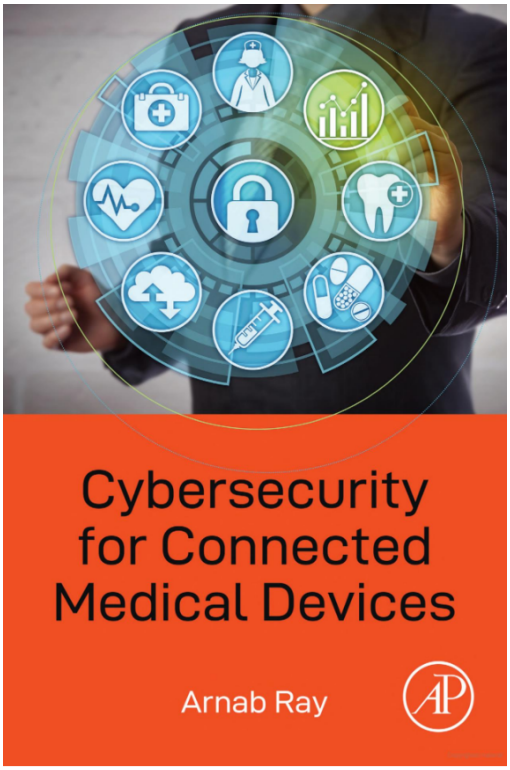
GlobalCE

Book Review

Cybersecurity for Connected Medical Devices
Arnab Ray
ISBN: 978-0-12-818262-8
Academic Press: Elsevier
First edition: Published November 2021
Book price: US$84.95

By Lloyd M. C. Lilley
Medical Devices IT Lead, Clinical Engineering, Nottingham University Hospitals NHS Trust, UK

This book review is about the Elsevier Academic Press newly published ***Cybersecurity for Connected Medical Devices*** by author Arnab Ray, Ph.D. In addition to the Preface, the book contains nine chapters, an Afterword, and an Index for a total of 332 pages. This book contains a bevy of information that could overwhelm on first reading, but helpfully, from Chapter 2 onwards, every chapter serves up a summary and key takeaways that consolidate the key messages. Arnab Ray is a computer scientist with a background in critical software development and cybersecurity design of medical devices that provides a cybersecurity developer's perspective throughout this book.



Whilst the key audience is manufacturers of medical devices who are responsible for designing a cyber secure product, clinical engineers with an interest in cybersecurity should find this book a handy supplement to make sense of the fast-evolving landscape. They will gain a broad understanding of basic cybersecurity principles, which can help influence integration choices in a healthcare delivery organization (HDO). Often medical device manufacturers (MDM) have not given enough consideration to the challenges of incorporating and maintaining a medical device in an HDO IT network. Importantly, Arnab recognizes that cybersecurity is a shared responsibility between the manufacturers and healthcare providers, but does not propose an effective mechanism for defining and sharing such responsibility.

The introduction provides context to support the assertion that the cybersecurity of medical devices is a growing concern. It cites some high-profile examples of cyber-attacks on medical devices in a controlled environment to provide proof of concept. While there are no reports of cybersecurity incidents in a real-life context it warns, that since most devices do not log cyber-related issues, a cyber incident could be incorrectly diagnosed as equipment malfunction. It would have been useful to highlight tools available to HDOs such as intrusion detection, dynamic network segmentation, and malware prevention systems and to examine how they impact medical devices' performance.

With the increasing integration of connected medical devices, with varying levels of endpoint security, to information systems, there are more opportunities for cybercriminals to gain illegal access to confidential information and disrupt wider operations within a healthcare

delivery organization. This chapter helpfully discusses the development of national cybersecurity policies in the U.S. with some acknowledgment of similar policies in the E.U. Acknowledgement of the widely accepted challenge of designing a cyber secure product without introducing unintended negative consequences on usability and patient safety, highlights the limitations in designing a cyber secure product. Medical device manufacturers (MDM) are encouraged to consider risk-based controls, which conflicts with the recommendation of a controls-based approach, mentioned in Chapter 4. The introduction concludes with cybersecurity lifecycle challenges, and a suggestion for the development of a manufacturer's business model, that makes cybersecurity a distinct structural part of the business.

A helpful analogy of a home, bank vault, and a precious asset is referred to throughout Chapter 2, Basic Cybersecurity Concepts, which effectively convey the fundamental concepts and challenges of cybersecurity and risk management. The key concepts of vulnerability and threats are articulated in simple, easy-to-understand terms. As the cybersecurity landscape evolves around the globe, terminology develops meanings that can seem rather vague, and often mean different things to different people, which might be a little disconcerting to a novice. The author approaches this conundrum by adopting certain definitions from authoritative sources and using them consistently throughout the book. As a result, the reader has a stable foundation from which to explore and understand the core principles.

The medical device's information security objectives are described as availability, integrity, and confidentiality in order of priority. However, one could argue that integrity has a higher priority since an altered record is more likely to go unnoticed, potentially causing widespread harm before it is detected, whereas the unavailability of information is obvious and should result in the implementation of contingency plans. This chapter clearly describes five categories of controls used to reduce the likelihood of an attack being successful. One of the categories, cryptography, is explored in detail with a study of the major cryptographic techniques used to establish secure communications between the sender and the intended receiver. The level of detail given is appropriate for one who is new to this discipline and is informative enough to help a designer make decisions about the most appropriate method to implement.

Standards and regulations, which aim to ensure manufacturers build safe medical devices, are developing to include cybersecurity requirements. The increasing focus on cybersecurity is the subject of Chapter 3, Regulatory Overview and includes a summary of the current US and EU regulatory frameworks. It is recognized that a robust quality management system (QMS) is necessary for manufacturers if they are to meet the standards expected by the regulatory authorities. This chapter discusses key manufacturing quality standards, suggesting cybersecurity is not yet fully formed in them, and in fact lags behind some standards that HDOs have had access to for some time. Manufacturers struggling to adapt are offered useful guidance on how to achieve a cyber aware QMS with a suggested 5 step process for introducing regulatory requirements into an existing system.

In Chapter 4, The Product Cybersecurity Organisation, the author suggests that with few tools available to quantify cybersecurity impact it is difficult for MDM's decision-makers to be convinced of the benefits of investing. One could argue that making the case for investing is not difficult because of many well-known instances where damage has occurred from cyber-attacks on IT systems – the connected medical device is another type of IT system prone to the same attacks therefore, much is already known about exploitable system weaknesses. The author prefers a controls-based framework as opposed to a risk-based framework for building a cyber secure product. I believe that both frameworks have a place in design and there will always be an element of risk-based design due to the costs in terms of build and device performance. Recommendations for addressing

organizational shortfalls are made by offering key building blocks to achieving a product cybersecurity organization.

Cybersecurity risk management is a complex field and the author clearly wanted to give more attention to this area therefore it occupies Chapters 5 and 6. Chapter 5 predominantly addresses risk assessment and looks at threat modeling from system and subsystem levels. To help demonstrate a systemic threat and vulnerability modeling approach, an infusion pump with network connectivity is specified, and used as an example. This provides a convenient vehicle to explain the transferrable process for assessing cybersecurity risk. There is a lack of threat modeling tools specific to medical devices but there are modeling tools for IT systems that can be adapted. The author demonstrates this by using Microsoft's STRIDE framework to identify system threats and complete a threat model.

Chapter 6, Cybersecurity Risk Management-II, builds on the previous chapter with an illustration of a complete system cybersecurity risk model. The main theme of this chapter is the response to an identified risk. The infusion pump example specified in Chapter 5, again proves useful but this time to explore system threats and the corresponding responses or controls. The MDM cybersecurity designer is walked through high-level examples of threat articulation, responses, and undertaking a risk-benefit analysis.

It is recommended that technical controls are traceable to regulations and standards. Chapter 7, Cybersecurity Design Engineering, takes a look at these controls identifying them as master controls, and with examples, key factors for building cyber-secure medical devices are considered. A brief look at the limiting factors in the hardware and battery-operated devices clearly demonstrates the challenge of incorporating effective cybersecurity controls without degrading performance. It would have been useful to provide examples from other safety-conscious industries such as aviation or nuclear power, which are at an advanced stage of maturity.

Chapter 8 delves deeper into five more capabilities of an MDM that were defined in Chapter 4. Each capability is clearly described, providing industry insights with recommended best practices.

The final chapter, Chapter 9, Product Security Governance and Regulatory Compliance explores two more capabilities that an MDM should demonstrate. This chapter describes the governance elements required to satisfy regulations, which are fundamentally supported by a QMS. The advice given here is simple and clear - MDM's need to continually refresh their resources and processes, and be transparent about the product's cybersecurity posture.

Although this book is aimed at medical device manufacturers (MDM), I feel it is suited to anyone with an interest in medical device cybersecurity, including those working in healthcare delivery organizations. A lot of ground is covered mostly from a regulatory and compliance challenges angle; as a result, it only provides an overview, which the author concedes. However, the reader will find this book a useful springboard, from which to develop a greater understanding of a fast-evolving domain. This book successfully provides a framework for MDMs to design a cybersecurity-focused organization.