A Value Blueprint Approach to Cybersecurity in Networked Medical Devices

George Tanev, Peyo Tzolov, and Rollins Apiafi

> *"When the value proposition requires multiple elements to converge, you need an approach that will allow you to assess alternative configurations and generate shared understanding and agreement among the partners as to how these elements should come together. … Left unarticulated, contradicting visions don't conflict until after commitments are made and pieces are brought together. But when the strategy meets reality, details become disasters."*
>
> Ron Adner
> Professor of Strategy and Entrepreneurship
> In *The Wide Lens*

Cybersecurity for networked medical devices has been usually "bolted on" by manufacturers at the end of the design cycle, rather than integrated as a key factor of the product development and value creation process. The recently released cybersecurity guidelines by the United States Food and Drug Administration (FDA) offer an opportunity for manufacturers to find a way of positioning cybersecurity as part of front-end design, value creation, and market differentiation. However, the technological architecture and the functionality of such devices require an ecosystem approach to the value creation process. Thus, the present article adopts an ecosystem approach to including cybersecurity as part of their value proposition. It extends the value blueprint approach suggested by Ron Adner to include an additional dimension that offers the opportunity to define: the potential locations of cybersecurity issues within the ecosystem, the specific nature of these issues, the players that should be responsible for addressing them, as well as a way to articulate the added cybersecurity value as a competitive differentiator to potential customers. The value of the additional blueprint dimension is demonstrated through a case study of a representative networked medical device – a connected insulin pump and continuous glucose monitor.

Introduction

Concerns over the state of medical device cybersecurity have become a topic of intense public discussion after cases such as the hacking of connected insulin pumps by researchers to deliberately deliver lethal insulin doses (Healey et al., 2015). Following these cases and similar others, the United States Department of Homeland Security began investigating two dozen medical devices for potential security vulnerabilities and the Food and Drug Administration released guidance to manufacturers for establishing cybersecurity management strategies for their medical devices (FDA, 2014). Experts have come forward stating that the medical device industry is significantly behind other industries in terms of its ability to both articulate and address cybersecurity issues (Fu & Blum, 2014). Also, with networked medical devices increasingly joining the Internet of Things, security will take a much more prominent role as risks to patient health, safety, and data privacy continue to grow (Wirth, 2011). Between 2013 and 2014, the increase in information security breaches for healthcare facilities was almost double that of other industries (Harries, 2014), and with networked devices moving from hospital networks to home networks, new threats are bound to emerge. With public and regulatory pressure rising, manufacturers are spending more time, effort, and resources on im-

A Value Blueprint Approach to Cybersecurity in Networked Medical Devices

George Tanev, Peyo Tzolov, and Rollins Apiafi

proving cybersecurity. At the same time, the existing ways of articulating customer value in the medical device industry do not seem to allow for a differentiation in terms of cybersecurity benefits. These growing cybersecurity concerns and the lack of cybersecurity benefit-articulation highlight the growing need for manufacturers to begin utilizing security as a market value and differentiator.

One of the main criticisms of medical device cybersecurity is that security tends to be added on at the end of the development process, instead of being "baked in" from the start as part of the design phase (Shah, 2015). This late consideration highlights a key problem in the way many manufacturers approach security. Security is perceived as a hurdle to jump over, rather than a key part of the value proposition that can be used as a market differentiator. With an estimated unit sale of networked medical devices to increase by five times from 2012 to 2018 (Healey et al., 2015), increased security efforts are becoming a necessity. These additional efforts provide an opportunity for manufacturers to add value and differentiate themselves in such a growingly competitive market.

Networked medical device are predominately software-based medical devices that are connected to networks involving patients, healthcare organizations, medical specialists, and other service providers. In most of the cases, their operation requires wireless connectivity and multiple interoperations including the sharing of clinical information and controlling other medical devices and systems as well as nonmedical equipment (e.g., routers and servers) and software. Complex networked systems, including medical devices, have now become common, and with this added sophistication, new behaviours and unexpected consequences have begun to appear that are outside the control of the medical device manufacturer (Rakitin, 2009). A report by the Atlantic Council assessing the benefits and risks of healthcare systems in the Internet of Things identifies four main types of networked medical devices (Healey et al., 2015):

1. Embedded devices (e.g., pacemakers)

2. External devices (e.g., insulin pumps)

3. Stationary devices (e.g., networked infusion pumps)

4. Consumer products for health monitoring (e.g., FitBit or Nike Fuel band)

Consumer products for health monitoring are sometimes not discussed with medical devices because they do not require regulatory approval (i.e., they do not fit the definition of a medical device in most regions), but the regulatory framework around them has been under intensive discussion and is likely to change in the coming years (Healey et al., 2015). We will therefore include them as part of our discussion. The rest of the article is organized as follows. We will next describe the specifics of cybersecurity issues in the medical device sector. Then, we will summarize the key points of the value blueprint approach (Adner, 2012) and suggest an additional dimension that addresses cybersecurity issues. The next section contains an application of the cybersecurity blueprinting approach to a specific case consisting of a connected insulin pump and continuous glucose monitor. Finally, we conclude by articulating the key contributions of the article and offering suggestions for future research.

Cybersecurity for Medical Devices

Cybersecurity for medical devices has traditionally been seen as a tradeoff to usability, and therefore as a potential challenge for market value. Even the FDA emphasizes that improved security should be counter-balanced against reduced usability (FDA, 2014). This tradeoff is true in certain cases, but an overemphasis would lead to missing the opportunity to articulate security as add-on value. For example, securing an insulin pump with a password for daily tasks is cumbersome and patients will most likely use a simple password or find a way around it. In another example, encrypting wireless communication of a pacemaker would improve security while also adding value to the patients because they would be safe from malicious threats. With the medical device market already being highly competitive, not articulating security improvements as an add-on value to the patient is a missed opportunity.

In order to articulate the created cybersecurity value, manufacturers of networked medical devices must first change the way they look at the security landscape. Networked medical devices should be seen as a platform in a diverse ecosystem of stakeholders (Shah, 2015), which is similar to mobile communication platforms in the automotive industry. The ecosystem depends on numerous software and hardware systems, some of which have been developed by suppliers and must be integrated using “glue code” so that they can function together (Amin et al., 2015). The integration increases the

A Value Blueprint Approach to Cybersecurity in Networked Medical Devices

George Tanev, Peyo Tzolov, and Rollins Apiafi

chances of introducing cybersecurity vulnerabilities at the interfaces between the different software and electronics systems. The glue code problem can be framed as a knowledge coordination problem between manufacturers and suppliers of networked medical devices. For example, a portable heart monitor communicates to a mobile device, which displays relevant health data and also uploads it to a server for additional post-processing and analytics. Thus, vulnerabilities could be at another location in the ecosystem and not in the device itself, which requires a high degree of knowledge coordination between manufacturers, suppliers, co-innovators, and adoption chain partners. To highlight security as part of the value proposition, we must move from a product-centric approach to an ecosystem-driven approach to security. This approach would allow manufacturers to:

1. *Identify key stakeholders* in the ecosystem together with all associated cybersecurity vulnerabilities.

2. *Create a plan* to address the highest risk cybersecurity vulnerabilities in collaboration with stakeholders.

3. *Articulate the value dimensions* associated with the security efforts to the relevant stakeholders.

4. *Improve security* by innovating the ecosystem.

This article aims to address these points by adapting a value blueprint approach to cybersecurity.

A Value Blueprint Approach to Cybersecurity

The value blueprint approach proposed by Ron Adner in his book *The Wide Lens* (Adner, 2012) takes an ecosystem approach to value creation. Translating a specific value proposition into a value blueprint makes it possible to identify and visualize the multiple dependencies within the ecosystem as well as deal with situations where multiple elements need to converge and a shared understanding between stakeholders is required. Adner suggests an approach to value blueprint development including the following steps:

1. Identify your end customer.

2. Identify your own project.

3. Identify your suppliers.

4. Identify your intermediaries.

5. Identify your complementors.

6. Identify the risks in your ecosystem (Red=Unmitigable risk; Yellow=Mitigable risk; Green=Acceptable risk):
    a. Level of co-innovation risk
    b. Level of adoption risk

7. For every partner whose status is not green, understand the problem and suggest a viable solution.

8. Update blueprint on a regular basis.

The risk levels in Adner's blueprint follow a green, yellow and red "traffic light" approach. It focuses solely on the interplay between co-innovation and adoption chain risks in managing value creation and articulating the market value of the product. For co-innovation risk, green means that the stakeholder is ready and in place, yellow means that they are in place, but do there is no plan, and red means that they are not in place. For adoption risk, green means that partners are eager to participate and see the benefit of their involvement, yellow means that partners are neutral but open to involvement, and red means that they prefer the status quo and are not willing to be involved. A red light would indicate that more substantial changes need to be made in the blueprint, such as a change in partners.

The blueprint could be used however to analyze an additional dimensions of value, and in particular, the value of cybersecurity in networked medical devices. In this way, a blueprint would allow for an explicit analysis of security vulnerabilities from an ecosystem perspective. It would also allow for using all value blueprint tools focusing on evolving the ecosystem to enhance the security of networked medical devices, as well as for articulating the newly created cybersecurity value for a better market differentiation.

The cybersecurity blueprint can be generated by the process proposed by Adner, with minor changes in the way of approaching risks in the ecosystem. For the sake of simplicity, we will assume that all other aspects of value for all stakeholders have been already articulated, and that the risk we are assessing in our value blueprint is strictly cybersecurity risk. This assumption requires some changes to Adner's steps, mostly after step 5. The steps for developing the cybersecurity blueprint for a networked medical device are as follows:

A Value Blueprint Approach to Cybersecurity in Networked Medical Devices

George Tanev, Peyo Tzolov, and Rollins Apiafi

1. Identifying your end customer, your own project, your suppliers, your intermediaries, complementors together with their specific cybersecurity concerns, if any (steps 1–5 in Adner's approach).

2. Identify the locations of security risks in your ecosystem by taking into account any concerns that were explicitly articulated by the different stakeholders (Red=Unmitigable risk; Yellow=Mitigable risk; Green=Acceptable risk).

3. For every location in the blueprint understand the co-innovation (i.e., technical) and adoption aspects of the problems and prioritize them by using an appropriate cybersecurity risk-analysis framework into green (acceptable), yellow (mitigable), and red (unmitigable) risks levels.

4. Develop a risk management action plan to address the highest priority risks (yellow and red) with a viable security risk mitigation measure to make the risk level acceptable (green) and add it to the blueprint as appropriate.

5. Use the cybersecurity blueprint to articulate the value created by your efforts and the next steps in your cybersecurity management plan in a way that you could differentiate in the marketplace.

6. Update and innovate the cybersecurity blueprint on a regular basis.

The changes would allow for the localization of cybersecurity risks within the ecosystem, subsequently taking adequate action to mitigate the risk, and using the blueprint to articulate the security efforts and the value added. As in Adner's blueprint, the levels of risk are represented by red (does not allow for delivery of end value), yellow (requires additional efforts to mitigate risk) or green (does not require additional efforts). The adoption of a meaningful risk analysis method is crucial for the implementation of the cybersecurity blueprint approach. Even though it is out of the scope of the present article, we could mention some points regarding the application of risk analysis methods as part of an ecosystem cybersecurity approach for networked medical devices. First, known risk analysis methods such as Failure Mode and Effect Analysis (FMEA), or Health FMEA (HFMEA) (Shaqdan et al., 2014) do not seem to grasp the full scope of the cybersecurity risks that can be addressed in our ecosystem approach. Approaches based on FMEA-type risk analysis typically address risks due to design failures rather than to malicious attacks. Cybersecurity risk analysis in an ecosystem context needs to address issues associated with intentional malicious agents attacking or interfering with networked medical devices. Secondly, the risk analysis for networked medical devices should focus on the cyber-resilience of the ecosystem, or in other words, the ability to withstand cyber-events or cyber-attacks. Cyber-resilience risks in the context of networked medical devices relate to the control of access, the quality/validity of information, and to the continuity of operation (Boyes, 2015). Risks must also be analyzed within the context of the full lifecycle of networked medical devices and with respect to all relevant stakeholders. In other words, what are the risks related to cases of future, unforeseen cyber-vulnerabilities such as the case of the Heartbleed incident (Krebs, 2014). What is important to point out is the need to move beyond two-dimensional definitions of risk (i.e., probability of harm occurring and severity of the harm once it occurs), which might oversimplify the ability of a medical device company to proactively manage cybersecurity and cyber-resilience risks. Thirdly, the product benefit or utility should be also added to the risk score as a relevant factor. Its addition could provide a higher degree of sophistication of the cybersecurity risk management logic. For example, a risk that remains unacceptable after performing all practicable cybersecurity mitigation measures may actually be tolerable if the device's clinical benefit or medical significance outweighs its residual risks. The next section offers an example case of the application of the value blueprint approach to the analysis of the cybersecurity issues associated with Animas insulin pumps.

Case Study: The Animas Vibe Insulin Pump Cybersecurity Value Blueprint

The described cybersecurity value blueprint was hypothetically applied from the perspective of the manufacturer of the already marketed Animas Vibe Insulin Pump (tinyurl.com/pavb3lp). The Animas insulin pump is used with the G4 PLATINUM Continuous Glucose Monitor made by DEXCOM (tinyurl.com/qda8x5x). The added value of security for the insulin pump has yet to be articulated by manufacturers. In most of the marketing materials, there is little mention of the security of the device, even though the vulnerabilities of insulin pump security have been extensively documented by researchers and presented in the media. The cybersecurity value blueprint would clearly articulate the ecosystem efforts made for improving cybersecurity and provide an additional opportunity for market differentiation.

A Value Blueprint Approach to Cybersecurity in Networked Medical Devices

George Tanev, Peyo Tzolov, and Rollins Apiafi

The Animas insulin pump is an example of the direction towards connected and personal medical devices, which are gaining platform-like properties as they are integrated with other devices and services. The insulin pump is not directly connected to a network, but is connected wirelessly to the glucose monitor, and can transfer data to a healthcare professional via the diasend web service (www.diasend.com/us/) by connecting the pump to a computer via USB or infrared connection. Future networked medical devices will send data to cloud web services wirelessly.

To begin building the cybersecurity blueprint, we first need to establish all of the key elements of the ecosystem. This process is addressed in the first five steps for generating the blueprint. The elements are listed in Table 1.

Following step 2, the cybersecurity blueprint for the Animas insulin pump was generated, as represented in Figure 1.

The security concerns that are highlighted in Figure 1 are graded at the level of "yellow risk" and therefore should be mitigated. The concerns are described below with potential mitigations that could be implemented and their added value reflected in the blueprint:

1. *Cybersecurity management practices of the insulin pump manufacturer:* The manufacturer has to follow a process for assessing and addressing security risks within the device.

   Mitigation: Implementing a cybersecurity management strategy and an open disclosure policy for device security vulnerabilities that have been found by external parties.

2. *Cybersecurity management practices of the continuous glucose monitor manufacturer:* The manufacturer of the Animas pump has limited power over the cybersecurity management practices of their partner device manufacturer. They can assess and address any security issues in the integration process of the two devices.

   Mitigation: None – To be addressed at other locations in the blueprint.

3. *Security implications in the integration of the two devices:* Combining two individual products into a package raises potential security concerns because security for the integrated product was not planned in the initial design process.

Table 1. Key ecosystem elements to be included in cybersecurity value blueprint of Animas insulin pump

Element	Description
End Customer	Patient directly or patient via insurance reimbursement
Your Project	Integrated insulin pump with continuous glucose monitor (from the perspective of insulin pump manufacturers)
Suppliers	Insulin pump mechanical components, hardware, and software
Intermediaries	Regulatory bodies, medical professionals, insurance companies
Complementors	Manufacturer of continuous glucose monitor (DEXCOM) and diasend web service provider

   Mitigation: A third-party firm can be utilized for security tests of the integrated product. This approach can also address vulnerability number 3 from Figure 1.

4. *Regulatory requirements and recommendations of cybersecurity:* The requirements that are set forth by the regulatory body in the region where the product is marketed are relevant for licensing the device. In many regions, there are still no explicit regulatory requirements for cybersecurity.

   M*itigation:* Many of the mitigation steps that are taken for the other vulnerabilities ensure that the manufacturer is not simply fulfilling the bare minimum regulatory requirements, but taking a proactive approach to cybersecurity.

5. *The role and impact of medical professionals on device security:* Medical professionals will most likely play an instructional role with patients and have access to sensitive patient data through web services. It is important that medical professionals are security conscious when dealing with networked devices.

   Mitigation: Training or instructions of good security practices with the device and accessing patient data.

6. *The role and impact of patients/users on device security:* The way that patients operate the device could also risk its security. It is important that patients

A Value Blueprint Approach to Cybersecurity in Networked Medical Devices

George Tanev, Peyo Tzolov, and Rollins Apiafi

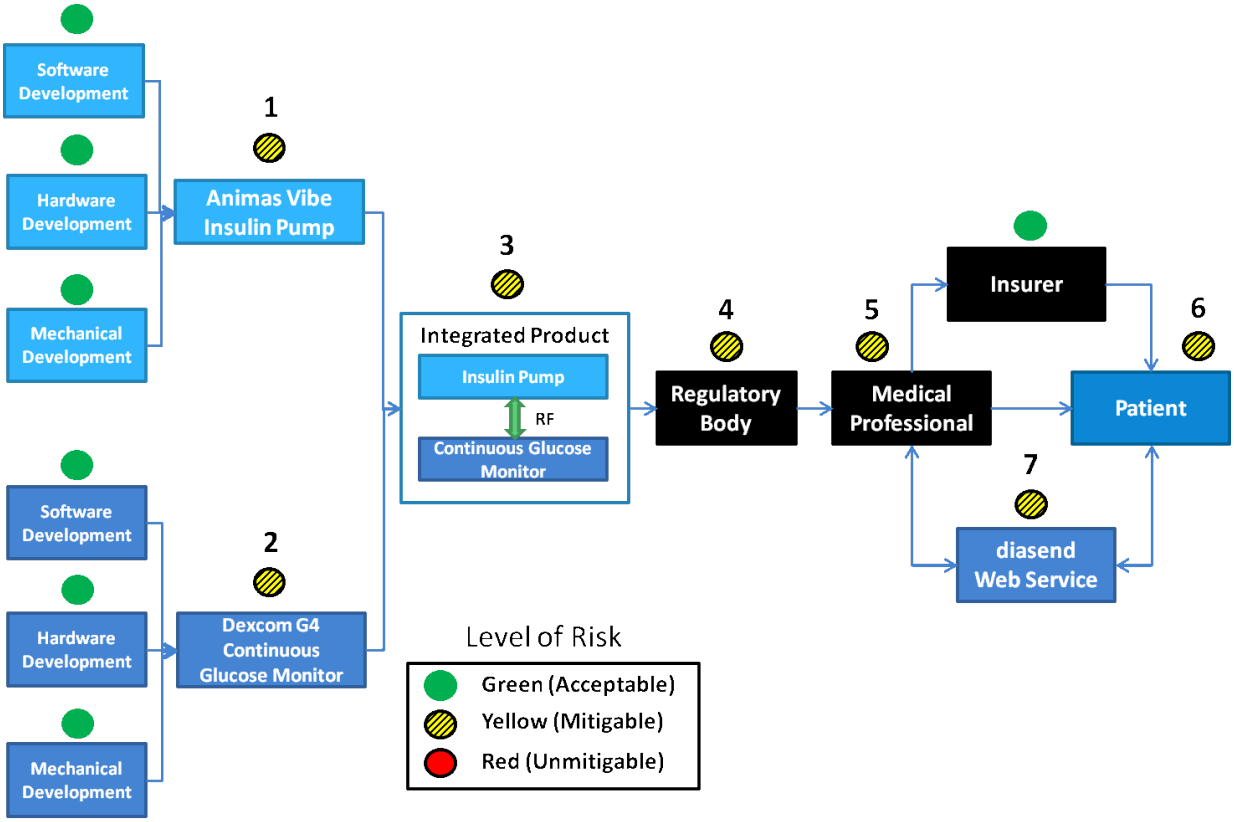

Figure 1. Cybersecurity blueprint for the Animas Vibe insulin pump with numbered locations that have cybersecurity risk levels that need to be mitigated (yellow)

know how to use their device securely and what the risks of compromised security are (e.g., privacy and health risks).

Mitigation: Training or instructions in good cybersecurity practices with the device and clear articulation of the manufacturer's open disclosure policy if they should find any security flaws.

7. *Transferring data between patients and medical professionals over the Internet:* Data that is transmitted from the insulin pump to a computer to upload data to the patient's physician could be susceptible to unauthorized access of the patient's health information. The data can currently be transferred by USB or by infrared data transfer.

   Mitigation: The manufacturer has already made a good choice in using diasend web services that specialize in transferring data between patients and physicians. They also should ensure that any infrared information is encrypted when being transferred.

It is evident that the cybersecurity of networked medical devices is the responsibility of many different stakeholders. When cybersecurity improvement measures are taken in the vulnerable parts of the ecosystem, articulating the value of these efforts is done visually in the blueprint. This type of visual representation of the security value dimension allows stakeholders and end customers to see a manufacturer's comprehensive efforts and highlights the added value and differentiation from competitors. The cybersecurity mitigations have been added to an amended cybersecurity blueprint in Figure 2. The risks that were formerly yellow (mitigable) have been shifted to green (acceptable) following the mitigations that were applied.

Contribution

The key contribution of this article is to extend the value blueprint approach (Adner, 2012) to address the additional value dimension of cybersecurity, in order to articulate cybersecurity value as a way for medical device companies to differentiate in the marketplace.

A Value Blueprint Approach to Cybersecurity in Networked Medical Devices

George Tanev, Peyo Tzolov, and Rollins Apiafi

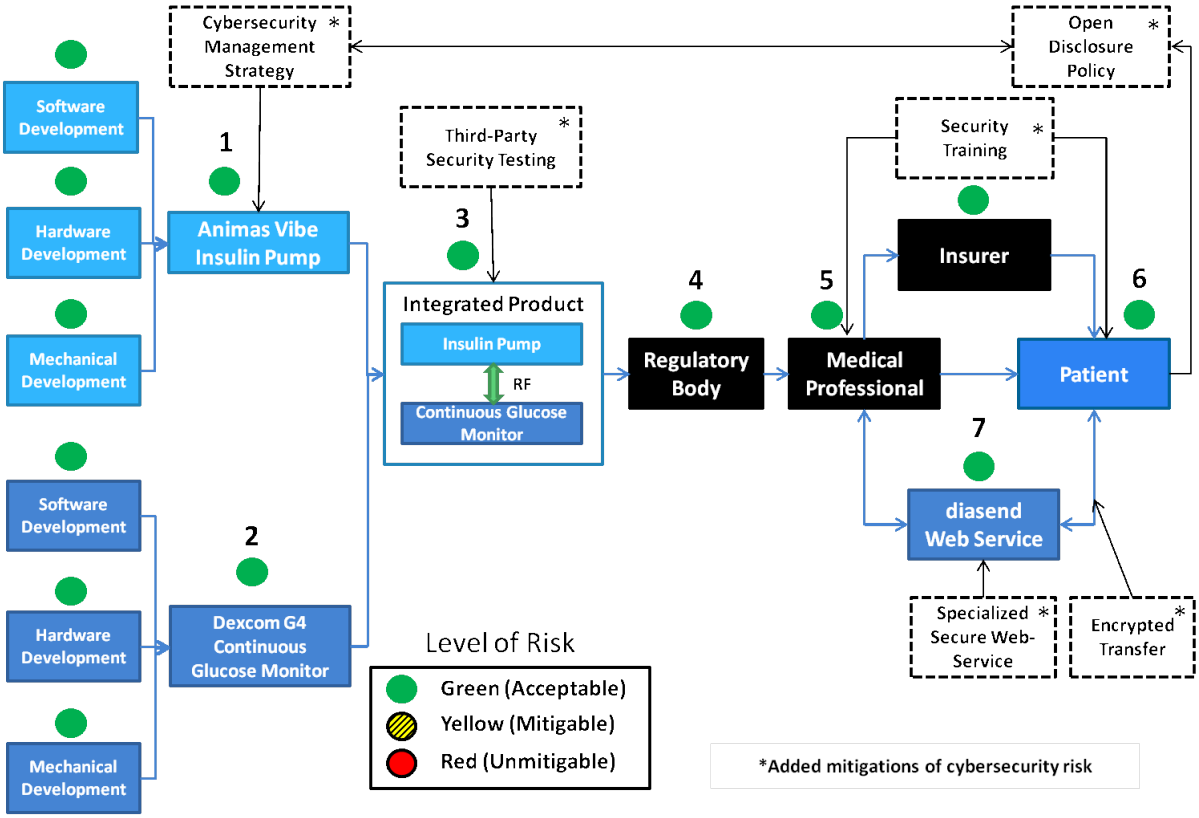

Figure 2. Cybersecurity blueprint for the Animas Vibe insulin pump with added cybersecurity risk mitigations (indicated by a dashed border of the box) and the risk level at the numbered locations reduced to acceptable (green)

The introduction of a cybersecurity value blueprint is important for the following four reasons:

1. It helps in identifying the key stakeholders in the ecosystem together with all associated cybersecurity vulnerabilities.

2. It helps in creating a prioritized plan to address the highest-risk cybersecurity vulnerabilities in collaboration with the rest of the stakeholders.

3. It articulates the value dimensions associated with the security efforts of all relevant stakeholders.

4. It enables innovating the ecosystem through the definition of a clear action plan for improving the security of medical devices over time in a way that could be articulated to business stakeholders and end customers.

This type of approach can change the way security is perceived to become a market differentiator built-in from the onset of design, instead of an add-on at the last stages of the development process.

For future contributions, the method for analyzing the cybersecurity risks within the ecosystem can be explored further. In this work, the emphasis was on establishing the principles for the cybersecurity value blueprint instead of the specific risk analysis, which requires a deeper insight into the various technological platforms enabling the operation of the device. It is clear, however, that the risk analysis within the ecosystem needs to focus on risks associated with the safety, privacy, and security of all stakeholders in the ecosystem. A potential future work could be to adapt a risk analysis method that incorporates cyber-resilience, lifecycle, and utility attributes in the context of networked medical devices and the ecosystem that is identified through the cybersecurity blueprint.

A Value Blueprint Approach to Cybersecurity in Networked Medical Devices

George Tanev, Peyo Tzolov, and Rollins Apiafi

Conclusion

The concern regarding cybersecurity in the increasing number of networked medical devices is growing. Manufacturers have yet to effectively convert their cybersecurity efforts into a market driver and market differentiator. This work argues that not positioning these efforts as a market value and differentiator is a missed opportunity that can be taken advantage of by looking at cybersecurity through an ecosystem perspective rather than a product-centric perspective. The suggested cybersecurity value blueprint approach offers the opportunity to enhance both the "resonating focus" and "points of difference" approach to the articulation of a value proposition by including the cybersecurity value dimension (Anderson et al., 2006). An explicit articulation of cybersecurity provides manufacturers with a tool for localizing and mitigating cybersecurity risks in the ecosystem, and presenting their efforts in a visual blueprint where the value and differentiation can be clearly seen. In an industry where security is beginning to take a central role, and where competition is fierce, the cybersecurity value blueprint could be a tool that would better position manufacturers in the market. Finally, it should be pointed out that, although the suggested tool should be considered as part of a more general risk management approach, it requires deep knowledge of the technological platforms and the specific business process implementation of all involved stakeholders. This is just another illustration of the fact that medical cybersecurity is truly a value co-creation problem that opens new opportunities for technology entrepreneurs and innovation management scholars and practitioners, which should be addressed through the coordinated activities of the entire business ecosystem within a systematic value chain resilience perspective (Boyes, 2015).

About the Authors

George Tanev is a Master of Applied Science candidate in the Technology Innovation Management program at Carleton University in Ottawa, Canada. He holds a Master of Science in Engineering degree in Medicine and Technology from the Technical University of Denmark and a Bachelor's degree in Biomedical and Electrical Engineering from Carleton University. George has industry and research experience in the development of portable medical device products. He also has interests in technology-based entrepreneurship, biomedical signal processing, medical device research and development, medical device regulatory affairs, and medical device cybersecurity.

Peyo Tzolov is a software engineer with a keen interest in entrepreneurship. He holds a Bachelor's degree in Communications Engineering from Carleton University in Ottawa, Canada, and is currently a Master of Applied Science candidate in the Technology Innovation Management program, also at Carleton University. Peyo has several years of experience as a software engineer working on highly scalable and distributed systems. He is very interested in technology, particularly in the security concerns arising from the rapid evolution and adoption of technology.

Tamunoiyowuna Rollins Apiafi is a Master of Applied Science candidate in the Technology Innovation Management program at Carleton University in Ottawa, Canada. He holds a Bachelor's degree in Industrial Chemistry from the University of Port Harcourt, Nigeria. Rollins is one of the co-founders of insight lenz, which specializes in wearable medical technologies that monitors the wearer's eyes to track the state of their health. Rollins is interested in medical device cybersecurity, medical device regulatory bodies, and networked portable medical device research and development.

A Value Blueprint Approach to Cybersecurity in Networked Medical Devices

George Tanev, Peyo Tzolov, and Rollins Apiafi

References

Adner, R. 2012. *The Wide Lens.* London: Penguin Books.

Amin, M., Tariq, Z., & Reed, I. S. 2015. Securing the Car: How Intrusive Manufacturer-Supplier Approaches Can Reduce Cybersecurity Vulnerabilities. *Technology Innovation Management Review,* 5(1): 21–25.
http://timreview.ca/article/863

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

Boyes, H. 2015. Cybersecurity and Cyber-Resilient Supply Chains. *Technology Innovation Management Review,* 5(4): 28–34.
http://timreview.ca/article/888

FDA. 2014. *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff.* Rockville, MD: US Food and Drug Administration.

Fu, K., & Blum, J. 2014. Controlling for Cybersecurity Risks of Medical Device Software. *Biomedical Instrumentation & Technology,* 48(1): 38–41.
http://dx.doi.org/10.2345/0899-8205-48.s1.38

Harries, P. 2014. The Prognosis for Healthcare Payers and Providers: Rising Cybersecurity Risks and Costs. PricewaterhouseCoopers Cybersecurity and Privacy Blog, December 17, 2014. Accessed June 1, 2015:
http://usblogs.pwc.com/cybersecurity/the-prognosis-for-healthcare-payers-and-providers-rising-cybersecurity-risks-and-costs/

Healey, J., Pollard, N., & Woods, B. 2015. The Healthcare Internet of Things: Rewards and Risks. *Atlantic Council,* March 18, 2015. Accessed June 1, 2015:
http://www.atlanticcouncil.org/publications/reports/the-healthcare-internet-of-things-rewards-and-risks

Krebs, B. 2014. 'Heartbleed' Bug Exposes Passwords, Web Site Encryption Keys. *Krebs on Security,* April 8, 2014. Accessed June 1, 2015:
http://krebsonsecurity.com/2014/04/heartbleed-bug-exposes-passwords-web-site-encryption-keys/

Rakitin, S. R. 2009. Networked Medical Devices: Essential Collaboration for Improved Safety. B*iomedical Instrumentation & Technology,* 43(4): 332–338.
http://dx.doi.org/10.2345/0899-8205-43.4.332

Shah, S. 2015. Cybersecurity as a Competitive Differentiator for Medical Devices. M*ed Device Online,* March 24, 2015. Accessed June 1, 2015:
http://www.meddeviceonline.com/doc/cybersecurity-as-a-competitive-differentiator-for-medical-devices-0001

Shaqdan, K., Aran, S., Daftari Besheli, L., & Abujudeh, H. 2014. Root-Cause Analysis and Health Failure Mode and Effect Analysis: Two Leading Techniques in Health Care Quality Assessment. J*ournal of the American College of Radiology,* 11(6): 572–579.
http://dx.doi.org/10.1016/j.jacr.2013.10.024

Wirth, A. 2011. Cybercrimes Pose Growing Threat to Medical Devices. *Biomedical Instrumentation & Technology,* 45(1): 26–34.
http://dx.doi.org/10.2345/0899-8205-45.1.26

Citation: 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. http://timreview.ca/article/903

Keywords: cybersecurity, ecosystem, networked medical devices, value proposition, market differentiation