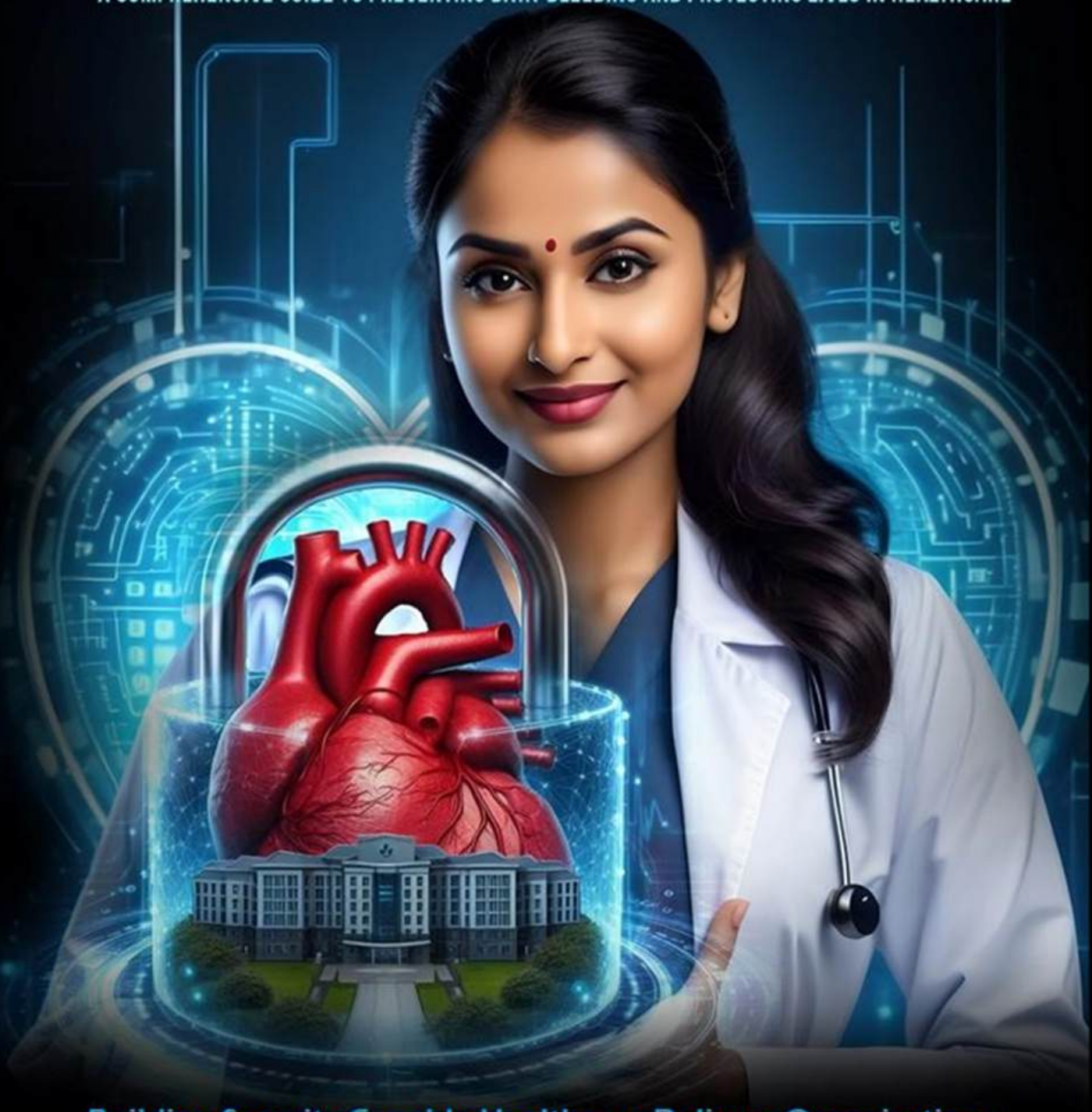
STOP CYBER HEMORRHAGE

A COMPREHENSIVE GUIDE TO PREVENTING DATA-BLEEDING AND PROTECTING LIVES IN HEALTHCARE



Building Security-Capable Healthcare Delivery Organisations

K S MANOJ & G JENIN

Iterative International Publishers
IIP

STOP CYBER HEMORRHAGE

A COMPREHENSIVE GUIDE TO PREVENTING DATA-BLEEDING AND PROTECTING LIVES IN HEALTHCARE

BUILDING SECURITY CAPABLE HEALTHCARE DELIVERY ORGANISATIONS

K S MANOJ & G JENIN

Title of the Book: STOP CYBER HEMORRHAGE: A Comprehensive Guide to Preventing Data- Bleeding and Protecting Lives in Healthcare

First Edition - 2024

K. S. Manoj, Research Engineer (OT Cybersecurity), iNTELEGRID, TF3, Galaxy Delights TC 42/3543, Near SCTIMST Keasari Lane, Poojappura Thiruvanathapuram Kerala, India.

G. Jenin, Senior Industrial cybersecurity Auditor, iNTELEGRID, TF3, Galaxy Delights TC 42/3543, Near SCTIMST Keasari Lane, Poojappura Thiruvanathapuram Kerala, India.

Disclaimer
The authors are solely responsible for the contents published in this book. The publishers don't take any responsibility for the same in any manner. Errors, if any, are purely unintentional and readers are requested to communicate such errors to the editors or publishers to avoid discrepancies in future.

E-ISBN: 978-93-6252-669-4

MRP: 350/-

Publisher, Printed at & Distribution by:
Selfypage Developers Pvt Ltd.,
Pushpagiri Complex,
Beside SBI Housing Board,
K.M. Road Chikkamagaluru, Karnataka.
Tel.: +91-8861518868
E-mail:info@iipbooks.com

IMPRINT: I I P Iterative International Publishers

For Sales Enquiries:
Contact: +91- 8861511583
E-mail: sales@iipbooks.com

गुरुर्ब्रह्मा गुरुर्विष्णुः गुरुर्देवो महेश्वरः ।
गुरुः साक्षात् परं ब्रह्म तस्मै श्री गुरवे नमः ॥

(The guru is Brahma (the God who creates), the guru is Vishnu (the God who preserves), the guru is Maheśwara (Śiva, the God who annihilates), the guru is the self-revealing limitless Brahman: means, Guru is absolutely the representation of Brahma, Vishnu and Shiva. In essence, guru creates, sustains knowledge and annihilates the weeds of ignorance. Salutations to that revered guru.)

MOST HUMBLE DEDICATION TO

SREE NARAYANA GURUDEV

OF SIVAGIRI MUTT

Foreword

Advancements in technology including proliferation of sensors, cloud enabled applications, privacy preserving techniques, artificial intelligence is enabling accelerated digitization across sectors. In the context of health sector apart from such technologies, usage of medical devices for critical activities are becoming important. While such advancements is making life easier through seamless access, quicker response time and efficient services it is important to ensure security and privacy making Cybersecurity as the core element and is no longer an optional or peripheral concern especially for sector like healthcare industry. Healthcare sector becomes more digitized and interconnected, it also becomes more vulnerable to cyberattacks that can compromise patient safety, privacy, and trust. Adversaries are constantly looking for ways to exploit the valuable and sensitive data that healthcare delivery organizations (HDOs) collect, store, and share. They are also targeting the advanced medical devices and procedures that rely on networked communication and control. These attacks can have devastating consequences, such as disrupting critical care, exposing confidential information, extorting ransom, or even causing physical harm.

Therefore, it is imperative for HDOs to adopt a proactive, comprehensive, and holistic approach to cybersecurity covering technical, human, organizational, and ethical aspects. HDOs need to understand the nature and motivations of their adversaries, the challenges and opportunities of their environment, the best practices and standards of their industry, and the future trends and innovations of their field.

This is where this book comes in handy. This book is a comprehensive guide to cybersecurity in healthcare, written by the authors, who are experts and leaders in both the ICT and cybersecurity fields. Writing a multidisciplinary work such as this would be difficult without the writers' evident depth of expertise and understanding in ICT, cybersecurity, healthcare, and biomedical engineering.

This book is a comprehensive and timely guide for anyone who is interested or involved in the field of healthcare cybersecurity. It covers the essential topics and concepts that are relevant and applicable to the current and future challenges of HDOs. It provides a clear and concise explanation of the technical, legal, ethical, and managerial aspects of cybersecurity in the healthcare context. Additionally, it provides useful guidance on how to enhance cybersecurity measures in HDOs, encompassing everything from the development and design of medical equipment and systems to the deployment and upkeep of hospital networks and infrastructure, as well as the integration and optimization of risk assessment and quality management.

This book is not only informative and useful, but also engaging and inspiring. It showcases the latest innovations and developments in the field of healthcare cybersecurity, such as the Internet of Medical Things (IoMT), surgical robots, artificial intelligence, and blockchain. It discusses cybersecurity threats in healthcare, challenges, stakeholder roles, and leadership. It covers emerging medical technologies, EHRs, device quality management, and product life cycles. It also explains the implementation strategies of defense-in-depth, layered security, and secure dataflow concepts in an HDO environment. This book provides insights into the regulatory and standards aspects along with case studies and best practices are provided. It also highlights the opportunities and challenges that these technologies pose for HDOs and their stakeholders. It encourages the readers to think critically and creatively about the current and future state of healthcare cybersecurity, and to contribute to its advancement and improvement.

This book is written in a clear, concise, and engaging style, with many case-studies, diagrams, tables, and figures to illustrate the concepts and ideas. The book also includes summaries and review questions at the end of each chapter, to help the readers review and reinforce their learning.

I highly recommend this book to anyone who wants to learn more about cybersecurity in healthcare and how to build security-capable HDOs that are more secure, resilient, and trustworthy. It is a valuable and relevant resource for students, researchers, practitioners, policymakers, and educators alike. This book is a must-read for anyone who cares about the future of healthcare and the well-being of humanity. I am sure that the authors will continue their research in the field of industrial cybersecurity, which is of vital importance in our society. May God bless them with longevity, energy, and the ability to put out more work of this nature for the benefit of our nation.

Dr. N. Subramanian
Executive Director,
Society for Electronic Transactions and Security (SETS),
Office of the Principal Scientific Adviser, Government of India,
2024.

Inspiration for this Book

This endeavour was inspired by the vibrant words and contributions of Dr. M. S. Valiyathan, Ch.M. (Liverpool), FRCS (England, Edinburgh & Canada), FRCP (London), D.Sc. (h.c.), FNA, FNASc, FNAE, FAMS, FTWAS, a renowned cardiac surgeon, technocrat, and recipient of the Padma Vibhushan award who is widely regarded as the Father of Indian Health Technology. He has made significant contributions to the development of indigenous medical devices like artificial heart valves, oxygenators, blood bags, etc. and the promotion of Ayurvedic research. Additionally, the "**Make in India"** initiative of Sri.Narendra Modi, the Indian Prime Minister, ignited and transformed our passion for technical and scientific writing into an obsession with producing top-notch technical publications and disseminating them globally.

The healthcare industry is becoming the most sought-after commodity for cybercriminals and hacktivists, as patient data is a highly valued product. What would be the impact if a cybercriminal gained access to a hospital network that controls the diagnostic, treatment, and life support equipment on which patient lives depend and prevented staff from accessing patient records or scheduling appointments? The connected medical equipment can also be hacked and shut down remotely as a form of extortion. In fact, cybercriminals are interested in disrupting patient care in many ways for vested and varied interests, including ransomware.

The cyber resilience of hospitals is a multifaceted and formidable issue that entails safeguarding patient data, hospital operations, and medical devices from cyber-attacks. Hospitals need to adopt a comprehensive and proactive approach to cybersecurity that encompasses robust ICT infrastructure, stakeholder alignment, risk assessment, threat prevention, detection, and response, and continuous improvement. Hospitals also need to collaborate with other stakeholders, such as vendors, manufacturers, regulators, and policymakers, to ensure a secure and resilient healthcare ecosystem. Unless hospitals and other healthcare facilities implement the measures necessary to fortify their computer and connected device networks, they will be vulnerable to cyber-physical attacks, potentially with life-threatening consequences.

After meticulously scrutinizing the situation, we arrived at the conclusion that a comprehensive book on cyber resilience in healthcare is imperative for a plethora of reasons, including the escalation in cyber threats, the intricacy of healthcare systems, regulatory compliance, collaboration and information sharing, patient safety and trust, education and training, risk management, incident response and recovery, innovation and technological advancements, and fostering a security culture. The recently passed Digital Private Data

Protection Act of India is definitely a game changer in data protection and privacy, especially in health delivery organizations (HDOs) in India. Of course, this book is a wake-up call for HDOs to comprehend the current ecosystem, the domains that are prey of cyber criminals, and the mitigation strategies to be implemented with layered security.

Being a transdisciplinary topic, writing this book was an enlightenment, an adventure, a challenge, and, of course, a source of nostalgia for one of the authors, as he had collaborated with the biomedical engineering research of the Sree Chitra Tirunal Institute for Medical Sciences and Technology (SCTIMST) in the nascent stages of his career.

Target Audience

The target audience for this book encompasses a broad spectrum of readers interested in fortifying the environment of healthcare delivery organizations, particularly those based on the layered security and defense-in-depth (DiD). Healthcare professionals, administrators, researchers, and regulators all need to understand cybersecurity requirements and challenges in their products and services. Healthcare administrators, such as hospital directors and quality managers, must adopt proactive cybersecurity management strategies. Healthcare researchers, including academics and students, must stay updated on current trends and conduct research. Healthcare regulators, such as government agencies and professional associations, must develop and implement effective cybersecurity norms and guidelines to ensure the safety and security of healthcare systems.

Security solution architects, technocrats, hospital administrators, medical practitioners, security consultants, biomedical engineers, clinical engineers, CISOs, DPOs, and policymakers will find this book beneficial. They will gain an understanding of healthcare cybersecurity concepts, challenges, mitigation strategies, healthcare security standards, secure communication, attack vectors, and risk assessment. The book is also intended for students pursuing automation, biomedical engineering, computer science, and cybersecurity, as well as professionals involved in production, testing, supply chain management, design, development, and technology transfer of advanced medical devices. Additionally, this book aims to assist those who aspire to a career in healthcare management after completing their MBBS. Patients who want to safeguard their digital health data may also be intrigued by this book.

Salient Features

The healthcare industry is a lucrative target for cybercriminals, as patient data is a coveted commodity. This makes cybersecurity vital for healthcare delivery organizations (HDOs). Further innovation with cutting-edge connected devices (IoMT, surgical robots, etc.) complicates the HDO network and demands holistic cybersecurity management. This book is an awakening effort that elucidates the current HDO ecosystem, the threats, the motives of cybercriminals, the cyberattack surfaces, and the DiD strategies for a proactive defense.

The Book

1. Defines the roles and duties of clinical engineers, biomedical engineers, and ICT specialists in the healthcare industry.
2. Discusses the cybersecurity of advanced medical devices and procedures.
3. Discusses electronic health records (EHRs) and cybersecurity issues, informed consent and data anonymization, and a strategy for data protection in HDOs.
4. Discusses hospital networks, zone-based architecture, and how it is used to deploy products, particularly embedded devices and IoMT.
5. Delivers a thorough grasp of the physical and digital security of an HDO to the reader.
6. Describes the cyber dangers, weaknesses, and mitigation strategies that affect healthcare systems.
7. Presents fundamental strategies for locating security holes, reducing vulnerabilities, and building stronger cybersecurity.
8. Gives a thorough understanding of the concept, design, development, technology transfer, supply chain, post-market surveillance, maintenance, decommissioning, and disposal of cybersecurity in high-tech hospital networks and medical device development.
9. Offers crucial information that enables clinical engineers to improve security systems and advance the field of healthcare cybersecurity.
10. Explains how to build security capable hospitals.
11. Describes the need, necessity, and the strategy integrating cybersecurity in TQM.
12. Describes the current norms and regulations for healthcare cybersecurity.

Structure of the Book

This book is intended for hospital administrators, physicians, biomedical engineers, CISOs, and DPOs to proactively incorporate and practice cybersecurity in healthcare delivery organizations (HDOs). The first chapter of this book introduces cybersecurity in HDOs. Due to the increasing complexity of the HDO ecosystem with innovations like IoMT, surgical robots, and high-tech connected devices, comprehensive cybersecurity management is essential. This book aims to raise awareness by providing information about the current HDO ecosystem, cyber threats that HDOs must contend with, the motivations behind attacking HDOs, cyber-attack surfaces, and proactive security techniques such as DiD methods.

***Chapter 1 Growing Cyber Threats & Complex Healthcare Eco-Systems*:** Healthcare delivery organizations (HDOs) are critical information infrastructure (CII) and must protect their infrastructure and electronic health records (EHR). This chapter discusses ICT and cyber risks, hackers, attack issues, cybersecurity challenges, and the roles of stakeholders like biomedical engineers, clinical engineers, ICT professionals, DPOs, and CISOs. It also explores ethical and legal aspects of healthcare cybersecurity, such as GDPR, and the future of cybersecurity in healthcare. The chapter concludes by looking at the future of cybersecurity in healthcare, considering the global perspective, the next generation of cyber-attacks, and the human factors and security capabilities of hospitals. The chapter aims to raise awareness and provide guidance on protecting the healthcare sector from cyber threats.

Chapter 2 Cybersecurity & Cutting-Edge Healthcare Technologies: This chapter explores the interplay between cybersecurity and medical technologies in the modern healthcare sector. It covers best practices for securing embedded systems, the benefits and challenges of surgical robots and telesurgery, telemedicine, IoTs and IoMTs, mobile health applications, big data and cloud computing, and artificial intelligence and blockchain technology. The chapter also discusses the challenges and opportunities of these technologies, highlighting the need for secure network communication, privacy, and security regulations.

Chapter 3 Cybersecurity & Digital Health Data Protection: This chapter explores the protection of digital health data, particularly electronic health records (EHRs), from cyber threats, data integrity, and data anonymization. It covers the types and sources of cyber threats, the potential impacts and costs of data breaches, and the challenges of securing EHR systems and networks. The chapter also discusses the importance of data integrity, data anonymization, and informed consent. It also discusses the implementation issues and future of

EHR, the need for training and empowerment, patient awareness, EHR interoperability, legal frameworks for EHR data protection, the impact of GDPR on healthcare data governance, and strategies for healthcare delivery organizations (HDOs) to comply with the DPDP Act(2023). It also discusses the use of open source intelligence (OSINT) in medical care and its benefits and challenges. The chapter provides a comprehensive overview of protecting digital health data and offers practical guidance and recommendations for the healthcare sector.

Chapter 4 QA of Medical Devices: Integrating Cybersecurity & Total Quality Management: For the accurate diagnosis, prevention, and treatment of illnesses, you must test your medical devices. The functionality of the medical equipment can be impacted by a number of things, including legal requirements, cyber-attacks, and software bugs. Therefore, quality assurance and quality Control have become essential in medical device testing in order to guarantee high-quality output. This chapter discusses how cybersecurity can be a part of TQM and how it relates to quality assurance of medical devices. This chapter covers the QA of medical devices from the perceptive of cybersecurity and how cybersecurity can be component of TQM.

Chapter 5 Product Life Cycle of Secure Medical Devices: Security experts must make sure the medical device life cycle is secure from conception to decommissioning, both inside the healthcare sector and in other security domains. In order to achieve this, cybersecurity must be incorporated into the product during the design phase, comprehensive multi-layered defensive mechanisms must be provided to pre-market and market-ready products, and ongoing security risk management must be provided once the medical device has been placed on the market, during deployment and operation in HDOs, and during decommissioning when it reaches the end of its useful life. A comprehensive description of these aspects is provided in this chapter.

Chapter 6 Defense-in-Depth (DiD) and Secure Dataflow: The chapter introduces the concept of defense-in-depth and information assurance, which are essential for protecting the confidentiality, integrity, and availability of data and services in HDOs. The chapter then provides a holistic view of HDO network architecture and the potential threats faced by security teams. The chapter emphasizes the need and benefits of network segmentation, which is a key strategy for reducing the attack surface and limiting the impact of breaches. The chapter explains how to segment HDO networks based on operational technology (OT) and information technology (IT) domains, as well as by functionality and risk level. The chapter also covers the topics of electronic security perimeter, layered security, end point security, OT-IT integration, bring your own device (BYOD) and mobile device management (MDM) security,

secure remote access, and security operations centre (SOC). The chapter concludes with some case studies of layered security in hospitals, highlighting the lessons learned and the best practices for improving HDO network security.

Chapter 7 Managing Cyber Risks in the Medical Device Supply Chain: This chapter explores cybersecurity and supply chain security in the healthcare sector, focusing on cyber threats, upstream and downstream stages of medical device design, development, production, distribution, and maintenance, regulatory requirements, supply chain cyber-attacks, outsourcing and third-party vendor management, mitigation strategies, and zero-trust security models. It discusses the benefits and challenges of outsourcing and using third-party vendors for cybersecurity, as well as the methods and tools for assessing and managing third-party vendor cybersecurity. The chapter also discusses the benefits and challenges of zero-trust security, which shifts from a traditional perimeter-based model to a data-centric and identity-based model. The chapter aims to provide a comprehensive overview of cybersecurity and supply chain security in the healthcare sector.

Chapter 8 Cybersecurity: A Risk Based Approach: This chapter explores cybersecurity in healthcare, focusing on identifying, assessing, managing, and responding to cyber threats and incidents. It covers topics such as the anatomy of a cyber-attack, vulnerability assessment (VA) in healthcare delivery organizations (HDOs), penetration testing (PT), vulnerability management, risk assessment, incident response and reporting, cyber threat intelligence and information sharing, cyber forensics of medical devices, cyber insurance in healthcare, and collaborative approaches to enhance healthcare cybersecurity. The chapter aims to provide a comprehensive overview of cybersecurity in healthcare and offer practical guidance and recommendations for the healthcare sector. It also discusses the role of AI in cybersecurity risk assessment and the need for collaboration among stakeholders in healthcare cybersecurity. The chapter aims to provide a comprehensive and up-to-date overview of cybersecurity in healthcare, offering practical and actionable guidance and recommendations for the healthcare sector.

Chapter 9 Security-Capable HDOs: Design Principles & Best Practices: System redundancy for seamless operation should be designed in accordance with applicable institutional standards, best practices, and regulatory requirements Systems that have both primary and secondary (backup) capabilities should be included in the design and the primary and secondary delivery should be designed as separated redundant systems to eliminate single points of failure. This chapter presents the most essential components for an HDO to be a security-capable hospital. A comprehensive description of these aspects is provided in this chapter.

Chapter 10 Regulatory Compliance, Policy & Governance: Of all the verticals that need a complete data governance policy – healthcare might be at the top. Consider the incredible amount of healthcare data that exists for any human, the personal nature of healthcare data, and the life or death scenarios that depend on accurate data. It makes sense that data governance in healthcare is super important. Security standards, regulations, policies, and procedures for HDOs, components and levels of security policies, steps for developing a cybersecurity policy, characteristics of a security-capable HDO, principles of data security governance, and metrics of security maturity are discussed in this chapter.

Contents

Table of Contents

List of Figures

List of Tables

Acknowledgement

Let's take a moment to thank God for his kindness in giving us the chance, mind-set, and ambiance needed to produce such a complex technical book. The two most important things for having a tireless body to write a complex technical book are inspired friends and a relaxed mind. Therefore, the authors greatly benefited from having colleagues and friends with a keen interest in technology who were willing to spend time discussing intricate technical issues and provide feedback on the format and content of this book. It would have been a nervous activity otherwise. We truly thank all of our friends, colleagues, and classmates who supported us by reading and leaving comments on the presentation of this, and we do remember our parents with respect at this point in time.

We sincerely thank Swami Rhithambarananda of Sivagiri Mutt for his spiritual and moral mentoring, without which we would not have been able to embark on this endeavor and learn about the world of technical book writing. We remember our dear professors and teachers with respect for their support and blessings. We also remember our cousins for their genuine love and support, which have also been crucial in non-academic aspects. We express our gratitude to Bhuvananji of the Ganesholsava Trust, Dr. Somanath, the current chairman of ISRO, and Dr. G. Madhavan Nair, former chairman of ISRO, for their blessings and support. Finally, with great reverence, we dedicate this modest work to Sree Narayana Gurudev of Sivagiri Mutt.

We respect the time, effort, and energy that Dr. G. Geetha of SCTIMST, Prof. Sreejith Alathur of IIM, Kozhikode, and Dr. Dittin Andrews of C-DAC, Thiruvanathapuram put into reviewing this book. We also appreciate their encouraging remarks and insightful ideas. When a circumstance in the book seems to call for it, certain points have been purposefully repeated to emphasize how important these concepts are. Even with our best efforts, there could still be a few shortcomings in the book. They may not be corrected without the help of knowledgeable reviewers and readers; suggestions for making this book better are always appreciated. The authors will definitely be privileged if the readers get the intended sense, which is the sole aim of this effort.

Additionally, we want to thank everyone who works in the field of operational technology (OT) cyber-security and is motivated by their enthusiasm, dedication, obsession, and genuine sense of doing the right thing. The best security personnel are those who have an ethical goal in mind. We sincerely appreciate the publishers' assistance and collaboration on this project, as well as the cover graphic designers.

K S Manoj & G Jenin

Authors' Details

K. S. Manoj is an engineering physicist and an electronics engineer with a design interest in industrial cybersecurity by deploying defense-in-depth (DiD) and layered security strategies. He has over 30 years of expertise in industrial automation, biomedical engineering, power system engineering, and industrial (OT) cybersecurity and is an alumnus of the Department of Electronics at CUSAT in India. He worked for KELTRON, SCTIMST, and KSEBL before joining Intelegrid ECC(P)Ltd as an R&D cybersecurity consulting engineer. With numerous technical books and articles to his credit, he is a prolific writer. He may be contacted at *ksmanoj321@yahoo.com.*

G.Jenin is a cybersecurity auditor and analyst is an alumnus of the University of Kerala**.** He has worked for KSEBL for almost 25 years, where he played a key role in examining and auditing the cybersecurity facets of projects involving data centre, disaster recovery centre, security operations centre, and SCADA-based power system automation. He currently works with Intelegrid Engineering & Cybersecurity Consulting (P) Ltd as a senior security analyst. At *g.jenin@gmail.com*, you can get in touch with him.

Reviews

The book ‘STOP CYBER HEMORRHAGE: A Comprehensive Guide to Preventing Data- Bleeding and Protecting Lives in Healthcare’ by K S Manoj and G Jenin gives an overall view of the kind of cyber resilience in healthcare including the present escalation in cyber threats.

This book is intended for hospital administrators, physicians, biomedical engineers, CISOs etc. The book is divided into ten chapters that vividly describe growing cyber threats, Cutting Edge Medical Technologies, methods for protecting data, methods to secure medical devices, managing cyber risks in the medical device supply chain, best practices, policies etc. All aspects of cyber risks and security from the very basic to the most advanced form is explained.

“This book is a must for every healthcare person, be it an ordinary citizen or the Managing Director / Chairman of a health delivery organization. The content of the book not only updates about the necessity of cybersecurity in healthcare but it also talks about the various ways in which cyber risks can be reduced.

This book brings to readers a wholesome experience by being an amalgamation of the benefits and risks of modern technology in healthcare. Hence, this book is a must-buy for all, especially healthcare groups if you are concerned about cyber threats.”

Dr. G.Geetha B.Tech (EC),M.Tech (CS), Ph.D (Bioinformatics)
Scientist G (Senior Grade), CISO, Computer Division
Sree Chitra Tirunal Institute For Medical Science & Technology
An Institution of National Importance, Department of Science and Technology, Govt. of India

---

The book's treatment of cybersecurity in the healthcare sector, focusing on how it addresses the protection of health data and infrastructure make this book a valuable addition to the domain of cybersecurity and healthcare. A meticulous authorship offering, the expertise of K S Manoj and G Jenin serves as a timely reminder to Health Delivery Organizations (HDOs) to better understand their health data ecosystem. An inherent merit of the book is its comprehensive technical depth and pragmatic understanding of the intricate healthcare ecosystem. The detailed examination of embedded systems, surgical robots, telemedicine, Internet of Medical Things (IoMT) and electronic health records (EHRs) as well as the corresponding protection strategies is especially remarkable. It demonstrates how vulnerable these technologies are to

cybercriminal attacks. A granular look into the product life cycle of medical devices, Defense-in-Depth (DiD), zero-trust and the implementation of Total Quality Management (TQM) in healthcare technology underscore the criticality of integrating cybersecurity measures at every phase. Regulatory compliance and governance section give the book authenticity and practical relevance in the era of strict health data protection regulations worldwide.

"*The necessity for this book arises from the fact that its authors, who possess profound expertise in cybersecurity, industrial automation, and bio-medical engineering, contribute a valuable perspective to the domain of health data security*".

Prof.(Dr) Sreejith Alathur,
Professor, Indian Institute of Management, Kozhikode,
An Institution of National Importance, Department of Science and Technology,
Govt. of India

This book has a well-organized structure, but it would be even more helpful for the readers if the "further reading" section was presented at the end of each chapter rather than presented at the end of the book. The sections on collaborative methods for cybersecurity, future developments in cybersecurity, and the human component in healthcare cyber-security are very engaging and inspiring. They spark the readers' interest and motivate them to learn more. This book also provides a brief introduction to the OWASP top 10 for web and mobile applications, SANS 25, AI, machine learning, blockchain technology, predictive analytics, and data integrity. These topics are fascinating and cutting-edge, and they invite the readers to engage in further research.

Dr. Dittin Andrews, Scientist, Centre for Development of Advanced Computing, Trivandrum, India

This book "STOP CYBER HAEMORRHAGE: A Comprehensive Guide to Preventing Data-Bleeding and Protecting Lives in Healthcare is a first of its kind, hence a must read for every healthcare person, be it an ordinary citizen or the managing director or chairman of a health delivery organization. The content of the book not only updates on the necessity of cybersecurity in healthcare, but it also talks about the various ways in which cyber risks can be reduced. This book brings readers a wholesome experience by being an amalgamation of the benefits and risks of modern technology in healthcare. Hence, this book is a must-buy for all, especially healthcare groups, if you are concerned about cyber threats.

-Dr. G.Geetha, CISO, Sree Chitra Tirunal Institute for Medical Science & Technology, India

The book provides a comprehensive understanding of cybersecurity in the healthcare sector, focusing on protecting health data and infrastructure. It examines embedded systems, surgical robots, telemedicine, IoMT, and EHRs, highlighting their vulnerability to cybercriminal attacks. The book also discusses product life cycles, defense-in-depth, zero-trust, and Total Quality Management in healthcare technology. The necessity for this book arises from the fact that its authors, who possess profound expertise in cybersecurity, industrial automation, and bio-medical engineering, contribute a valuable perspective to the domain of health data security.

-Prof.(Dr) Sreejith Alathur, Professor, Indian Institute of Management, Kozhikode, India

This book has a well-organized structure and the sections on collaborative methods for cybersecurity, future developments in cybersecurity, and the human component in healthcare cyber security are very engaging and inspiring. They spark the readers' interest and motivate them to learn more. This book also provides a brief introduction to the OWASP TOP 10 for web and mobile applications, SANS 25, AI, machine learning, blockchain technology, predictive analytics, and data integrity. These topics are fascinating and cutting-edge, and they invite the readers to engage in further research.

-Dr. Dittin Andrews, Scientist, Centre for Development of Advanced Computing, India

*Hospitals must have cybersecurity; it is a must, not optional. It must be integrated as security during the HDO design phase, adhering to the principles of cyber-informed engineering (CIE) and seamlessly maintained. In order to prevent harm to patients and a loss in patient trust, hospitals need to act swiftly. In view of this, "**STOP CYBER HAEMORRHAGE: A Comprehensive Guide to Preventing DataBleeding and Protecting Lives in Healthcare**" is an essential book for everyone concerned about software-based medical procedures, security, and patient privacy.*

E-ISBN:978-93-6252-669-4

9 789362 526694

MRP Rs. 350/-

Selfypage Developers Pvt Ltd