The Cybersecurity Guide to Governance, Risk, and Compliance

Jason Edwards
Griffin Weaver

The Cybersecurity Guide to Governance, Risk, and Compliance

The Cybersecurity Guide to Governance, Risk, and Compliance

Dr. Jason Edwards
New Braunfels
TX, USA

Griffin Weaver
San Antonio
TX, USA

WILEY

This edition first published 2024

Registered Offices
John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, USA
John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, UK

For details of our global editorial offices, customer services, and more information about Wiley products visit us at www.wiley.com.

Wiley also publishes its books in a variety of electronic formats and by print-on-demand. Some content that appears in standard print versions of this book may not be available in other formats.

Limit of Liability/Disclaimer of Warranty

While the publisher and authors have used their best efforts in preparing this work, they make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives, written sales materials or promotional statements for this work. This work is sold with the understanding that the publisher is not engaged in rendering professional services. The advice and strategies contained herein may not be suitable for your situation. You should consult with a specialist where appropriate. The fact that an organization, website, or product is referred to in this work as a citation and/or potential source of further information does not mean that the publisher and authors endorse the information or services the organization, website, or product may provide or recommendations it may make. Further, readers should be aware that websites listed in this work may have changed or disappeared between when this work was written and when it is read. Neither the publisher nor authors shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

Library of Congress Cataloging-in-Publication Data applied for

Hardback ISBN: 9781394250196

Cover Design: Wiley
Cover Image: © Andriy Onufriyenko/Getty Images

Set in 10.5/13pt Muli by Straive, Chennai, India

Dedication by Griffin Weaver

As I present this book on cybersecurity and governance, coauthored with immense dedication and passion, my thoughts turn not only to the profound complexities of our digital world but also to the incredible journey that has led me here. As a legal expert deeply entrenched in the nuances of cybersecurity, I've embarked on this endeavor with a singular purpose: to bridge the gap between theoretical knowledge and practical application in a field that is as challenging as it is essential.

To my wife, Whitney, and our three children, Harper, Gideon, and Flynn, my journey in this field is a testament to the balance between pursuing professional passions and cherishing the invaluable support of family. It is with this balanced perspective that I've approached the writing of this book, aiming to infuse it not just with legal and technical insights but also with the underlying values of dedication, curiosity, and perseverance.

Cybersecurity and the law are not just areas of professional interest to me; they are vital pillars upon which our digital society rests. In writing this book, my hope is to illuminate these complex subjects for a diverse audience, from students who are just beginning their academic pursuits to seasoned practitioners looking to deepen their understanding and enhance their skills.

The landscape of cybersecurity is ever-evolving, and with it, the legal frameworks that govern our digital interactions. It is my earnest desire that this book serves as a beacon, guiding readers through the intricacies of cybersecurity and governance with clarity, depth, and relevance. May it inspire you to explore further, question deeper, and contribute to the shaping of a secure, ethical digital future.

Dedication by Jason Edwards

This book is dedicated to my family, whose unwavering support and love have been the cornerstone of my endeavors; to my wife, Selda, whose wisdom and strength have been my guiding light; and to my children, Michelle, Chris, Ceylin, and Mayra, who inspire me daily to be the best version of myself. The book is a testament to my professional journey and a reflection of the values and resilience you have instilled in me.

I acknowledge my fellow veterans and colleagues in the cybersecurity community, who have been comrades and mentors on this challenging yet rewarding path. Your camaraderie and insights have been invaluable in shaping the perspectives shared on these pages. A special acknowledgment goes out to those who serve in silence, dedicating their lives to the safety and security of our digital world.

This book is also dedicated to educators, students, and professionals in cybersecurity and related fields. May this work serve as a beacon, guiding you through the complexities of governance, risk, and compliance in our ever-evolving digital landscape. Your commitment to learning and adapting will drive us forward in these unprecedented times.

And, with a wry smile, I dedicate this book to the indomitable spirits of the “A7” project team. For two years, we waded through a quagmire of confusion and challenges that often teetered on the edge of chaos. Yet, against all odds, we emerged victorious. This dedication is a salute to our collective perseverance, ingenuity, and slightly warped sense of humor that saw us through the hellish yet unforgettable adventure of “A7.”

Contents

Purpose of the Book

The first step in any journey of understanding is to clarify the why. This book was born out of a need for comprehensive yet practical insights into cybersecurity governance, risk management, and compliance. Navigating these complex domains can be a daunting task without a reliable roadmap. This book aims to guide, elucidating the pathways through the labyrinth of cyber threats and security measures, organizational policies, and regulatory requirements.

This book aims to bridge the knowledge gaps in the dynamic cybersecurity field. While many resources tackle the subject, they often focus on a narrow aspect, leaving you to stitch together various pieces of information. This guide takes a different approach to provide a holistic understanding of cybersecurity from a governance, risk, and compliance perspective.

A critical aspect of cybersecurity is compliance. Compliance is not just about checking off boxes on a list. Instead, it is about integrating practices safeguarding an organization's data and digital assets. This book strives to provide insights that can elevate an organization's compliance activities from mere tasks to strategic initiatives, thus enhancing the resilience of the enterprise against cyber threats.

Professional development is a continual process. The pace of technological change necessitates that professionals in the field of cybersecurity continually upgrade their skills and understanding. This book is designed to be a valuable tool in that process, providing in-depth insights and practical approaches that can be applied in various professional settings.

The regulatory landscape related to cybersecurity is multifaceted and ever-evolving. Without a clear understanding of these complexities, an organization can easily find itself noncompliant and vulnerable. This book aims to aid you in navigating this challenging environment, providing you with the knowledge needed to build a cybersecurity program that aligns with regulatory requirements.

While this book strongly focuses on financial compliance, the insights and guidance can be applied to all industries. Cyber threats and the need for effective cybersecurity measures are universal issues impacting businesses of all sizes and sectors. Therefore, this guide can be beneficial for a diverse range of professionals.

Finally, this book is not just about learning but also about sharing experiences. You contribute to the book's purpose by exploring the content and applying the insights in your professional environment. By adding your expertise to the collective wisdom, you can help others navigate their cybersecurity journey.

Target Audience

The subject of cybersecurity touches a wide range of professionals. One of the key strengths of this book is its cross-industry applicability, which means it can benefit a diverse audience. This guide targets cybersecurity professionals, from those beginning their careers to seasoned experts. It provides foundational knowledge and in-depth insights into cybersecurity governance, risk, and compliance.

Compliance officers are another primary audience for this book. These professionals ensure that their organizations adhere to the necessary regulations and standards. Compliance officers can more effectively align their practices with the organization's cyber risk management efforts with a clear understanding of cybersecurity principles.

IT professionals can gain substantial value from this guide, whether directly involved in cybersecurity or not. Cybersecurity is not a stand-alone function; it is deeply interwoven with other IT practices. Therefore, understanding cybersecurity principles can aid IT professionals in designing, implementing, and maintaining systems and networks that are resilient against cyber threats.

For business executives, understanding cybersecurity is about much more than technology; it is about ensuring business continuity and preserving stakeholder trust. This book aims to give executives the knowledge they need to make informed decisions related to cybersecurity and drive cyber risk governance in their organizations.

The book is equally valuable for boards of directors. Boards are responsible for overseeing risk, including cyber risk. With the knowledge in this guide, board members can play a more active role in directing their organization's cybersecurity strategy and ensuring compliance with relevant regulations.

Legal professionals can also find value in this book. As laws and regulations related to cybersecurity continue to evolve, legal professionals must stay informed. This guide can help them understand cybersecurity's technological and compliance aspects, enabling them to provide more practical advice and support to their clients or organizations.

Regulators are the final primary audience for this book. Effective regulation requires a deep understanding of the subject being regulated. This guide can support regulators in developing and implementing effective cybersecurity regulations by providing comprehensive insights into cybersecurity from a governance, risk, and compliance perspective.

Structure of the Book

As authors, we have crafted this book to offer a well-rounded and engaging journey through cybersecurity governance, risk, and compliance. The book is thoughtfully divided into specific sections, each concentrating on a unique aspect of the subject. These sections are filled with in-depth discussions, practical tips, and real-world examples that help bring the subject to life.

Our book is not just for sequential reading from cover to cover. We have designed it so you can read specific sections depending on your immediate needs or interests. Each chapter is independent, providing a focused exploration of a distinct cybersecurity dimension. This means you can always revisit or explore new sections at your own pace and according to your requirements.

Throughout the book, we have highlighted key themes such as the crucial role of cybersecurity in an organization's strategy, the use of risk management in cyber defense, and the importance of compliance in safeguarding against cyber threats. We believe that understanding these themes is fundamental to grasping the complex world of modern cybersecurity.

We've also included over 70 Key Risk Indicators (KRIs) and Key Performance Indicators (KPIs) and references to relevant regulations, standards, and online resources. These additions are intended to aid you in measuring your cybersecurity efforts and to provide extra material for your learning.

We want you to understand and act on what you learn. So, after each section, we offer a few actionable recommendations. With over 1300 suggestions in the book, we are equipping you with the tools to translate the knowledge into practical steps.

One of our favorite features of the book is the real-life case studies and examples. They illustrate the concepts we are discussing and help you envision how they can be applied in real-world situations.

Finally, we have mapped the Federal Financial Institutions Examination Council (FFIEC) Information Security Handbook to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). This will serve as a guide, helping you navigate these critical regulatory and guidance documents. It will enable you to understand their connections and overlaps for an efficient approach to compliance, thus bolstering your cybersecurity stance.

Foreword by Wil Bennett

Over the past 30 years in cybersecurity, I've witnessed its transformation from a simple defense mechanism to an intricate architecture interwoven with governance, risk, compliance, leadership, technology, and business strategies. This evolution was unimaginable three decades ago.

Having worked extensively in crafting and steering cybersecurity strategies, I've been fortunate to observe the expertise and dedication of Jason and Griffin closely. Their combined strengths in cybersecurity strategy, regulatory remediation, and legal aspects have proved crucial in meeting contemporary cybersecurity challenges.

The Cybersecurity Guide to Governance, Risk, and Compliance represents the wealth of knowledge and practical insights that Jason and Griffin possess. Having collaborated with Jason at USAA, I can attest to his unwavering commitment and strategic expertise in cybersecurity, especially in regulatory remediation. Similarly, Griffin's expertise in legal aspects has significantly shaped our understanding of cybersecurity laws and regulations.

This book delves deeply into the multifaceted realm of cybersecurity in today's age. Designed for professionals across the board, from seasoned cybersecurity veterans to business leaders, auditors, and regulators, this guide integrates the latest technological insights with governance, risk, and compliance (GRC). Every chapter brims with actionable recommendations from the authors' vast experience and forward-thinking vision.

Readers will find a comprehensive range of topics, from key performance indicators and cutting-edge technological advancements to risk management strategies and regulatory insights. This book stands not just as a testament to the knowledge of Dr. Jason Edwards and Griffin Weaver but also as a beacon guiding those eager to navigate current and future cybersecurity challenges.

In sum, this book is more than a text – it's an enlightening compass for traversing the dynamic terrain of cybersecurity governance, risk management, and compliance. I wholeheartedly endorse this guide as a pivotal resource for anyone striving for cybersecurity excellence and resilience.

—Wil Bennett
Vice President,
Chief Information Security Officer
CISSP

Foreword by Gary McAlum

In an era of constant digital evolution and deepening ties between governance, risk, compliance, and cybersecurity, *The Cybersecurity Guide to Governance, Risk, and Compliance* emerges as a pivotal resource. This guide combines practical insights with actionable strategies, providing a detailed road map through the complexities of modern cybersecurity.

During my tenure as Chief Security Officer at USAA, I had the privilege of working with Griffin Weaver and Dr. Jason Edwards. Griffin's expertise as a cyber attorney enhanced our cybersecurity strategies, ensuring their robustness and alignment with regulatory requirements. Dr. Jason Edwards' strategic approach and practical experiences significantly contributed to our efforts, and their insights are evident in this book.

Jason and Griffin have crafted a versatile guide suitable for beginners, educators, cybersecurity professionals, and executive leaders. With over 1300 actionable recommendations, KPIs, and KRIs, it offers a comprehensive route to a more secure cyber environment. From my role as Chief Information Security Officer, I appreciate the guide's exploration of cutting-edge topics like AI, cloud, and quantum computing, providing insights into their potential impacts on security and compliance.

This guide's coverage of governance, leadership, legal frameworks, and regulatory nuances ensures organizations can establish resilient cybersecurity postures. Each chapter delivers actionable knowledge, making the guide thorough and practical.

In summary, this book is a testament to the authors' expertise and commitment to advancing cybersecurity knowledge. It's a valuable resource for anyone in the field of cybersecurity, governance, risk, and compliance.

—Gary McAlum
Senior Vice President,
Chief Information Security Officer
CISSP

Acknowledgments

This journey of writing "Mastering Cybersecurity" has been one of profound learning, discovery, and collaboration. It would not have been possible without the unwavering support of my family and the invaluable insights from a remarkable community of cybersecurity professionals.

First and foremost, I extend my deepest gratitude to my family—my wife, Selda, and our four children, Michelle, Chris, Ceylin, and Mayra. Your love, patience, and encouragement have been my anchor and inspiration through the countless hours dedicated to this project.

I also wish to express my sincere thanks to the incredible individuals I have had the privilege of meeting and working within cybersecurity. Each of you has contributed to this book in ways words can hardly capture:

Wil Bennet
Gary McAlum
Rob Fisher
Wendell Ladd
Brady Justice
Kurt Lubelan
Kim Kemp
Don Wuebben
Brennan Holland, Esq.
Derek Burkes
Amy Reed
Kanishk Mehta
Chris Gile
Jodi Marlette
Dr. Patrick Woods
Dr. Paul Cooper
Joe Arthur
Mike Stewart
Eric Fisch
Sandra Cerda
Jason Witty
Jeff Spaeth
Clark Cummings
Selda Edwards
Derek Burkes (acknowledged twice for their exceptional contribution)
Meltem Burkes

Clarke Cummings
Kristyn Lette
Chinho Ko
Subash Poudyal, PhD
Kul Subedi, PhD
Jim Huseman
Gordon Bjorman
Dr. Angela Dogan
Jerry Smith
Leead Negri
Kesha Lindbergdashwork
Michael Castillo
Kelley Dadah

Your expertise, enthusiasm, and willingness to share knowledge have enriched this book and contributed to our cybersecurity community's growth and resilience.

To those embarking on or considering a career in cybersecurity, let this book serve not just as a guide but as a testament to the power of collaboration, curiosity, and continuous learning. The path to mastering cybersecurity is challenging but immensely rewarding. It offers the opportunity to impact safeguarding our digital world significantly. May you find inspiration in these pages and from the people mentioned above to pursue your passions, overcome obstacles, and contribute to a safer, more secure future for all.

Thank you, one and all, for being part of this journey.
Warmest regards,
Dr. Jason Edwards