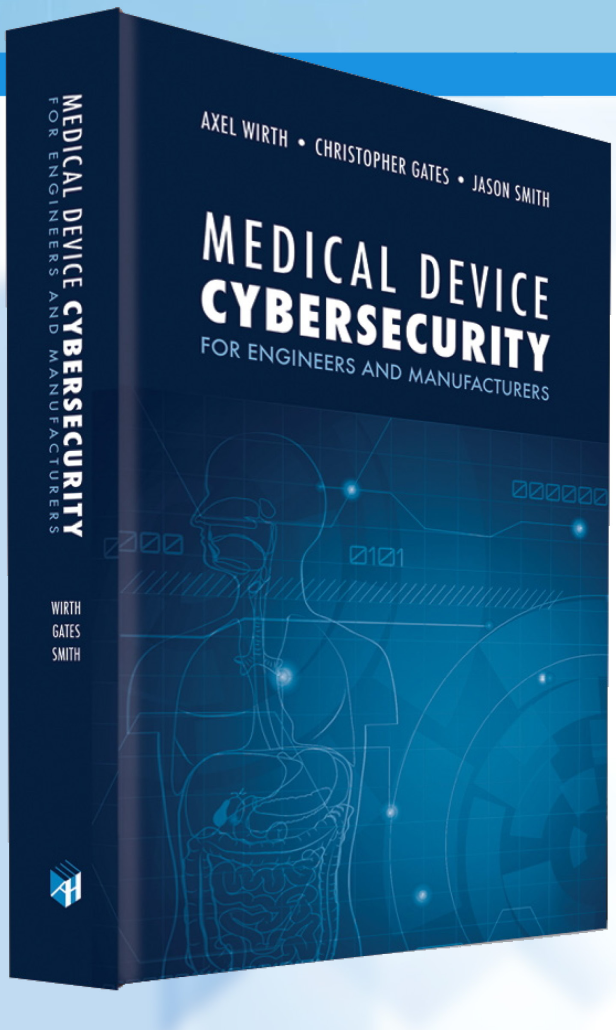
ARTECH HOUSE
BOSTON I LONDON


AXEL WIRTH • CHRISTOPHER GATES • JASON SMITH
MEDICAL DEVICE
CYBERSECURITY
FOR ENGINEERS AND MANUFACTURERS
MEDICAL DEVICE CYBERSECURITY FOR ENGINEERS AND MANUFACTURERS
WIRTH
GATES
SMITH

MEDICAL DEVICE CYBERSECURITY
FOR ENGINEERS AND MANUFACTURERS

AXEL WIRTH | CHRISTOPHER GATES | JASON SMITH

FOREWORD BY GREG GARCIA Executive Director, HSCC

ARTECH HOUSE BOSTON I LONDON
685 Canton Street, Norwood, MA 02062, USA
16 Sussex Street, London SW1V 4RW, UK

ARTECH HOUSE
BOSTON I LONDON

BOOK SUMMARY

Medical Device Cybersecurity for Engineers and Manufacturers removes the mystery from cybersecurity engineering for embedded devices. It is designed to walk readers through the lifecycle management processes and best practices of secure design, implementation, regulatory submissions, production, sales, as well as postmarket activities, including surveillance, field support and updates, and end-of-life.

This book coaches professionals to shape or retool their organization's approach to development so that devices will meet emerging regulatory and customer expectations while reducing business and patient exposure to cybersecurity risks, minimizing schedule impacts, and accelerating time-to-market.

Wirth, Gates, and Smith's step-by-step approach educates engineers and managers about implementing cybersecurity best practices in accordance with industry practices and expectations. Readers are advised on subjects ranging from high-level concepts in embedded medical device security to implementable real-world solutions and tools.

Medical Device Cybersecurity for Engineers and Manufacturers delivers awareness and insight into the practices, processes, and outputs necessary to create secure medical devices capable of gaining regulatory approval and meeting market entry requirements.

> *“Cybersecurity is no longer optional. We must not allow sensationalism or headlines to drive the discussion… Nevertheless, we must proceed with urgency.*
>
> *In the end, this is about preventing patient harm and preserving patient trust.”*

ARTECH HOUSE
BOSTON I LONDON

AUTHORS

Axel Wirth

https://www.linkedin.com/in/axelwirth/

Christopher Gates

https://www.linkedin.com/in/christopher-gates-8912a81a/

Jason Smith

https://www.linkedin.com/in/smith-jason/

CONTRIBUTORS

Alan Friedman
SBOMs

https://www.linkedin.com/in/allanafriedman/

Michelle Jump
Regulatory & Standards

https://www.linkedin.com/in/michellejump/

Michael McNeil
Governance & Organizations

https://www.linkedin.com/in/mcneilmichael/

Greg Garcia
Foreword

https://www.linkedin.com/in/gregorytgarcia/

Sat Ketkar
Code Review

https://www.linkedin.com/in/satyajit-k-14569111/

Eric Pancoast
Cryptography

https://www.linkedin.com/in/epancoast/

ARTECH HOUSE
BOSTON | LONDON

YOUR COMPLETE GUIDE

TO THE CYBERSECURE DEVICE LIFECYCLE

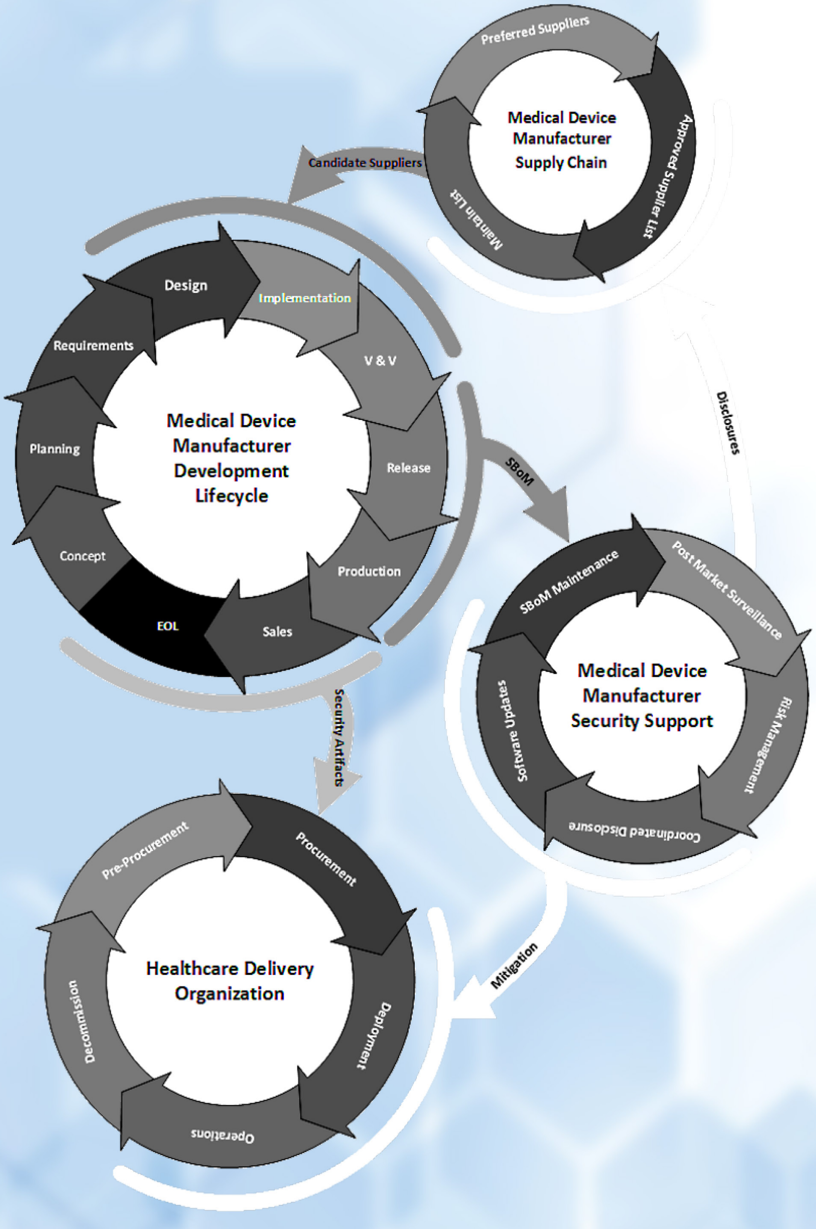


Figure © H-ISAC. Used by Permission.

Medical Device Engineering for Engineers and Manufacturers

AXEL WIRTH | CHRISTOPHER GATES | JASON SMITH

ARTECH HOUSE
BOSTON I LONDON

TABLE OF CONTENTS

Medical Device Engineering for Engineers and Manufacturers

AXEL WIRTH | CHRISTOPHER GATES | JASON SMITH

TABLE OF CONTENTS—CONTINUED

FOREWORD

Greg Garcia is Executive Director for Cybersecurity at HSCC, the Health Sector Coordinating Council.

From 2006-2009, he served as the nation's first Assistant Secretary of Cyber Security and Communications for the U.S. Department of Homeland Security.

Whether we're in the doctor's office for a routine checkup, monitoring our heart rate with a wearable device on a morning jog, or having surgery in the operating room, we rarely think about the devices that we use for medical care being vulnerable to a cybersecurity attack. However, the benefits from rapid advances in the use and capabilities of "connected health" also come with potential risks.

According to the American Hospital Association (AHA), the US is home to over 6,000 hospitals, ranging from small community hospitals with less than 50 beds to health systems with over 5000 beds. In general, hospitals have 3-6 networked medical devices per bed. That means with a total of 931,203 staffed hospital beds across the United States, there are some 3-6 million connected medical devices at hospital bedsides alone, all of which must be protected against cyber-attacks. In addition, health delivery organizations, including hospitals, depend on non-medical devices such as infrastructure systems that keep elevators running, maintain temperature and air quality, and provide lighting and facilitate rapid remote communications for their continued operations. Thus, it is evident that patient safety and quality of care depend on cyber safety, yet we have a large risk exposure of an estimated 10-15 million total connected devices (including infrastructure and supporting devices) that, if compromised, could lead to patient harm or care delivery impact.

This fact is acutely on the minds of both healthcare providers who manage the devices and medical technology and health I.T. companies who manufacture them. Certain principles must be understood when we think about healthcare cybersecurity:

1) Because the threat landscape is constantly evolving, network and device security have difficulty keeping up;

2) Healthcare institutions do not have the time, money, capabilities, or resources to independently fix cyber vulnerabilities;

3) Patching updates and addressing vulnerabilities in the active medical device ecosystem can be more complicated than your average IT update because there may be a human, not an app or machine, connected to that device and "system reboot" may not be an option; and

4) There are limits to the ability of government regulation to achieve the necessary balance of innovation, effectiveness, security, and privacy.

It is now recognized that these shared challenges are also a shared responsibility. In response, the public and private sectors are working together to address these healthcare cybersecurity challenges in multiple forward-looking ways. It can indeed be argued that working together is an imperative. Healthcare is considered one of the nation's 17 critical infrastructure sectors—like electricity, telecommunications, water, chemicals, transportation, and more. And because private industry owns and operates the vast majority of these critical infrastructures, which constitute essential public resources, it is their responsibility to serve the public good in addition to their commercial interests. That's why this shared responsibility is so important, from the engineers to the C-Suite, to work toward strengthening the security of our healthcare systems and the medical technology that has become indispensable for our nation's health.

The Health Sector Coordinating Council (HSCC)—a public private partnership of health sector and government stakeholders dedicated to strengthening the nation's critical healthcare infrastructure against all hazards—convenes these interdependent stakeholders to improve the security and resiliency across the healthcare ecosystem. An HSCC task group addressed the medical device security issue head-on, working over 18 months to publish in January 2019 a best practices guide for medical technology companies—the Medical Device and Health I.T. Joint Security Plan (JSP).

The JSP utilizes "security by design" principles throughout the product lifecycle of medical devices and health I.T. solutions. It encourages shared responsibility in the adoption of security-related standards, risk assessment methodologies, and vulnerability reporting requirements to improve information sharing between manufacturers and healthcare organizations. The JSP is a living document and will be updated as appropriate to adapt to the ever-changing threat environment for medical devices and health I.T. solutions.

More follow-on thought is now being given to how hospitals, device manufacturers, and government can coordinate to better communicate with patients about device vulnerabilities and security, and how we can deal with the challenging issue of aging medical technologies that have reached the end of supported life—whether for security or operational efficiency—but are not easily replaced because of tremendous expense. Again, the shared challenge meets shared responsibility and collaborative solutions.

These and other critical issues are being addressed in sector-wide workstreams, such as:

- HSCC's resource for health providers, the Health Industry Cybersecurity Practices (HICP)
- The FDA's September 2019 Patient Engagement Advisory Committee, which sought out how best to communicate cybersecurity risks in health risk communications to patients
- Efforts to define and operationalize the imperative for "software bills of materials" to help health systems understand which software components are in the devices and systems they purchase and hence how to manage the associated risk
- Expansion of the annual DefCon Biohacking Village Device Hacking Lab, where hackers, healthcare providers, and device manufacturers collaborate to identify vulnerabilities
- The International Medical Device Regulators Forum (IMDRF) cybersecurity working group, made up of industry and regulators and co-led by FDA and Health Canada, which is seeking to promote a globally harmonized approach to medical device cybersecurity via the drafting of a cybersecurity guide

We see all these collaborations as signs of significant progress. In 2017, a health care cybersecurity task force of industry and government leaders diagnosed that healthcare cybersecurity is in "critical condition." While we have had no reports to date that cyber incidents involving medical devices have led to direct patient harm, our collective action, premised on the recognition that patient safety depends on cyber safety, will go a long way toward maintaining public trust in the security, resiliency, and integrity of the life-saving and life-sustaining devices we depend on, and upgrading our healthcare cybersecurity diagnosis to "stable".

Good cyber hygiene is found in the products and systems we design, manufacture and maintain, and in the management of those devices and the clinical systems in which they operate. Active and continuous adoption and refinement of resources, like this guide, will help medical technology companies—their engineers, service departments, and executive management, as well as their health provider customers, step up to this shared responsibility.

ARTECH HOUSE
BOSTON I LONDON

INTRODUCTION TO SECURE MEDICAL DEVICES

EXCERPTED FROM CHAPTER ONE

Why Secure Medical Devices?

We were inspired to write this book after a long history of working with and for medical device manufacturers (MDMs), as well as with healthcare delivery organizations (HDOs). The medical device industry was the first industry to be regulated to produce secure embedded devices. This has left MDMs in the odd position of being trailblazers in an industry where cybersecurity is not necessarily their principal skill set. Secure development has nothing in common with the practice of medicine; instead, it has everything to do with the subtlety of design, quality of implementation, the threat landscape, and awareness of the attack vectors utilized by attackers. How to balance these concerns with the creation of a new medical device is the overriding topic of this book.

Approaches for incorporating secure development practices into the development lifecycle have not been taught in traditional education programs until very recently, nor are models or best practices available specific to the medical device environment. This lack of training for all levels of engineers, project managers, and senior leadership is a critical shortfall, making it difficult for MDMs from producing proactively secured devices and preventing them from constructively engaging with their customers and regulators.

This book intends to provide guidance to MDMs on how to implement a secure medical device lifecycle in a manner that is repeatable, trackable, produces artifacts needed for regulatory submission, and actually improves the security standing of the individual medical devices as well as the larger device ecosystem. This book may also serve HDOs as an informative resource for understanding the security activities and support MDMs should perform and how HDOs and MDMs can collaborate to keep devices secure and users safe.

There are many domestic and international standards for securing medical devices (and IoT in general). However, these guidelines are not harmonized and do not provide sufficient details to implement such a program. In other words, they provide the "what" but not the "how." This book intends to close that gap.

Medical Device Engineering for Engineers and Manufacturers

AXEL WIRTH | CHRISTOPHER GATES | JASON SMITH

The Evolution of Cybersecurity in Healthcare

Over the past decade, our understanding of cybersecurity risks in the healthcare industry has been evolving. Healthcare has been moving from a compliance-driven industry to a more cybersecurity-aware one. This is largely due to two factors:

> 1) Driven by government initiatives and the desire to reduce costs and improve efficiency, healthcare has increasingly digitalized (implemented more digital systems) and digitized (amassed more digital data). This increasing connectivity and integration of systems and devices containing more valuable information have not only created a broader attack surface and more attractive opportunity for malicious cyber actors, but it has also increased our dependency on the availability of these systems.
>
> 2) Cyber adversaries, driven by financial or political motivation, have become increasingly advanced and their attacks have become more sophisticated, targeted, stealthy, and, unfortunately, successful. Their impact on businesses around the globe is significant and is now exceeding $1 trillion USD by some estimates.

Consequently, we are no longer thinking about cybersecurity risks merely in the context of our information systems and the data they hold but now have a more comprehensive view, including the potential impact on patient health, care delivery, hospital operations, and even on health systems at the national level.

Unfortunately, this learning experience came from a number of painful experiences. Ransomware attacks have resulted in the payment of the demanded ransom or have forced hospitals to go through a complex and costly recovery period. For example, the WannaCry attack on the UK National Health Service (NHS) in May 2017 affected more than 1,000 IT systems and medical devices, resulting in the full or partial shutdown of 81 NHS Trust hospitals, the cancelation of 19,000 patient appointments, and an estimated financial impact of £92 million.

This was followed by the NotPetya pseudo-ransomware (wiper) attack in June, which impacted few healthcare delivery organizations directly but had a broad negative impact on hosted documentation services, the availability of pharmaceuticals and vaccines, and global shipping and logistics companies.

Both attacks resulted in multi-billion-dollar losses around the globe and across multiple industries. Yet both WannaCry and NotPetya were imperfect malware that contained design and execution flaws. In other words, in spite of the damage done, it could have been much worse.

The Unique Role of Medical Devices

As medical devices moved from the early days of beneficial uses of electricity and radiation to a tightly integrated “system of systems” with complex data flows not only between devices, but also between devices and hospital IT systems, we became aware that these devices were not only more vulnerable and difficult to protect, but also that the security compromise of any of these could result in patient harm or impact on care delivery—in addition to the traditional security concerns around data confidentiality, integrity, and availability.

Industry stakeholders have been aware of the security risks of medical devices since security researchers demonstrated their ability to hack into an Implantable Cardiac Defibrillator (ICD) in 2008. Since then we have seen individual researchers, hospitals, and government agencies conduct their own additional research, all with the same results: our medical device ecosystem is highly vulnerable, and we have failed to establish cybersecurity as non-negotiable, either as a buying criterion or as a design objective. Fortunately, regulators and leading medical device manufacturers have recognized the problem and are establishing a path forward.

It also should be understood that even though this book is generically using the term “medical devices,” the lifecycle management and security best practices described can equally be applied to a wide range of devices that are used on hospital networks, not just the ones classified as medical devices by the local regulators. A cyber incident involving a hospital elevator impacts patient transportation. A change in temperature or humidity in the operating theater may force procedures to be delayed. Shutting down a blood or organ refrigerator can have a serious impact on patients waiting for a transplant or infusion. Therefore, even though international regulators’ guidances are focused on medical devices and their potential security risks to patient harm or care delivery, the practices outlined in the following chapters are equally beneficial and can be applied to other care-critical, albeit not-yet-regulated, device types.

Clearly, cybersecurity for medical devices needs to be proactively addressed on the level of the individual device. But since no device will ever be perfectly secure (and certainly not devices already in use today), additional security measures should be applied on the level of the integrated system of devices, whether in the traditional, hospital-based care environment or in the evolving telehealth and home care settings. A system is only as secure as the sum of its parts, and can only achieve a sufficient level of security if all stakeholders accept and live up to their responsibilities. However, it is generally accepted that the security posture of the device itself is the most critical component, and that device manufacturers need to live up to their responsibility of providing more secure designs and devices with an easier-to-maintain security posture.

Today's medical device ecosystem goes far beyond the device or local device network itself and includes electronic health record (EHR) and image management (PACS) systems, inventory and business automation systems, cloud based value-added services, access via mobile devices, home based routers, and public networks. In order to provide sufficient security, each party needs to understand and accept their responsibility as well as provide their contribution.

Regulatory Environment

Over the past years, many international regulators have taken steps to provide a guidance framework and to establish their expectations on cybersecurity for medical devices. The US Food and Drug Administration (FDA) has been taking the lead with its Premarket Guidance (2014), Postmarket Guidance (2016), and updated draft Premarket guidance (2018). Other notable contributions have been and are being provided by the International Medical Device Regulators Forum (IMDRF) and the European Union, in addition to individual countries like Canada, Japan, China, Australia, or France.

The regulatory background will be discussed in subsequent chapters, but a commonly-voiced objection worth addressing here is that these publications are "guidance only," therefore not legally binding. This is a common misunderstanding. Many regulators view guidances as clarification of the agency's expectations for compliance with existing regulations.

In other words, regulators have stated that cybersecurity is no longer optional. The exact details on how to set up a secure lifecycle management process that results in sufficiently secure devices may be the manufacturer's choice, but that fact that such a program is needed is now beyond dispute in most—soon-to-be all—markets.

The healthcare industry, including the medical device industry, is highly regulated so as to assure patient safety and reliable quality care delivery. But these regulations, combined with a formal design process and conservative decision making, are just the opposite of what many cybersecurity professionals are accustomed to in information technology, where we want to be flexible and nimble so as to quickly respond to new cyber threats and risks.

In short, we need to improve our processes to be able to move faster in response to security challenges without compromising device safety. But we also need to improve device design to provide a more secure state "out of the factory" so that fewer downstream field changes are needed, while also improving device design so that these fewer changes are easier and faster to deploy. The following chapters include both general principles and actionable prescriptions for programmatic and procedural changes that will enable MDMs to move forward with confidence.

Looking Ahead

Over the past decade, much research has been published about the potential risks of failing to secure medical devices. We do not have the luxury of brushing off this problem or sweeping it under the table. Security researchers have demonstrated over and over again the often-appalling security weaknesses of medical devices and how they could be exploited by an attacker, including the examples already provided. But we should think of this problem not only in the context of a targeted attack with malicious intent:

- Since 2015, security researchers have repeatedly gathered evidence that medical devices are used as an entry point and beachhead for an attack on other targets.
- Even if the device is not the target at all, it may get caught up in an attack if the device happens to fit the threat profile, as happened during the WannaCry malware outbreak.
- In another non-targeted event, medical equipment in a Siberian hospital was shut down by ransomware in the midst of brain surgery. Even though the patient was reported unharmed, this was a close call.
- We know that even minutes of delay in care can have impact on emergency patient mortality rates, and that in the aftermath of a cyberattack hospitals saw additional patient deaths due to heart attacks. Due to the care-critical nature of medical devices, any security incident affecting device and service availability will indirectly impact patient safety.

Athough we have few reported cases of direct patient harm, we need to ask ourselves whether we've been able to accurately assess the true impact of cybersecurity events on patient outcomes. As cybersecurity professionals, it is our job to resist the urge to allow sensationalism and headlines drive the discussion. However, we must also proceed with a sense of urgency. It is our hope that this book will contribute to a measured and reasonable approach that ultimately leads to a more secure and therefore safer healthcare ecosystem.

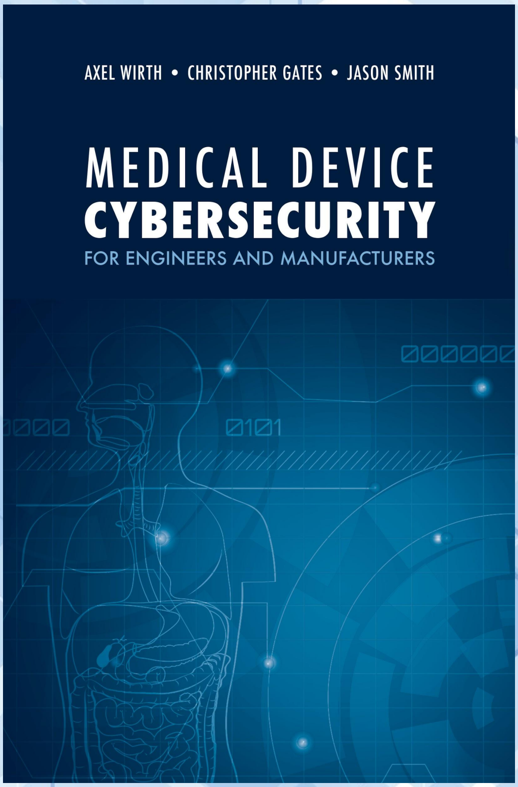
In the end, this is about preventing patient harm and preserving patient trust.

ARTECH HOUSE
BOSTON | LONDON

EXCLUSIVE
30% Discount!

Medical Device Cybersecurity for Engineers and Manufacturers

Axel Wirth, Christopher Gates, Jason Smith


AXEL WIRTH • CHRISTOPHER GATES • JASON SMITH
MEDICAL DEVICE
CYBERSECURITY
FOR ENGINEERS AND MANUFACTURERS

Hardcover • 270 pp. • Sept 2020
ISBN: 978-1-63081-815-9
£138 30% Savings! Only £96.60
$159 30% Savings! Only $111.30

A comprehensive guide to medical device secure lifecycle management, this is a book for engineers, managers, and regulatory specialists. Readers gain insight into the security aspects of every phase of the product lifecycle, including concept, design, implementation, supply chain, manufacturing, postmarket surveillance, maintenance, updates, and end of life.

- Learn how to mitigate or completely avoid common cybersecurity vulnerabilities introduced during development and production;
- Grow your awareness of cybersecurity development topics ranging from high-level concepts to practical solutions and tools;
- Get insight into emerging regulatory and customer expectations;
- Uncover how to minimize schedule impacts and accelerate time-to-market while still accomplishing the main goal: reducing patient and business exposure to cybersecurity risks.

Save 30% with Promo Code: WIR30
Order now at www.ArtechHouse.com
Cannot be combined with other discounts. Offer expires 31/10/2020.

To Order
For customers in the US, Canada, South America, Australia, New Zealand:
Call: 1-800-225-9977 (in the U.S. or Canada),
or 1-781-769-9750, ext. 4030
Fax: 1-781-769-6334
E-mail: artech@ArtechHouse.com

For customers in the UK, EMEA, Asia, or International orders:
Call: +44 (0)20 7596-8750
Fax: +44 (0)20 7630-0166
E-mail: artech-uk@ArtechHouse.com