*Foreword by **Phil Gardner**, CEO, IANS Research*

Enterprise Cyber Risk Management as a Value Creator

Leverage Cybersecurity for Competitive Advantage

—

Bob Chaput

Apress®

Enterprise Cyber Risk Management as a Value Creator

Leverage Cybersecurity for Competitive Advantage

Bob Chaput

Foreword by Phil Gardner, CEO, IANS Research

Apress®

Enterprise Cyber Risk Management as a Value Creator: Leverage Cybersecurity for Competitive Advantage

Bob Chaput
Belleair Beach, FL, USA

ISBN-13 (pbk): 979-8-8688-0093-1 ISBN-13 (electronic): 979-8-8688-0094-8
https://doi.org/10.1007/979-8-8688-0094-8

Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Susan McDermott
Development Editor: Laura Berendson
Coordinating Editor: Jessica Vakili

Distributed to the book trade worldwide by Springer Science+Business Media New York, 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail booktranslations@springernature.com; for reprint, paperback, or audio rights, please e-mail bookpermissions@springernature.com.

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at http://www.apress.com/bulk-sales.

Any source code or other supplementary material referenced by the author in this book is available to readers on the Github repository: https://github.com/Apress/Enterprise-Cyber-Risk Management-as-a-Value-Creator. For more detailed information, please visit https://www.apress.com/gp/services/source-code.

Paper in this product is recyclable

I dedicate this book to my wife, Mary.

It's like deja-vu all over again.

—Yogi Berra (1925–2015), American professional baseball catcher, manager, and coach.

Table of Contents

Endorsements for *Enterprise Cyber Risk Management as a Value Creator*

Throughout my 28 years in CISO roles at two of the highest-risk organizations in the world, I have sweated through countless budget and resource challenges and struggled to connect my cybersecurity program to business objectives in the minds of business leaders and our board. A major hurdle was that cybersecurity was viewed as risk avoidance—a cost center that did not add value, that is, a painful but necessary overhead. This book lays out the holy grail for cybersecurity, how to flip that script to make cybersecurity a business enabler and part of the core growth strategy, and how to integrate that approach into business strategy.

No one is more knowledgeable and qualified to make this case than Bob Chaput, who is a living legend in cybersecurity and an unmatched thought leader in enterprise cyber risk management (ECRM). He lays out a compelling case, with details on how to apply this thinking to your organization, and then provides a detailed road map for making it happen.

This should be mandatory reading for CISOs, CFOs, CEOs, and board members. It will close communication gaps and change the mindset because it shines a light on the opportunities to expand and accelerate business transformation and earn customer and stakeholder trust—through cybersecurity.

—Paul Connelly, First CISO at the White House and HCA Healthcare

Bob Chaput picks up where most books leave off by providing powerful insight into ECRM engagement by providing a factual background coupled with strategic examples that can and will have positive impacts on any company's cyber risk strategy and approach. This resource should become the standard guidebook for every risk manager, general counsel, CISO, CTO, C-suite, and board member who has an interest in or a concern around cyber and privacy liability and entire ECRM protocols.

—Kevin Hewgley, Senior Vice President,
Financial Services at Lockton Companies

In *Enterprise Cyber Risk Management as a Value Creator*, Bob Chaput's latest contribution to simplifying the often impenetrable field of cybersecurity, Bob turns from calling attention to the problem to helping us think differently about it. Are investments in cybersecurity a cost of doing business, with cost containment as the overarching goal? Is cybersecurity a "check the box" exercise, allowing us to throw up our hands if an adverse event occurs after we've checked all our boxes? Or is cyber a strategic priority meriting an offensive rather than defensive mindset? As always, Bob doesn't just pose the questions. He provides practical and timely answers alongside a wealth of real-world examples. A must-read for everyone from the cybersecurity novice to the seasoned pro looking for proper organizational focus on a business pandemic that has no miracle cure in sight.

—Ralph W. Davis, Independent Director/Board Advisor,
Operating Partner, The Vistria Group

Bob Chaput's latest book is a powerful read that explains cybersecurity in a new context, one that will be helping business leaders, including corporate directors, reframe cybersecurity as a critical part of the need for every organization to drive and create value. With so much economic

growth and output already dependent upon complex digital systems, this mindset will help leaders understand the importance of cybersecurity to the organization's future.

—Bob Zukis, CEO, Digital Directors Network

Enterprise Cyber Risk Management as a Value Creator delves deep into the critical realm of enterprise cyber risk management, providing a comprehensive guide to not just safeguarding against digital threats but also harnessing the power of cybersecurity as a catalyst for growth and innovation. Today, businesses and organizations are more reliant on technology and data than ever before, and the need for robust cybersecurity practices cannot be overstated. This book serves as an indispensable resource, offering both practical wisdom and strategic insights to navigate the ever-evolving landscape of cyber risks.

Authored by Bob Chaput, a seasoned expert in the field, this material is backed by a wealth of knowledge derived from real-world experiences. It's not merely a theoretical exercise but a hands-on manual for organizations seeking to proactively protect their digital assets and leverage them for strategic advantage. The lessons to be learned from this book are not confined to a single sector or industry. Its principles are universally applicable, ensuring that both large and small organizations can find applicable and valuable takeaways. It's not just about fortifying defenses; it's about adopting a proactive stance toward cybersecurity.

As data breaches and cyberattacks continue to make headlines, this book is a timely and crucial resource for organizations looking to safeguard their integrity and reputation. Moreover, it provides the tools and strategies needed to turn cyber risk management into a value creator, helping organizations thrive amid an era of digital transformation.

Enterprise Cyber Risk Management as a Value Creator is a guiding light in the intricate maze of cybersecurity. It's a valuable asset for organizations of all sizes, empowering them to not only withstand digital threats but emerge stronger, more resilient, and ready to seize the boundless opportunities of the modern digital age.

—Michael E. Whitman, PhD, CISM, CISSP
Executive Director, Institute for Cybersecurity Workforce Development
Professor of Information Security and Textbook Author

Having performed dozens of risk analyses for companies during my career at a public accounting firm, this book is a masterclass in strategic management of digital risks in an enterprise and provides great insight to turn digital risk management into a competitive advantage. This is a good resource for business leaders, security professionals, and anyone seeking to navigate the complex landscape of digital security. With profound insights and practical wisdom, it successfully highlights the critical role of cyber/digital risk management in driving business value. Bob Chaput's expertise shines through as he presents a comprehensive and forward-thinking approach to managing cyber/digital risks. The inclusion of actionable insights and practical frameworks adds immense value to the content, ensuring that readers can immediately apply what they've learned.

—Raj Chaudhary, Independent Director, Board Advisor,
Retired Cybersecurity Partner, Crowe LLP

Someone told me recently that "cybersecurity is boring." Cybersecurity *is* boring if it is other people listening to CIOs, CISOs, and other IT people talking about it. They understand the issues, the risks, the solutions. Cybersecurity *should not be boring* to people who don't live it but must make decisions about it—big decisions like staffing, funding, prioritization against other business issues. How do you talk about cybersecurity in meaningful ways with the full C-suite, with your board of directors or trustees?

Bob Chaput has answered that question and solved the problem with his latest book: *Enterprise Cyber Risk Management as a Value Creator*. For too long, cybersecurity has been viewed as a defensive play, a cost center. What if the tables were turned and executives and boards thought about cybersecurity in a positive light and as an opportunity to create competitive advantage and add value to the organization and drive business growth?

This book, using data, statistics, and real business examples, is a primer for redirecting and refocusing those discussions for the leaders who must be engaged in cybersecurity but for too long have stayed out of the fray. The book provides lots of guidance and many questions—in each chapter—to get the business to start answering the right questions and asking their own. Multiple studies (many cited in this book) clearly indicate that business leaders and consumers agree that establishing trust in products and experiences (AI, digital technology, data) that meet expectations will deepen trust and promote growth.

This is the book to start those conversations, up and down the organization. Cybersecurity isn't boring if you have the right people talking about it—here is how to engage those "right" people in your organization. You'll need to arm your IT, security, risk management, operational, and innovation leaders, but you'll use the learning to deeply engage the C-suite, the boards, and committees of the board in positive discussion around cybersecurity and how to leverage a more secure organization to move faster and drive new opportunities.

—David Finn, Health IT Advocate,
Recovering Healthcare CIO, Security and Privacy Officer
Baldrige Foundation Award for Cybersecurity Leadership Excellence

Enterprise risk management, and cybersecurity risk management in particular, is more important now than ever. Bob's book takes the reader through easy-to-follow steps and provides "food for thought" when implementing an ERM program. A compliment to any bookshelf.

—Rachel V. Rose, JD, MBA, Principal at
Rachel V. Rose—Attorney at Law, PLLC

Chaput's new book on enterprise cyber risk management is a tour de force on this subject. Building a value-creating ECRM culture is not a sprint or a marathon, but a relay. Making this book an all-team read for your leadership and the first part an all-board read is an excellent way to start building that culture.

—Nancy Falls, Independent Board Director and CEO,
The Concinnity Company

I heard a friend recently bemoaning the state of ECRM within their organization, "We do risk management as an art, not a science." Bob breaks ECRM down to science. Bob's prescription for ECRM is on point and execution-ready. I looked at the Table of Contents and jumped right to Chapter 8. Each organization I've been part of has had a different ECRM strategy. Bob's book helps distill what success looks like. Bob coaches the reader through aligning business strategy and ECRM strategy—I especially appreciated his wisdom on what "HOW your organization will conduct ECRM?" means. Now, the challenge is ours to learn and implement.

—Dan Bowden, Global CISO, Marsh

Where others have focused primarily on the defensive aspects of cyber risk management, Bob Chaput sees opportunities in ECRM. Mr. Chaput states: "Companies with a strong security posture are more likely to retain existing customers and attract new ones, as they value their data protection. This customer trust and brand loyalty can increase revenue and market share for the organization." C-suite and board members will ignore this timely advice at their peril. This book provides a road map

for the actions necessary to turn defensive thinking and processing into positive and value-creating actions and programs. Mr. Chaput makes the case for competitive and reputational advantage with logic, intelligence, and wit and draws from a depth of personal knowledge and experience in ECRM. Each chapter includes a set of "Questions Management and the Board Should Ask and Discuss," and these provide a great agenda of items worthy of consideration. You need this on your reading list.

—Stephen R. Rusmisel, JD, NACD.DC, 12-Year Independent Director and Former Lead Director of Life Storage, Inc.

Enterprise Cyber Risk Management as a Value Creator is a wide-ranging, thought-provoking book on an often-overlooked topic. Bob not only lays out why executives should care about ECRM but gives meaningful advice on how to get it done, and done well. He shares lessons, learned from years in the trenches, on how companies can get a handle on this vital yet often-misunderstood topic. This book addresses the key success factors as well as the common pitfalls in world-class risk management. It focuses on what leaders need to know and do, rather than get lost in the minutia of "this configuration of this system." This focus makes this book applicable across any industry that has to manage its cyber risk, which is, of course, all of them. The questions for the board of directors alone make this a worthwhile read—merely asking these questions will, at the very least, start you on the right path.

—William Niner, CISO

Bob Chaput in his latest book, *Enterprise Cyber Risk Management as a Value Creator*, works magic by revealing why cybersecurity risk is an essential ingredient of enterprise risk management. He introduces a new paradigm with enterprise cyber risk management (ECRM) being not just a defensive play, but as a proactive business enabler that can improve customer trust and stickiness through security services and increasing revenue sources by way of security capabilities. Bob lays out a well-understood foundation

by elegantly taking us through a comprehensive survey of the changing cybersecurity governance landscape. He skillfully reveals timely concepts such as the new federal regulations, the evolving financial industry governing body trends, and the quiet but growing court system precedents. Bob makes a sound case for why ECRM is a must-have concept that is to be understood and adopted by organizations today.

With tight financial margins facing many organizations, it is critical that business value is achieved with every dollar spent. Bob shows us how ECRM goes well beyond just being an IT problem. He clearly explains how ECRM can serve to propel an organization forward with a host of benefits, some of which are by facilitating digital transformation and innovation, attracting higher-quality investments, bringing in more talent, supporting mergers and acquisitions (M&A) activities, reducing regulatory exposure, assuring operational continuity and resiliency, and creating increased competitive advantage.

Bob makes it easy for us to not only comprehend this evolving topic but practically take steps forward to implement the ECRM strategy by outlining a simple five-step approach. He sheds light on how small and large organizations can justify and practically build out an appropriate budget needed to establish a successful ECRM program, with specific guidance on how to educate and win over the C-suite and board, including key questions to ask and discuss. Bob deftly reveals the role of ECRM Program and Cybersecurity Strategy within the context of ERM, tying cybersecurity strategy into the board's responsibilities. His insights on the business ownership of risk through authorization to operate and use are particularly compelling.

This text is a must-have for boards of directors, senior management, IT and security leaders, and anyone who wants to know just how vital ECRM can be in ensuring the future success of your organization.

—James Brady, PhD, Healthcare CIO/CTO/CISO

Legal Disclaimer

Although the information provided in this book may be helpful in informing you and others who have an interest in data privacy, security issues, and cyber risk management issues, it does not constitute legal advice. This information may be based in part on current international, federal, state, and local laws and is subject to change based on changes in these laws or subsequent interpretative guidance. Where this information is based on federal law, it must be modified to reflect state law where that state law is more stringent than the federal law or where other state law exceptions apply. Information and informed recommendations provided in this book are intended to be a general information resource and should not be relied upon as a substitute for competent legal advice specific to your circumstances. Furthermore, the existence of a link or organization reference in any of the following materials should not be assumed as an endorsement by the author. YOU SHOULD EVALUATE ALL INFORMATION, OPINIONS, AND RECOMMENDATIONS PROVIDED IN THIS BOOK IN CONSULTATION WITH YOUR LEGAL OR OTHER ADVISORS, AS APPROPRIATE.

Acknowledgments

First, I must start by thanking my wonderful wife, Mary, to whom I dedicate this book. From coffee, food, patience, and encouragement to keeping the cats off my lap so I could write, she was as important to this book getting done as I was. Thank you so much, Mary.

I would also like to thank all the colleagues, executives, and board members with whom I've had an opportunity to work over the course of my career at GE, Johnson & Johnson, Healthways, and Clearwater. Those career opportunities helped me develop as an information technology and cyber risk management executive, entrepreneur, and educator and, ultimately, prepared me to write this book. Everyone with whom I worked contributed to this book in some way. Thank you.

When I first considered writing this book, I prepared a book proposal and turned to several cybersecurity, regulatory, and risk management veterans to provide feedback on the concept of a book on positive cyber risks or cyber opportunities. I sincerely appreciate Jim Brady, Raj Chaudhary, David Finn, Rachel Rose, and Paul Connelly for their careful reviews and constructive and encouraging feedback.

I want to thank the entire publishing team at Apress and, specifically, Susan McDermott and Laura Berendson for their support and guidance throughout the process.

Finally, I would like to thank my friend, former colleague, and technical reviewer of this book, Jon Stone, for skull sessions on the subject matter in this book that go back to our early work on Clearwater Security together.

About the Author

Bob Chaput, NACD.DC, is the author of *Stop the Cyber Bleeding: What Healthcare Executives and Board Members Must Know About Enterprise Cyber Risk Management (ECRM)*. He is also Founder and Executive Chairman of Clearwater, a leading provider of cybersecurity, cyber risk management and compliance software, consulting, and managed services. As a leading authority in cybersecurity regulatory compliance and enterprise cyber risk management, Bob has assisted dozens of organizations and their business partners, including Fortune 100 organizations, wanting to improve their risk posture. Bob's degrees include an MA in mathematics from Clark University and a BA in mathematics from the Massachusetts College of Liberal Arts. In addition to the NACD Directorship Certification (NACD.DC), Bob holds numerous privacy, security, and cyber risk management certifications. He is a faculty member at IANS Research.

About the Technical Reviewer

Jon Stone is Senior Vice President and Chief Product Officer for Clearwater. In this role, he leads product innovation and product development.

Formerly, Jon served in numerous roles at Healthways, Inc., including Senior Portfolio and Project Management Director. He provided leadership of complex projects, product development, product strategy, and health information management consulting services to healthcare, managed care, and health information technology companies.

Before joining Healthways, Jon served as Director of Project Management and Healthcare Quality Metrics at Cigna Healthcare.

Jon has a master's in public administration and healthcare regulatory policy from the University of Tennessee at Chattanooga. He is certified as a Project Management Professional and has a Project Management for Information Systems certification from the University of Colorado.

Foreword

The issue of value creation has long been a contentious topic in cybersecurity. In this book, Bob Chaput makes a compelling argument that cybersecurity executives can function as value creators by taking on a leadership role in enterprise cyber risk management (ECRM). Bob then articulates a road map for how infosec executives, business leaders, and board members can work together to develop an ECRM-driven approach to security.

This book couldn't have come at a more critical time. The release of new cyber breach disclosure rules from the US Securities and Exchange Commission in July 2023 accelerated a growing movement among boards to govern cyber in a more strategic manner. Public companies are expected to identify the materiality of breaches and report on any material incidents within four days of determining materiality. To meet this need, the board, business executives, and CISOs must work together to develop a cohesive ECRM strategy. While the mandate only extends to public companies, the impact is expected to extend well beyond that jurisdiction.

Moving the cybersecurity conversation away from a focus on controls to an emphasis on ECRM is essential, and Bob is perfectly positioned to provide guidance here. From his executive technical leadership positions at GE, Johnson & Johnson, and Healthways to his work as CEO and, since 2018, Executive Chairman at Clearwater Compliance, not to mention his essential contribution as a member of the IANS Faculty, Bob has been exposed to countless executive cyber risk conversations. Bob is also a member of the National Association of Corporate Directors and has served

as a board advisor. This blend of experience allows Bob to not only speak with authority about ECRM issues but also provide practical guidance on how to deliver value to the business.

On a personal note, I've found Bob to be one of the best active listeners that I've ever met. Bob's other great skill is in his ability to distill his conversations with CISOs, business leaders, board members, and regulators into compelling, actionable insights. He cares deeply about this topic and it shows.

The wisdom he passes on in this book is not just for CISOs. Anybody with a responsibility to manage or govern enterprise cyber risk can benefit from Bob's guidance.

This work is essential in the industry today, especially because it is not an academic work. Instead, Bob provides real, practical guidance on how to build out an ECRM program and use that to influence the business effectively. It takes what is often a theoretical idea and presents tangible ways to make that value a reality. That actionability makes it stand out and turns it into a necessary read for executives seeking a perspective on enterprise cyber risk.

—Phil Gardner, CEO, IANS Research

Preface

It feels like we're going through a similar positive cycle to what I experienced early in my career in the mid-1980s when businesses recognized that information and information technology were an asset that companies could leverage for competitive advantage. In 1985, Michael E. Porter and Victor E. Millar published their seminal article, "How Information Gives You Competitive Advantage." In it, they highlighted how the information revolution critically affected competition, including changing industry structure, altering competition rules, creating competitive advantage by giving companies new ways to outperform their rivals, and spawning whole new businesses.

In this book, I highlight parallels between what happened over the course of the last 40 years and what is underway today with cybersecurity. In short, with the explosion in data, systems, and devices in connection with massive digitization programs that businesses have undertaken, it has become clear that organizations must safeguard these new information assets. Organizations, their C-suites, and boards must now realize that they can leverage a robust Enterprise Cyber Risk Management (ECRM) Program and Cybersecurity Strategy to create a competitive advantage for their organization. As Yogi said, it's like déjà vu all over again.

I was gratified to see how well executives, board members, and many stakeholders in the healthcare ecosystem received my book *Stop the Cyber Bleeding* in 2020. I appreciated the opportunity to give something back to the healthcare industry in the form of practical, tangible recommendations to establish, implement, and mature an ECRM program. For many organizations, building such a program represented paying off "ECRM debt" after having gone on a spending binge as they digitized what were,

in many cases, ancient clinical and administrative information systems. Most of that book focused on basics to build defenses to assure the confidentiality, integrity, and availability of data, systems, and devices against adversarial and other threat sources.

To a lesser extent, I addressed the possibility of a strong ECRM program becoming a business enabler. I discussed that not only is ECRM not an "IT problem," it can become a business enabler if appropriately handled. I briefly discussed how a robust ECRM Program and Cybersecurity Strategy might be leveraged as a competitive advantage. I presented several possible cyber opportunities, such as facilitating M&A, reducing the cost of capital, lowering executive risk insurance premiums, and helping their organizations compete with "technology invaders."

In *Enterprise Cyber Risk Management as a Value Creator*, I go further. I wrote this book to encourage organizations in all industries to start to move away from ECRM and cybersecurity strategy as a purely defensive play. I think most organizations are overdue to proactively seek ways to use their ECRM Program and Cybersecurity Strategy to not only manage risks or "manage the downside" but also identify ways to use their ECRM Program and Cybersecurity Strategy to identify and exploit opportunities or "manage the upside" and create competitive advantage.

This book provides an overview of why a robust ECRM Program and Cybersecurity Strategy is a strategic imperative for your organization and how executives and board members should think more positively about ECRM and cybersecurity and, finally, outlines how to develop your ECRM Program and Cybersecurity Strategy, including a discussion of the contents of documentation that will help establish, implement, and mature your program and meet increasingly more stringent requirements legislators, regulators, and the courts are setting.

My goal is that C-suite executives, board members, and their Chief Information Security Officers (CISOs) use this book to bridge communication gaps and meet at the intersection of where boards focus:

talent management, strategy, and risk management. As an existential risk to most organizations, they need to manage these risks and leverage their programs' strengths to create value and drive business growth.

For ECRM to be effective, the entire organization must be engaged in the program. Although this book is written primarily for C-suite executives, board members, and CISOs, I am confident that the information I present will also be helpful to other leaders, managers, and professionals in all functional areas in all organizations in all industries.

Bob decided to write this book to help facilitate the role of Chief Information Security Officers (CISOs) to better integrate into their businesses and interact with C-suite executives and board members. As happened when Chief Information Officers (CIOs) began to "earn a seat at the table" decades ago, there is a significant communication gap between this newly discovered role, the C-suite, and the board. Bob's goal is to make CISOs and their boards successful in better understanding one another and better managing cyber risks and cyber opportunities. The aim of this book is to help close the communication gap by linking CISOs with the three main topics that boards deal with: talent management, strategy, and risk management.

—Bob Chaput, Founder and Executive Chairman, Clearwater