\ score - 0.12)}{3.9 - 0.12} x \frac{Min\ TAC + (4\ x\ Most\ Likely\ TAC) + Max\ TAC}{6} \quad (3)$$

The calculation for the loss event frequency is shown in (4).

*Loss Event Frequency = Threat event frequency * vulnerability* (4)

3.2.9 Assign Single Loss Event Magnitude Estimate 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 (NIST- NVD, n.d.) of the CVSS score (FIRST, 2019), discussed in the vulnerability identification step, to further refine the loss magnitude. The CIA impacts each have a value of 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 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 5 shows the loss magnitude multipliers. The calculation for Single Loss Magnitude is show in (5).

Table 5: 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

$$\text{Single Loss Magnitude} = Loss\ Magnitude\ Multiplier\ x\ \frac{Min\ Single\ Loss\ Mag\ Est. + (4 * Most\ Likely\ Single\ Loss\ Mag\ Est.) + Max\ Single\ Loss\ Mag\ Est.}{6} \quad (5)$$

3.2.10 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 in (6).

Risk = Expected Loss Magnitude = Single Loss Magnitude * Loss Event Frequency (6)

4 Discussion & 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.

References

Caralli, R., Stevens, J., Young, L. and Wilson, W. (2007), *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*, No. CMU/SEI-2007-TR-012, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA.

CIS. (2019), "CIS Critical Security Controls v7.1", Center for Internet Security, April.

Collier, K. (n.d.). "Baby died because of ransomware attack on hospital, suit says", *NBC News*, available at: https://www.nbcnews.com/news/baby-died-due-ransomware-attack-hospital-suit-claims-rcna2465 (accessed 29 June 2022).

Cooke, R.M. and Goossens, L. (n.d.). "Procedures guide for structured expert judgment", *EUR(Luxembourg)*, Office for official publications of the European Communities.

Eddy, M. and Perlroth, N. (2020), "Cyber Attack Suspected in German Woman's Death", *The New York Times*, 18 September.

FDA. (2018), "Overview of Medical Device Classification and Reclassification", *US Food & Drug Administration*.

Federal Bureau of Investigation (FBI). (2022), "220912 Unpatched and Outdated Medical Devices Provide Cyber Attack Opportunities", Federal Bureau of Investigation (FBI), 12 September.

FIRST. (2019), "Common Vulnerability Scoring System v3.1", FIRST, June.

Freund, J. and Jones, J. (2014), *Measuring and Managing Information Risk: A FAIR Approach*, Butterworth-Heinemann.

Ganin, A.A., Quach, P., Panwar, M., Collier, Z.A., Keisler, J.M., Marchese, D. and Linkov, I. (2020), "Multicriteria decision framework for cybersecurity risk assessment and management", *Risk Analysis*, Wiley Online Library, Vol. 40 No. 1, pp. 183–199.

Goossens, L.H., Cooke, R., Hale, A.R. and Rodić-Wiersma, L. (2008), "Fifteen years of expert judgement at TUDelft", *Safety Science*, Elsevier, Vol. 46 No. 2, pp. 234–244.

Hassan, N.A. and Hijazi, R. (2018), *Open Source Intelligence Methods and Tools*, Springer.

HIMSS. (2018), *2018 HIMSS Cybersecurity Survey*, HIMSS North America, Chicago, IL.

HIMSS. (2022), *2021 HIMSS Healthcare Cybersecurity Survey Report | HIMSS*.

Hireche, R., Mansouri, H. and Pathan, A.-S.K. (2022), "Security and Privacy Management in Internet of Medical Things (IoMT): A Synthesis", *Journal of Cybersecurity and Privacy*, MDPI, Vol. 2 No. 3, pp. 640–661.

HITRUST Alliance. (2019), "HITRUST CSF, Version 9.2", HITRUST Alliance, January.

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

ISO. (n.d.). "ISO - Standards", *ISO*, available at: https://www.iso.org/standards.html (accessed 11 October 2022).

Kaplan, S. and Garrick, B.J. (1981), "On The Quantitative Definition of Risk", *Risk Analysis*, Vol. 1 No. 1, pp. 11–27, doi: 10.1111/j.1539-6924.1981.tb01350.x.

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

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

Lee, I., Sokolsky, O., Chen, S., Hatcliff, J., Jee, E., Kim, B., King, A., *et al.* (2012), "Challenges and Research Directions in Medical Cyber Physical Systems", *Proceedings of the IEEE*, Vol. 100 No. 1, pp. 75–90, doi: 10.1109/JPROC.2011.2165270.

Lichtenstein, S. and Fischhoff, B. (1980), "Training for calibration", *Organizational Behavior and Human Performance*, Elsevier, Vol. 26 No. 2, pp. 149–171.

Martin, T.G., Burgman, M.A., Fidler, F., Kuhnert, P.M., Low-Choy, S., McBride, M. and Mengersen, K. (2012), "Eliciting expert knowledge in conservation science", *Conservation Biology*, Wiley Online Library, Vol. 26 No. 1, pp. 29–38.

NIST. (n.d.). "Predisposing Condition - Glossary | CSRC", *NIST Computer Security Resource Center*, available at: https://csrc.nist.gov/glossary/term/predisposing_condition (accessed 17 July 2022).

NIST - CF. (2018), "Framework for Improving Critical Infrastructure Cybersecurity Version 1.1", National Institute of Standards and Technology, 16 April.

NIST - CPE. (n.d.). "Common Platform Enumeration", *National Institute of Standards and Technology (NIST)*, Government, , available at: https://csrc.nist.gov/Projects/Security-Content-Automation-Protocol/Specifications/cpe (accessed 4 March 2018).

NIST - SCAP. (n.d.). "Security Content Automation Protocol | CSRC", *NIST*, Government, , available at: https://csrc.nist.gov/projects/security-content-automation-protocol/ (accessed 4 March 2018).

NIST- NVD. (n.d.). "National Vulnerability Database", *Government*, available at: https://nvd.nist.gov/ (accessed 20 November 2017).

NTIA. (2019), *Software Component Transparency*, National Telecommunications and Information Administration, p. 20.

Ortiz, N.R., Wheeler, T.A., Breeding, R.J., Hora, S., Meyer, M.A. and Kenney, R.L. (1991), "Use of expert judgement in NUREG-1150", *Nuclear Engineering and Design*, Netherlands, Vol. 126 No. 3, pp. 313–331.

Reel, M. and Robertson, J. (2015), "It's Way Too Easy to Hack the Hospital", *Bloomberg.Com*, November, available at: http://www.bloomberg.com/features/2015-hospital-hack/ (accessed 17 April 2016).

Rosenquist, M. (2009), "Prioritizing information security risks with threat agent risk assessment", Intel Corporation White Paper.

Ross, R. (2012), *Guide for Conducting Risk Assessments - Special Publication (NIST SP) - 800-30 Rev 1*, NIST Special Publication No. 800–30 Rev 1, National Institute of Standards and Technology, Gaithersburg, MD.

Samonas, S. and Coss, D. (2014), "The CIA strikes back: Redefining confidentiality, integrity and availability in security.", *Journal of Information System Security*, Vol. 10 No. 3.

TrapX Labs. (2015), *MEDJACK (Medical Device Hijack)*, TrapX Security, Inc., p. 39.

US Dept of Homeland Security. (2019), "A Lifeline: Patient Safety & Cybersecurity", U. S. Department of Homeland Security.

Verizon. (2022), "2022 Data Breach Investigation Report (DBIR)", *Verizon Enterprise Solutions*, available at: https://www.verizon.com/business/resources/reports/2022/dbir/2022-dbir-data-breach-investigations-report.pdf (accessed 18 June 2022).

Williams, P.A. and Woodward, A.J. (2015), "Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem", *Medical Devices (Auckland, NZ)*, Dove Press, Vol. 8, p. 305.