A Cybersecurity Risk Assessment Framework that Integrates Value-Sensitive Design

Aida Alvarenga and George Tanev

> *"The fact we have insecure embedded computers responsible for critical health functions should give pause to everyone involved. We hold banks responsible for security of a $10 online purchase, but we'll give medical device makers a free pass on not securing the devices responsible for our health or even our lives?"*
>
> Jay Radcliffe
> Cybersecurity researcher and diabetic
> who hacked his own insulin pump

Medical devices today are more effective and connected than ever before, saving more patient lives and making healthcare practitioner's jobs more efficient. But with this interconnectedness comes inherent concerns over increased cybersecurity vulnerabilities. Medical device cybersecurity has become an increasing concern for all relevant stakeholders including: patients, regulators, manufacturers, and healthcare practitioners. Although cybersecurity in medical devices has been covered in the literature, there is a gap in how to address cybersecurity concerns and assess risks in a way that brings value to all relevant stakeholders. In order to maximize the value created from cybersecurity risk mitigations, we review literature on the state of cybersecurity in the medical device industry, on cybersecurity risk management frameworks in the context of medical devices, and on how cybersecurity can be used as a value proposition. We then synthesize the key contributions of the literature into a framework that integrates cybersecurity value considerations for all relevant stakeholders into the risk mitigation process. This framework is subsequently applied to the hypothetical case of an insulin pump. Using this example case, we illustrate how medical device manufacturers can use the framework as a standardized method that can be applicable to medical devices at large. Our ultimate goal is to make cybersecurity risk mitigation an exploitable asset for manufacturers rather than a regulatory obligation.

Introduction

Advancements in technology have revolutionized the healthcare industry by making medical devices more productive, reducing the amount of human error, and enabling automation – all of which are helping healthcare practitioners treat more conditions and save more patient lives today than ever before (American Hospital Association, 2014). Connectivity of medical devices with the Internet and with other devices, however, has made them vulnerable to an array of cybersecurity threats (Burns et al., 2016). Since wireless interaction with these devices has become possible, they are no longer a standalone component in the clinical care process – they depend on connections and can interact with other devices remotely (Williams & Woodward, 2015). Over the next five years, interconnected health products are expected to be worth $285 billion in economic value – a number that is expected to grow exponentially over time (Harris, 2014). As medical devices become increasingly connected, and as some high-profile vulnerabilities are being exposed, cybersecurity of medical devices is garnering increased public, regulatory, and industry attention regarding cybersecurity risk and risk mitigation strategies. One dimension of these efforts that has not been readily addressed is how to convert these security efforts from an obligation to an asset that can maximize the value delivered to medical device stakeholders (MDPC, 2014). This value dimension of security requires a unique approach, first in the way that security risk is assessed and mitigated, and second in the way it affects stakeholders of medical devices themselves.

In this article, we first review the literature through the perspective of using security initiatives as a value proposition. We separated the literature into three streams: the current medical device cybersecurity landscape, medical device risk assessment, and cybersecurity as a value proposition. We then synthesized the results of the literature review into a framework that integrates stakeholder values with cybersecurity risk mitigation. This framework aims to provide a benchmark for medical device manufacturers when assessing cybersecurity concerns for a wide array of medical devices. In order to illustrate how the medical device cybersecurity risk assessment framework can be applied, and in particular how to choose risk controls that maximize value to key stakeholders, we applied it to the theoretical case of an insulin pump.

Literature Review

Medical devices: A unique cybersecurity landscape

A medical device is defined as "an instrument, apparatus, machine, implant, or similar article, including a component part or accessory… intended for the use in the diagnosis of disease or other conditions or in the cure, mitigation, treatment or prevention of disease" (Williams & Woodward, 2015). What makes medical devices unique is that security concerns involving these devices could directly affect treatments, safety, and even the life of a patient (Burns et al., 2016). For instance, implantable medical devices that have wireless connections – such as pacemakers, drug pumps, and defibrillators – if accessed, could leave control of the device in the hands of the hacker. Williams and Woodward (2015) identify key vulnerabilities faced by medical devices when it comes to cybersecurity. These include, but are not limited to: accessing the Internet through devices that are connected to internal networks, default admin passwords, web interfaces to infusion pumps, and web services that do not have encrypted communications.

Although no lives have been threatened yet through the hacking of a medical device, Jay Radcliffe, a cybersecurity researcher and diabetic proved that it was possible to hack and access his own insulin pump (Buntz, 2011). Even though attacks on medical devices with the goal of purposeful harm are expected to be very rare, the theoretical possibility cannot be ignored. Possible motivations for such attacks could be the acquisition of private information for financial gain, damage to the reputation of a manufacturer, or even terrorism (Maisel & Kohno, 2010). Attacks on healthcare IT networks have also become more prevalent in recent years. A SANS Institute (Filkins, 2014) report estimates that "up to 94% of medical organizations networks have been victims of a cyber-attack". This prevalence highlights the vulnerable environment that many medical devices are being exposed to. In light of this, the United States Federal Bureau of Investigation (FBI, 2015) has issued warnings that intrusions against medical devices and in the healthcare industry overall will increase due to lenient standards and the increased value of health data in the black market. Medical device manufacturers are also potential targets of cyber-attacks, and the "failure to properly prevent or patch cybersecurity risk may result in disapproval of a device, recall, or other regulatory or legal action" (Farrel & Hanet, 2016). Given these mounting cybersecurity concerns, the United States Food and Drug Administration (FDA) has issued a non-binding draft guidance for industry to follow in order to ensure the confidentiality, integrity, and availability of patient data (Maisel & Kohno, 2010). Some of the FDA's key recommendations include: identifying risks and vulnerabilities, determining risk levels and mitigation strategies, reporting vulnerabilities, and issuing routine updates or patches (FDA, 2016).

Security risk assessment for medical devices

The Medical Device Privacy Consortium (MDPC), which includes some of the largest medical device companies in the world, published a whitepaper proposing a security risk assessment framework for medical devices (MDPC, 2014). They identify a number of key issues to consider when applying existing security risk assessment frameworks to a medical device. For example, they found that existing methods focus primarily on patient safety risks (i.e., negative impacts to a patient's health), or that they assess impact too broadly. They also observed a lack of uniformity around security risk assessment across the medical device industry, and even within different business units. Due to these differences, the outcomes of these assessments are not always understood and create challenges when knowledge needs to be transferred between stakeholders. Furthermore, for medical devices, there is minimal experimental data on security risks and the probability of occurrence of harm, which creates challenges for producing accurate and consistent probability determinations MDPC (2014).

To resolve these issues, the security assessment framework proposed by the MDPC (2014) is based on four core ideas:

1. *Device focused:* Integrate common principles and language that are used in existing security standards in order to facilitate transferability and comprehension of information.

2. *All devices:* The framework is to be universally applicable to all medical devices, throughout the full product lifecycle.

3. *Tailored impact:* The framework will focus specifically on the impact to the confidentiality, integrity, and availability of information within the context of medical devices.

4. *Simplified probability:* Risk probability will be defined in a qualitative manner, focusing on the ability to exploit vulnerabilities associated with identified risk scenarios.

The MDPC framework requires manufacturers to identify threat sources and vulnerabilities, develop risk scenarios, assess exploitability, assess impact, obtain risk scores, and make decisions about how the risk can be mitigated. The framework provides a structured and straightforward approach to identifying security risks and scenarios that caters to the unique dimensions of the medical device industry. It provides the general goal of determining whether additional security controls are necessary to reduce the residual risk. The MDPC adapts the NIST 800-30 definition of security control for its application to medical devices as “The management, operational and technical controls (i.e., safeguards or countermeasures) prescribed for an information system and/or medical device to protect the confidentiality, integrity, and availability of the system and/or device and its information” MDPC (2014). The MDPC framework does not suggest a process or criteria for choosing the right security control for a given risk, given that the options are not singular, or trivial. One of the keys to success emphasized in the MDPC (2014) whitepaper is that manufacturers should strive to make product security an asset, not an obligation. This point highlights the need to integrate the value creation process into the security risk controls that are generated by the risk assessment process.

Wu and Eagles (2016) take the approach of leveraging medical device manufacturer’s proficiency with safety risk analysis (typically based on the ANSI/AAMI/ISO 14971 medical devices risk management standard) for cybersecurity risk analysis. They draw the parallel in the term “asset”, which is typically used indirectly in security standards, to the term “harm”, which is used in ANSI/AAMI/ISO 14971. Asset refers to the subject in need of protection, whereas harm implies that the subjects to be protected are people, property, or the environment. Wu and Eagles base the assessment process on a causal chain analogy which breaks down all of the stages and factors in an attack.

Wu and Eagles’ (2016) risk assessment approach takes a similar but significantly more detailed approach than the framework proposed by MDPC (2014) . Some of the key differences are their elaboration of risk control considerations, their emphasis on linking cybersecurity risk to safety risk, and their guidance on documentation. However, there are differences between safety and cybersecurity risks within the context of medical devices. Safety risks, as defined in the ISO 14971 (2010) standard, relate specifically to unintended hazards that can result in potential harm to patients. Cybersecurity risks relate specifically to intentional threats to the confidentiality, integrity, and availability of information of a medical device. Cybersecurity risks could therefore have safety impacts if they represent a source of harm to a patient. The security risk controls are not different from safety controls, given that they both aim to reduce the likelihood or severity of an event. As described in the MDPC (2014) framework, the process of choosing controls is not trivial, especially when there are multiple control options. Wu and Eagles (2016) highlight that cybersecurity controls need to be balanced against usability, which is also articulated in the FDA’s guidance (FDA, 2016). An example of the tradeoff is the use of a password to access information on a medical device, which could result in a delay of treatment. The impact of security on usability is important to consider, but Wu and Eagles, as well as the FDA, frame it as a tradeoff. This view overlooks the fact that security controls can be implemented in a way that adds value to stakeholders. This value could potentially be added in usability, by adding a fingerprint reader for both authentication and turning on the display, peace of mind, by securing patients’ private information by encryption, or in other ways based on the type of the device. Wu and Eagles also stress the importance of articulating cybersecurity controls implemented by a manufacturer in order to communicate the value of these controls within their organization and to external stakeholders and externally. This articulation of controls is a challenge for many medical device manufacturers when dealing with regulatory bodies, customers, and other stakeholders (Denning et al., 2014). Wu and Eagles propose that cybersecurity assessment information should be structured as an assurance case to facilitate the review process. An assurance case is a communication method that organizes information in a systematic and structured way to articulate evidence and critical thinking, and it is traditionally applied to safety assessments (FDA, 2014). Wu and Eagles (2016) provide a template of a cybersecurity assurance case and propose that this assurance case can be used to articulate cybersecurity assessment to outside stakeholders, specifically to regulators, which has also been recommended by the FDA for infusion pump manufacturers.

The qualitative measure of risk probability is one of the major contributions of the MDPC framework and could also strengthen and simplify the risk assessment of Wu and Eagles. Wu and Eagles do not clearly articulate how a risk is graded or scored in order to determine whether or not the risk warrants further controls. The MDPC highlights that this is an existing challenge, which is why they present their qualitative security risk probability measure. Wu and Eagles do stress the importance of security usability, value, and articulation, which is only briefly mentioned by the MDPC. Together, these two frameworks provide a comprehensive approach to medical device cybersecurity risk mitigation and the consideration of the value that is being created.

Cybersecurity as a value proposition

As reported above, the MDPC (2014) risk assessment whitepaper recommends that medical device manufacturers should view cybersecurity as an asset, rather than an obligation. Related to this view, Denning and colleagues (2014) have applied the principles of value-sensitive design to security system design, and Tanev and colleagues (2015) propose an ecosystem value blueprint approach to including cybersecurity as part of the manufacturer's value proposition.

We define value as something that resonates with and is perceived as useful to a relevant stakeholder (Anderson et al, 2006). Beyond a mere listing of benefits, value must resonate with the stakeholder. The approach to cybersecurity system design taken by Denning and colleagues (2014) is based on the idea that the most effective design is the one that brings the most value to all stakeholders. They apply principles of value-sensitive design to first identify all stakeholders to a medical device and second to identify value dams and flows. They apply this approach to the security and access control system of implantable cardiac devices. The authors argue that medical device value is typically discussed in terms of security, privacy, and convenience, with other dimensions being overlooked. These value dimensions include human values such as trust, physical welfare, autonomy, and human dignity. With a more holistic approach to all stakeholder values, manufacturers could potentially produce more secure devices that deliver greater value. Maximizing the value created by security controls that are produced from the risk assessment process warrants this type of holistic analysis of value.

Some of Denning's earlier work applies value-sensitive design to the security and access control system of implantable cardiac devices based on the patient's perception of value (Denning et al., 2010). In Denning and colleagues' follow-up work (2014), they approached value from the perspective of 24 healthcare providers whom they asked to identify which one of six security design concepts they favoured most based on their value-sensitive design approach. The ultimate goal was to identify which security and access system design concept created the most value for stakeholders. The value-sensitive methodology used by Denning and colleagues is separated in two parts. In the first part, they identified direct and indirect stakeholders (healthcare providers) to implantable medical devices. In the second part, they conducted a workshop, which included a metaphor-generating session for key terms associated with medical devices and security, a "critiques and concerns" session about the security of implantable cardiac devices, and a question-based evaluation highlighting the security controls that the participant liked or disliked and would or would not recommend.

The goal of this approach was to gain an in depth understanding of what aspects of the different security and access control systems generated value (value flows), and what aspects generated concern (value dams).

One of the key takeaways from the metaphor generation stage is that different stakeholders conceptualize security concepts differently when translated into lay terms. It is important for researchers to analyze these metaphors and to understand whether they are positive or negative when conceptualized into laymen terms. For example, a metaphor for a medical device could be positive (e.g., life saver) or negative (e.g., site of infection).

By combining the information generated by the question-based evaluation of the security and access control systems, and the critiques and concerns, the researchers found that the fail-open/safety wristband was best received. This was chosen as the hypothetical design choice from the six options.

Tanev and colleagues (2015) emphasize the importance of medical device manufacturers leveraging cybersecurity as a valuable differentiator. They propose a cybersecurity value blueprint approach that visually identifies all relevant stakeholders as part of an ecosystem and all associated security vulnerabilities. These vulnerabilities could be manifested by the stakeholders themselves or could simply involve the stakeholder in the security risk scenario. In any case, once manufacturers identify all high-risk vulnerabilities, they develop a plan in collaboration with stakeholders to mitigate these risks. The value dimensions of these cybersecurity mitigation efforts are articulated through a visual blueprint of all stakeholders in the medical device ecosystem.

Proposed Framework for Cybersecurity Value Creation through Risk Mitigation

By synthesizing key contributions from our review of the literature, we propose an approach to integrating cybersecurity value propositions into the risk assessment process. The work of Tanev and colleagues (2015) provided the overall structure to identify key stakeholders and to resolve high-risk vulnerabilities by addressing the security value dimensions. The MDPC (2014) security assessment framework provides an approach to identifying these high-risk vulnerabilities that is specific to the context of medical devices. We also found that the consideration of value created by security risk controls needs to be integrated into the risk assessment process. The value created can be related to usability, privacy, safety or other factors. The value-sensitive design approach for security by Denning and colleagues (2014) provides a methodology in considering stakeholder values when presented with a set of risk control options. Figure 1 shows how these various sources were synthesized into our proposed framework for cybersecurity value creation through risk mitigation.

Our framework divides the risk mitigation process into four stages:

A. *Identify stakeholders and their ecosystem relationships:* All key stakeholders to the medical device manufacturer are identified, along with how they relate to each other within the ecosystem. Stakeholders can be grouped in one of the stakeholder groups. For example, intermediaries would represent anyone between the manufacturer and end customer, such as regulators, insurance companies, or healthcare providers. The overall goal is to identify all relevant stakeholders that could either affect, or be affected by, cybersecurity risks.

B. *Identify security risks to be addressed:* The proposed approach for identifying key risks is the MDPC (2014) medical device security assessment framework, which proposes a qualitative method for calculating the probabilities of security risks.

C. *Identify all possible risk controls:* For each security risk that requires mitigation, a list of risk controls is to be developed in collaboration with subject matter experts and stakeholders, taking relevant security standards and regulations into consideration.

D. *Choose risk controls using value-sensitive design:* When risk controls that meet all security requirements have been identified for a specific risk, a value-sensitive design approach is used to choose the control that generates the most value (or reduces the least amount of value) for relevant stakeholders. This approach requires a workshop with a sample of all relevant stakeholders. This involves ranking all risk controls for a risk and choosing the one that ranks the highest.

The goal of this framework is to integrate stakeholder identification (Tanev et al., 2015) and value-sensitive design (Denning et al., 2014) to a security risk assessment designed specifically for medical devices (MDPC, 2014). With this framework, we aim to produce a reproducible process for stakeholders to effectively address cybersecurity concerns while maximizing stakeholder value.

Applying the Framework to a Hypothetical Case

In this section, we illustrate how the framework could be applied using the hypothetical example of an insulin pump. An insulin pump is a small, portable device that helps people with diabetes regulate their blood glucose levels by continuously monitoring and delivering insulin into the bloodstream as needed to maintain target levels. Some insulin pumps have Internet connectivity to enable features such as improved monitoring, remote monitoring and record keeping, and software updates.

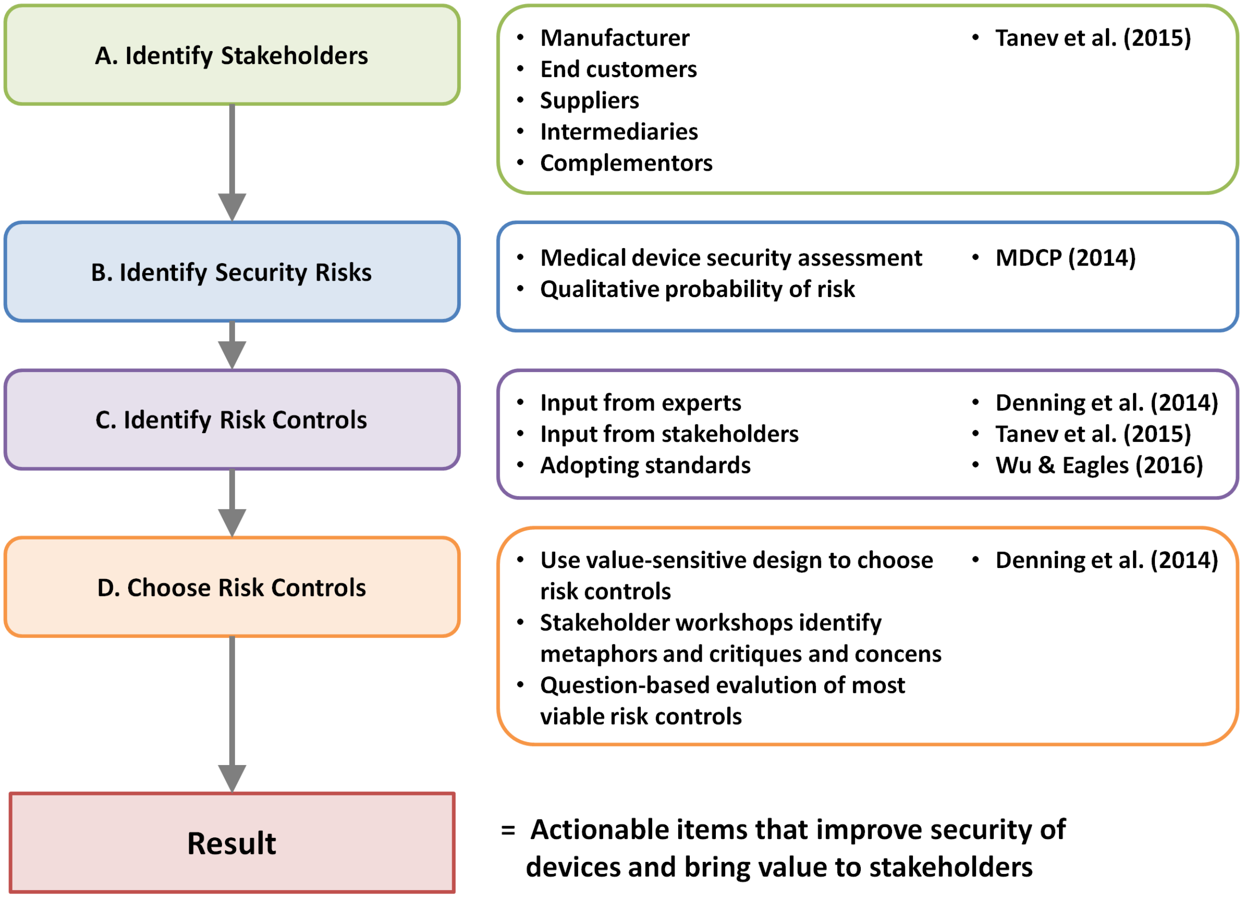
A. Identify Stakeholders
• Manufacturer
• End customers
• Suppliers
• Intermediaries
• Complementors
• Tanev et al. (2015)
B. Identify Security Risks
• Medical device security assessment
• Qualitative probability of risk
• MDCP (2014)
C. Identify Risk Controls
• Input from experts
• Input from stakeholders
• Adopting standards
• Denning et al. (2014)
• Tanev et al. (2015)
• Wu & Eagles (2016)
D. Choose Risk Controls
• Use value-sensitive design to choose risk controls
• Stakeholder workshops identify metaphors and critiques and concens
• Question-based evalution of most viable risk controls
• Denning et al. (2014)
Result
= Actionable items that improve security of devices and bring value to stakeholders

Figure 1. Framework for cybersecurity value creation through risk mitigation

During first three stages, the application of the framework to the insulin pump device gathers findings from the article by Paul, Kohno, and Klonoff (2011) who review key risks and possible controls for the specific case of an insulin pump. We used their article to derive existing knowledge from experts and incorporated it into the new framework. In practice, during the fourth stage, real workshops involving all relevant stakeholders would take place to identify stakeholder values and priorities. Here, given that our goal is simply to provide an example of how to approach this framework, we selected only a few key stakeholder groups and produced hypothetical data for stage four in order to illustrate the entire process.

Below, we organize the results of applying the framework to this case into subsections based the four stages of the framework, as outlined above and in Figure 1. We start by identifying stakeholders and their ecosystem relationships (Stage 1). We then identify the security risks that need to be addressed (Stage 2) and possible risk controls (Stage 3). Finally, we choose risk controls using the value-sensitive design approach (Stage 4).

A. Identify stakeholders and their ecosystem relationships
In the case of an insulin pump manufacturer, five key stakeholders were identified based on traditional stakeholders in a medical device ecosystem (Tanev et al., 2015):

1. *Manufacturers:* This group includes manufacturers of insulin pumps, or even different business units within the manufacturing organization. For example, the design team may have different goals than the engineers.

2. *Suppliers:* This group include both software and hardware suppliers.

3. *Complementors:* This group includes glucose monitor manufacturers, providers of insulin (the medicine used to treat diabetes), and database or cloud storage companies that work with the manufacturer.

4. *Intermediaries:* This group includes federal regulatory bodies that dictate the requirements and safety guidelines for devices as well as approve them for market release; Insurance companies that may fund the purchase of these devices for users; distributors of medical devices (e.g., hospitals or other agencies providing insulin pumps to patients); and healthcare providers (doctors and other practitioners who interact with the device but are not the end user).

5. *Users:* This group includes patients that have diabetes and use insulin pumps to regulate their glucose levels.

B. Identify security risks to be addressed

The insulin pump system under review (Paul et al., 2011) included a series of components: the insulin pump, a continuous glucose management system, a blood glucose monitor, and other devices (e.g., a mobile phone or computer). Two types of common security risks were chosen as examples given the type of insulin pump under review (Paul et al., 2011):

- **Risk 1:** Ensuring that remote control is only available to pre-approved individuals (i.e., the patient or their doctor) to maintain the integrity of system settings, to address system communication availability, and to ensure the software has not been altered without consent.

- **Risk 2:** Maintaining the integrity and confidentiality of data.

C. Identify all possible risk controls

Given the security risks, the manufacturer must decide what control to apply, if any. The following options for controlling the risks were identified:

Risk 1: Ensuring remote control is only accessed by pre-approved individuals

1. *Fail-safe physical interface:* Enables patient control when wireless communication fails (i.e., is lost, stolen, or interrupted).

2. *Wireless-enabling button:* Enables wireless communication on the device for short periods of time.

3. *Wireless-disabling switch:* Disables remote control, for example to start or stop insulin delivery when data is compromised or someone has interfered with the device.

Risk 2: Maintaining the integrity and confidentiality of data

1. *Encryption with button:* Along with encryption of data that follows the advanced encryption standard (Selent, 2010), a tactile button allows physicians to access the data in emergency situations.

2. *Encryption with infrared port:* Along with encryption of data that follows the advanced encryption standard (Selent, 2010), an infrared port interfaces with a data reader.

D. Choose risk controls using value-sensitive design with stakeholders

Following Denning and colleagues (2014), we identified stakeholders and simulated the steps suggested by the value-sensitive design process. The relevant stakeholders for this case study are: medical device manufacturers, patient's (end-users), and healthcare providers. Tables 1, 2, and 3 show the outcomes of metaphor generation and concern collection, question-based evaluation, and ranking and selection of risk controls for Risk 1. Below, we outline the steps followed in this stage for Risk 1 (Ensuring that remote control is only accessed by pre-approved individuals):

1. *Metaphor generation:* Ask stakeholders to generate metaphors for "insulin pumps" and "remote control access and security controls".

2. *Critiques and concerns:* Ask stakeholders to voice their concerns, fears, or insecurities about remote control of insulin pump technology.

3. *Question-based evaluation:* Ask stakeholders a series of questions (see Denning et al., 2014) about which concepts they like and dislike, which they would choose or recommend, etc.

4. *Rank and select risk controls:* Qualitatively analyze items 1 and 2 and quantitatively analyze item 3.

Table 1. Stakeholder metaphor generation and collection of concerns for Risk 1

Stakeholder	Fail-Safe Physical Interface	Wireless-Enabling Button	Wireless-Disabling Switch
Patient	• Might make device bigger and harder to wear • Pushing buttons accidentally	• Vulnerable if pushed by accident • Caregivers might not know that wireless needs to be enabled in emergencies	• Battery might be drained if turned on by accident • Caregivers might not know that wireless needs to be enabled in emergencies
Healthcare Provider	• Patients pushing buttons accidentally • Patients more likely to lose their programming module	• Not automatically clear to emergency caregivers that they need to press a button	• Not automatically clear to emergency caregivers that they need to press a button
Manufacturer	• More expensive to develop physical control interface	• Battery drains if patient accidentally presses button repeatedly or holds it down	• No concerns

Table 2. Stakeholder question-based evaluation for Risk 1

Stakeholder	Like	Dislike	Recommend	Do Not Recommend
Patient 1	• Fail-safe interface • Wireless-disabling switch	• None	• Fail-safe interface • Wireless-disabling switch	• None
Healthcare Provider	• Fail-safe interface • Wireless-enabling button • Wireless-disabling switch	• None	• Fail-safe interface • Wireless-disabling switch	• None
Manufacturer	• Wireless-enabling button • Wireless-disabling switch	• Fail-safe interface	• Wireless-enabling button • Wireless-disabling switch **Why:** Controlled access to programming of device.	• Fail-safe interface **Why:** Redundant feature that does not provide increased security against attacks.

Table 3. Ranking and selection of risk control for Risk 1. (Percentages are independent of each other.)

Risk Control	Like	Dislike	Recommend	Do Not Recommend
Fail-Safe Interface	66%	33%	66%	33%
Wireless-Enabling Button	66%	0%	33%	0%
Wireless-Disabling Switch	100%	0%	100%	0%

Table 4. Stakeholder metaphor generation and collection of concerns for Risk 2

Stakeholder	Encryption with Button	Encryption with Infrared Port
Patient	• No concerns	• Emergency staff may not have infrared device on hand • Someone with a stolen infrared device could read the data
Healthcare Provider	• No concerns	• Additional hardware necessary for emergency staff
Manufacturer	• Potential backdoor for decrypting information if tactile button is directly on the device • Encryption keys now need to be managed with partners	• Additional hardware required • Novel technology within this space • Encryption keys now need to be managed with partners

Table 5. Stakeholder question-based evaluation for Risk 2

Stakeholder	Like	Dislike	Recommend	Do Not Recommend
Patient 1	• Tactile button	• None	• Tactile button **Why:** Simple implementation and easy no hardware necessary.	• Infrared **Why:** Vulnerable if someone steals infrared reader
Healthcare Provider	• Tactile button	• Infrared port	• Tactile button **Why:** Doesn't require additional hardware for emergency staff	• Infrared port **Why:** Requires additional hardware for emergency staff
Manufacturer	• Tactile button	• Infrared port	• Tactile button **Why:** Simple and secure implementation both technologically and for emergency staff and caregivers	• Infrared port **Why:** Requires additional hardware for emergency staff, and additional resources to develop designated reader

Table 6. Ranking and selection of risk control for Risk 1. (Percentages are independent of each other.)

Risk Control	Like	Dislike	Recommend	Do Not Recommend
Encryption with Button	100%	0%	100%	0%
Encryption with Infrared Port	0%	66%	0%	100%

Tables 4, 5, and 6 show the outcomes of metaphor generation and concern collection, question-based evaluation, and ranking and selection of risk controls for Risk 2. Below, we outline the steps followed in this stage for Risk 2 (Maintaining the integrity and confidentiality of data):

1. *Metaphor generation:* Ask stakeholders to generate metaphors for "insulin pumps" and "patient glucose data".

2. *Critiques and concerns:* Ask stakeholders to voice their concerns, fears, or insecurities about the data integrity of glucose monitors and privacy of data in insulin pump technology.

3. *Question-based evaluation:* Ask stakeholders a series of questions (see Denning et al., 2014) about which concepts they like and dislike, which they would choose or recommend, etc.

4. *Rank and select risk controls:* Qualitatively analyze items 1 and 2 and quantitatively analyze item 3.

Discussion

In the hypothetical example, the results for Risk 1 (Ensuring remote control is only accessed by pre-approved individuals) show that the risk control that brought the most value to all three of the selected stakeholders was incorporating a switch to disable and enable wireless communication in the insulin pump. For Risk 2 (Maintaining the integrity and confidentiality of data), the risk control that was preferred by the three selected stakeholders was that of encrypting data with a tactile button instead of using an infrared port.

Our aim with this hypothetical application of the framework is to show how risk controls can be chosen in a way that considers the perceived value notion from a variety of stakeholders. In this illustrative example, we do not suggest that the stakeholders selected, the risks described, or the mitigation controls offered are best suited to making insulin pumps cybersecure. We acknowledge that there may be many more stakeholders, risks, and controls need to be accounted for when fully assessing insulin pumps and medical devices at large.

Our contribution is to showcase (at a small scale) how the proposed framework is applicable to a particular medical device. With this framework, we aim to make it easier to:

- Consider key stakeholders when evaluating and addressing cybersecurity risks in medical devices.

- Improve the safety of all stakeholders that are affected by these medical devices.

- Provide manufacturers with a framework that provides actionable items on how to improve their device's security in a way that brings value to their stakeholders (including themselves).

- Transform cybersecurity from a regulatory obligation into an asset (competitive advantage) for manufacturers.

- Evolve the medical device industry from its current position into one that puts cybersecurity at the forefront of its priorities.

Conclusion

In this article, we developed the key concepts necessary to articulate cybersecurity as a value proposition. Based on a review of the literature on the current landscape of medical device cybersecurity, on medical device risk mitigation, and on cybersecurity as a value proposition, we proposed a framework that integrates value articulation with the risk assessment and mitigation process. This framework takes into account the unique aspects of medical device security, the benefits of considering value creation when choosing risk controls, and the importance of perceiving value through the perspective of multiple stakeholders. The hypothetical case study of an insulin pump provided a practical example of applying the framework. It identified stakeholders, risks, potential mitigations, and the value that can be created for stakeholders for each mitigation. We used available resources to hypothetically analyze and choose risk mitigation options based on the perspectives of several key stakeholders. This framework is intended to be applied to any medical device with the purpose of articulating the value generated by cybersecurity within the context of medical device risk assessment.

About the Authors

Aida Alvarenga Castillo is a Master's student in the Technology Innovation Management program at Carleton University in Ottawa, Canada. Aida undertook her undergraduate studies at McGill University in Montreal, Canada, with a focus on Economics, Business Management, and Political Science. She has experience in the financial industry for well-established banks, in a business development role for a technology startup, and as an entrepreneur in launching her own family food business. Within the field of technology innovation, Aida's main interests are in financial technologies (FinTech) and innovation within the financial industry.

George Tanev is a Master's student in the Technology Innovation Management program at Carleton University in Ottawa, Canada. George holds a Master's of Science degree in Medicine and Technology from the Technical University of Denmark and a Bachelor of Engineering in Biomedical and Electrical Engineering from Carleton University. George has experience in the medical device industry and the air navigation services industry. His interests are in technology entrepreneurship, cybersecurity, medical device product development, signal processing, and data modelling.

References

American Hospital Association. 2014. A Message from the AHA: Considering Unique Cybersecurity Risks of Medical Devices Is Critical. *AHA News,* December 4, 2015. Accessed April 10, 2017: http://www.aha.org/advocacy-issues/141204cybersecurityrisksnews.shtml

Anderson, J., Narus, J., & van Rossum, W. 2006. Customer Value Propositions in Business Markets. *Harvard Business Review,* 84(3): 90–99.

Buntz, B. 2011. Insulin Pump Hacking: Sensationalism or Legitimate Threat? *Medical Device and Diagnostic Industry,* August 12, 2011. Accessed April 10, 2017: http://www.mddionline.com/blog/devicetalk/insulin-pump-hacking-sensationalism-or-legitimate-threat

Burns, A. J., Johnson, M. E. P., & Honeyman, P. 2016. A Brief Chronology of Medical Device Security. *Communications of the ACM,* 59(10): 66–72. http://dx.doi.org/10.1145/2890488

Denning, T., Borning, A., Friedman, B., Gill, B. T., Kohno, T., & Maisel, W. H. 2010. Patients, Pacemakers, and Implantable Defibrillators: Human Values and Security for Wireless Implantable Medical Devices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems:* 917–926. New York: Association for Computing Machinery.

Denning, T., Kramer, D. B., Friedman, B., Reynolds, M. R., Gill, B., & Kohno, T. 2014. CPS: Beyond Usability: Applying Value Sensitive Design Based Methods to Investigate Domain Characteristics for Security for Implantable Cardiac Devices. In *Proceedings of the 30th Annual Computer Security Applications Conference: ACSAC 2014:* 426–435. New York: Association for Computing Machinery. http://dx.doi.org/10.1145/2664243.2664289

Farrel, E., & Hanet, J. 2016. *Cybersecurity and Medical Devices: Electronic Medical Data Increases Product Liability Risk For Medical Device Manufacturers.* Toronto: Gowling WLG.

FBI. 2014. *FBI Cyber Division Bulletin: Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions.* Washington, DC: Federal Bureau of Investigation. https://publicintelligence.net/fbi-health-care-cyber-intrusions/

FDA. 2014. *FDA Case Study: An Infusion Pump Company Considers Risk Assessment and Mitigation.* Silver Spring, MD: U.S. Food and Drug Administration

FDA. 2016. *Draft Guidance: Postmarket Management of Cybersecurity in Medical Devices.* Silver Spring, MD: U.S. Food and Drug Administration

Harris, P. 2014. *The Prognosis for Healthcare Payers and Providers: Rising Cybersecurity Risks and Costs.* London: PricewaterhouseCoopers.

ISO. 2007. *ISO 14971: Medical Devices-Application of Risk Management to Medical Devices.* Geneva: International Organization for Standards.

Maisel, W. H., & Kohno, T. 2010. Improving the Security and Privacy of Implantable Medical Devices. *The New England Journal of Medicine,* 362(13): 1164–1166. http://dx.doi.org/10.1056/NEJMp1000745

MDPC. 2014. *Security Risk Assessment Framework for Medical Devices: A Medical Device Privacy Consortium White Paper.* Washington, DC: Medical Device Privacy Consortium.

Paul, N., Kohno, T., & Klonoff, D. C. 2011. A Review of the Security of Insulin Pump Infusion Systems. *Journal of Diabetes Science and Technology,* 5(6): 1557–1562. https://doi.org/10.1177/193229681100500632

Filkins, B. 2014. *Health Care Cyberthreat Report: Widespread Compromises Detected, Compliance Nightmare on Horizon.* Bethesda, MD: SANS Institute.

Selent, D. 2010. Advanced Encryption Standard. *Rivier Academic Journal,* 6(2): 1–14.

Tanev, G., Tzolov, P., & Apiafi, R. 2015. A Value Blueprint Approach to Cybersecurity in Networked Medical Devices. *Technology Innovation Management Review,* 5(6): 17–25. https://timreview.ca/article/903

Williams, P. A. H., & Woodward, A. J. 2015. Cybersecurity Vulnerabilities in Medical Devices: A Complex Environment and Multifaceted Problem. *Medical Devices: Evidence and Research,* 8: 305–316. https://doi.org/10.2147/MDER.S50048

Wu, F., & Eagles, S. 2016. Cybersecurity for Medical Device Manufacturers: Ensuring Safety and Functionality. *Biomedical Instrumentation and Technology,* 50(1): 23–34. http://dx.doi.org/10.2345/0899-8205-50.1.23

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

cc BY

Keywords: cybersecurity, risk assessment, framework, value-sensitive design, medical devices, value propositions