Managing Risk and Information Security

Protect to Enable

Second Edition

Malcolm W. Harkins

Apress open

Managing Risk and Information Security: Protect to Enable

Malcolm W. Harkins
Folsom, California, USA

ISBN-13 (pbk): 978-1-4842-1456-5 ISBN-13 (electronic): 978-1-4842-1455-8
DOI 10.1007/978-1-4842-1455-8

Library of Congress Control Number: 2016949414

Cover image designed by Freepik.

Managing Director: Welmoed Spahr
Lead Editor: Robert Hutchinson
Development Editor: James Markham
Editorial Board: Steve Anglin, Pramila Balen, Aaron Black, Louise Corrigan, Jonathan Gennick, Robert Hutchinson, Celestin Suresh John, Nikhil Karkal, James Markham, Susan McDermott, Matthew Moodie, Natalie Pao, Gwenan Spearing
Coordinating Editor: Melissa Maldonado
Copy Editor: Mary Behr
Compositor: SPi Global
Indexer: SPi Global
Artist: SPi Global

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.springer.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 rights@apress.com, or visit www.apress.com.

Apress and friends of ED books 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 Special Bulk Sales–eBook Licensing web page at www.apress.com/bulk-sales.

Any source code or other supplementary materials referenced by the author in this text is available to readers at www.apress.com. For detailed information about how to locate your book's source code, go to www.apress.com/source-code/.

Printed on acid-free paper

About ApressOpen

What Is ApressOpen?

- ApressOpen is an open access book program that publishes high-quality technical and business information.
- ApressOpen eBooks are available for global, free, noncommercial use.
- ApressOpen eBooks are available in PDF, ePub, and Mobi formats.
- The user friendly ApressOpen free eBook license is presented on the copyright page of this book.

This book is dedicated to my family.

Contents at a Glance

Contents

Foreword

Security and first-person shooter video games have one obvious thing in common: if you're not continuously moving, you're dead. In this second edition of *Managing Risk and Information Security*, Malcolm Harkins helps us move our thinking into areas of risk that have become more prominent over the last several years.

Because there is so much new content in this edition, I will focus on a topic that has risen to greater prominence since the first edition: people are the perimeter. When we reflect on what has changed in recent years, with an eye to the vulnerabilities that result in real-world compromises, a pattern emerges: virtually all the major breaches that we have seen involve manipulation of people. When nearly everyone has heard of phishing, we have to ask ourselves: why is it still such an effective tool?

The obvious theory is that we haven't managed people risk as well as we should. Perhaps we have been standing still and need to learn how to dodge and experiment with the way we drive better people-security outcomes. Unfortunately, the path is not 100% clear. Unlike technology, the field of influencing human behavior in security is remarkably complicated and supported by limited research.

Malcolm provides us with a great foundation and framework to build our "security engagement" functions. I like to use the word "engagement" because it speaks to how the security organization relates to the workforce in a manner that isn't simply bounded by the more traditional term "training and awareness." Engagement encompasses anything that shifts the desired behavior outcome in the direction we want it to go. I have seen remarkable shifts in measured behavior from the use of non-traditional tools such as security gamification and simulation.

The way Malcolm differentiates between "compliance" and "commitment" is key. *Managing Risk and Information Security* is an ever-evolving classic in the field of security management.

—Patrick Heim
Head of Trust & Security, Dropbox

Praise for the second edition of Managing Risk and Information Security

We assign Malcolm's book to our Carnegie Mellon CISO-Executive Program students on their first day of class. It is relevant, pragmatic, and solution oriented. Our adversaries are changing their practices and so must we. Malcolm's book is a terrific tool for the modern-day info sec leader who wants to shift from security as a restriction to security as a business enabler.

—Andy Wasser
Associate Dean, CMU Heinz College

Malcolm is a top-notch executive, security leader, and innovator, with a keen ability to convey thought-provoking and valuable insights. His latest effort demonstrates remarkable foresight into the skills necessary to excel as a security leader today and tomorrow.

—Clayton J. Pummill
Executive Director, Security Advisor Alliance

I could go on and on about what I liked specifically—there was much, including the discussion about governance models and social responsibility—but here is the net: this is the first time I've seen someone be able to speak to security specifics while also raising the conversation to a much higher level. It begins to take on an Alvin Toffler feel from his astounding book, The Third Wave. *Malcolm's thoughts are philosophically sweeping while at the same time imminently practical.*

—Todd Ruback, Esq., CIPP-US/E, CIPT
Chief Privacy & Security Officer & V.P. Legal Affairs, Ghostery

Malcolm Harkins is a foremost expert at managing risk and information security. In this latest book, he further expands his Protect to Enable philosophy and does so in a way that offers practical and actionable initiatives that any risk manager or CISO can implement to protect their enterprise while enabling business growth. A must-read for CISOs and their teams!

—Tim Rahschulte, Ph.D.
Chief Learning Officer & Content Officer, Evanta

Malcolm Harkins is a visionary thought leader on cyber security and risk management. Managing Risk and Information Security *is a must read. Malcolm helps readers immediately take the information and apply it to their own organizations. You will find that this book cuts through the fog and provides a clear picture of where and what to focus on to effectively manage cyber business risk.*

—Phil Ferraro
Global CISO and Cyber Security Consultant

The CISO is more than just a technology expert; she must be savvy about leadership, influence, and change across complex organizations; someone who sees her mission not to just drive implementation of a large system, but to foster sustainable culture change at every level. As an organizational psychologist, I recognize Harkins' keen eye for group dynamics and leadership tactics that enable CISOs to enhance enterprise security. He puts his finger on the habits, assumptions, and decision processes typical of many employees and teams, as they unknowingly increase security risk, and for that alone this book is a gem. It should be required reading for aspiring CISOs and for anyone who has a role in the recruitment and hiring of CISOs.

—Marc Sokol, PhD
Executive Editor, People + Strategy

Malcolm Harkins' take on information security and risk is a refreshing change from the increasingly frequent alarm bells raised in the press with regard to the "brave new world" where technology is presented as an ever-escalating conflict between our seemingly insatiable appetite for connectivity, cool applications, and customized information, on the one hand, and a desire to control who has our information and how they may use it, on the other. Harkins instead offers a cool, clear-eyed perspective where managing information and risk are placed in a wider context. His prescriptions and frameworks are recipes for well-managed organizations in the broadest sense. They allow us to embrace our new-found

technological abilities without fear because we have defined their purpose capaciously enough to be a positive good, to be of service to all a company's stakeholders. That is, once we set a truly human course, technology serves rather than threatens us. Organization purpose, when defined in this way, is an expression of our values and is empowered by that fuel. Harkins' book is a practical as well as purposeful guide to a values-driven implementation of information technology.

—Mary C. Gentile, PhD
Author of *Giving Voice To Values: How To Speak Your Mind When You Know What's Right* (Yale University Press)

In today's rapidly evolving security landscape, security professionals are navigating a complex set of dynamics across the enterprise. In Managing Risk and Information Security, *Malcolm Harkins draws on his rich security experience to present a connected view of where companies should be focused. He puts forth a valuable perspective, as organizations around the world look to create a necessary balance of protection and innovation, which ultimately enables business success.*

—Bret Arsenault
Corporate Vice President and CISO, Microsoft Corporation

Malcolm generously shares through personal experiences and story telling the formula for a successful 21st century CISO. It is one part multi-disciplinary leader and one part trusted advisor to the business, combined with behavioral models required for balanced risk decision making. A must-read for all new CISOs. Malcolm lives his beliefs.

—Nasrin Rezai
GE Corporate Security & Compliance Officer

In the second edition of his book, Malcolm seamlessly articulates the future horizon of cyber security and the critical role that the CISO and security professionals will need to fulfill in order to defend both the company and consumers they serve. The guidance he provides into the skills, leadership, and approach required for successfully navigating the emerging challenges of securing a digital economy is invaluable. Regardless of your current role, this is a must-read for everyone who has accepted this great responsibility and privilege.

—Steven Young
CISO, Kellogg Company

While other security officers are looking to the traditional or the latest "cool" product, Harkins goes against the tide and asks the questions that need addressing. His forward-thinking mindset and Protect to Enable approach inspire others to innovate and go beyond the mainstream. If you cannot bring Harkins to your company for mentoring, this book will at least spark thought and will change how your engineers view security within the business.

—Charles Lebo
Vice President and CISO, Kindred Healthcare

Malcolm's vast experience makes him one of the most credible security leaders on the international stage and serves as the perfect platform for this book. Rational, compelling, and authoritative writing is far too rare in the world of risk and information security, but Malcolm completely nails it in Managing Risk and Information Security *with invaluable advice and recommendations for anyone planning a future in the security world. His extensive experience in business before becoming a CISO is one of the missing ingredients in many security executives' professional toolbox, which is which is why this is such an important book. Make sure to keep a highlighter and notepad handy because there are a lot of nuggets in here you'll want to remember on your journey to becoming a better security professional.*

—Mark Weatherford
Chief Cybersecurity Strategist at vArmour and
former Deputy Under Secretary for Cybersecurity
at the US Department of Homeland Security

I've had the privilege of working with many talented CISOs over the years and Malcolm is one of the best. His logical, methodical approach to solving the most complex cybersecurity problems is reflected in his lucid style. An enlightened approach to understanding risk that unites all stakeholders and a systemic intelligence-based approach to security infrastructure are the only ways to reduce the threat to manageable levels. This is our best path forward if we are ever to realize the vast potential of the innovative digital world we are creating. In Managing Risk and Information Security, *Malcolm shines a light on that path in a comprehensive yet very readable way.*

—Art Coviello
Former CEO and Executive Chairman, RSA

About the Author

Malcolm Harkins is the Chief Security and Trust Officer (CSTO) at Cylance Inc. In this role, he reports to the CEO and is responsible for enabling business growth through trusted infrastructure, systems, and business processes. He has direct organizational responsibility for information technology, information risk, and security, as well as security and privacy policy. Malcolm is also responsible for peer outreach activities to drive improvement across the world in the understanding of cyber risks and best practices to manage and mitigate those risks.

Previously, Malcolm was Vice President and Chief Security and Privacy Officer (CSPO) at Intel Corporation. In that role, Malcolm was responsible for managing the risk, controls, privacy, security, and other related compliance activities for all of Intel's information assets, products, and services.

Before becoming Intel's first CSPO, he was the Chief Information Security Officer (CISO) reporting into the Chief Information Officer. Malcolm also held roles in finance, procurement, and various business operations. He has managed IT benchmarking and Sarbanes-Oxley–compliance initiatives. Harkins acted as the profit and loss manager for the Flash Product Group at Intel; was the general manager of Enterprise Capabilities, responsible for the delivery and support of Intel's Finance and HR systems; and worked in an Intel business venture focusing on e-commerce hosting.

Malcolm previously taught at the CIO Institute at the UCLA Anderson School of Management and was an adjunct faculty member at Susquehanna University in 2009. In 2010, he received the RSA Conference Excellence in the Field of Security Practices Award. He was recognized by Computerworld as one of the Premier 100 Information Technology Leaders for 2012. $(ISC)^2$ recognized Malcolm in 2012 with the Information Security Leadership Award. In September 2013, Malcolm was recognized as one of the Top 10 Breakaway Leaders at the Global CISO Executive Summit. In November 2015, he received the Security Advisor Alliance Excellence in Innovation Award. He is a Fellow with the Institute for Critical Infrastructure Technology, a non-partisan think-tank that provides cybersecurity briefings and expert testimony to the U.S. Congress and federal agencies. Malcolm is a sought-after speaker for industry events. He has authored many white

papers and in December 2012 published his first book, *Managing Risk and Information Security*. He also was a contributing author to *Introduction to IT Privacy*, published in 2014 by the International Association of Privacy Professionals.

Malcolm received his bachelor's degree in economics from the University of California at Irvine and an MBA in finance and accounting from the University of California at Davis.

Acknowledgments

I received valuable feedback from many readers of the first edition of this book. That feedback helped me to expand the book with additional insights, clarifications, and updated examples. It also encouraged me to add two more chapters to the second edition: one on corporate social responsibility, and the other on performance coaching.

Special thanks to Mike Faden: without his help this book would not have happened.

As I noted in the first edition, many people during my journey at Intel helped me learn and grow. A number of them published material that is still referenced in this second edition.

Other experts who have helped me come from a variety of different peer groups. They include members of the Bay Area CSO Council, the Executive Security Action Forum, the members and staff of CEB and its Information Risk Leadership Council, participants in the Evanta CISO Executive Summits and the CISO coalition, as well as the Security Advisor Alliance.

Finally, I wish to thank Stuart McClure for giving me the opportunity to join Cylance.

Preface

If you don't believe in the messenger, you won't believe the message.
You can't believe in the messenger if you don't know what the messenger believes.
You can't be the messenger until you're clear about what you believe.

—James Kouzes and Barry Posner,
in *The Leadership Challenge*

A great deal has transpired since the first edition of this book was published in January 2013, both in the world of information risk and in my personal life and career. To briefly cover the latter, in January 2013, I was named Intel's Chief Security and Privacy Officer. My broad role was one of the first of its kind in corporate America: I was charged with managing and mitigating risk for Intel's products and services worldwide, in addition to Intel's internal IT environment. In June 2015, I left Intel to become CISO at Cylance Inc., and in May 2016, I was named Cylance's Chief Security and Trust Officer.

These career changes occurred during an extraordinary period of escalating information risk, as evidenced by an almost continuous stream of major hacks and breaches, and a corresponding rise in society's awareness of risk. Some key examples:

- May 2013: Edward Snowden flies to Hong Kong after leaving his job at an NSA facility in Hawaii. The following month, he reveals thousands of classified NSA documents. The disclosures, including previously unknown government surveillance programs, continue to cause worldwide repercussions today.
- December 2013: The blog Krebs On Security reports a massive data breach at Target. The company confirms the breach the next day. Within months, Target's CIO and CEO both resign amid the fallout.
- May 2014: A U.S. grand jury indicts five Chinese military officers on charges of hacking American companies and stealing trade secrets.
- November 2014: Employees at Sony Pictures arrive at work to discover their network has been hacked. Attackers steal and then erase data on thousands of systems, forcing studio employees to revert to using fax machines and pen and paper. The attackers then dump huge batches of confidential business and personal information online.

- March 2015: Google's Project Zero hacking team demonstrates the ability to exploit a fundamental flaw in DDR3 SDRAM to perform privilege escalation attacks on systems containing the chips. Some mitigation approaches are available, other than replacing the DDR3 memory in millions of systems worldwide.
- June 2015: The US Office of Personnel Management announces a data breach targeting the personal data of up to 4 million people. The attack, which includes security clearance-related information, is one of the largest-ever breaches of government data. By July, the estimated number of stolen records increases to 21.5 million.
- February 2016: The Hollywood Presbyterian Medical Center in Los Angeles says it has paid a bitcoin ransom to attackers who held its systems hostage, encrypting data and blocking access by hospital staff. Some believe the healthcare industry is the next major target for cyber criminals.

Given this escalating cycle of risk, and the potential catastrophic societal implications of today's attacks, we must all be ready to be held accountable. This may require a large mental shift for those used to simply assigning responsibility and blame for a breach to the people who traditionally perform post-attack cleanup: corporate IT departments, internal information security teams, and investigations and computer forensics groups. Everyone, from corporate executives to security practitioners, shares responsibility for security and privacy. We must all step back and contemplate our own personal responsibilities, not only to the organizations we work for and the customers we serve, but also to society as a whole.

The challenge we sometimes face is how to characterize that responsibility. Is our responsibility to limit liability for our organizations? Or is it a duty of care to the people whose information we store? What values are we using when we make decisions about cyber risk, and what bias do those values create in our decisions? Are we forward-looking enough, or will the decisions we make to fix our problems today create other problems in the future? As Benjamin Franklin once said, "All human situations have their inconveniences. We feel those of the present but neither see nor feel those of the future; and hence we often make troublesome changes without amendment, and frequently for the worse."

As security and privacy professionals, a key part of our role is to ensure the right dialogue and debate occurs. We need to ask "high-contrast" questions that sharply define the implications of the choices our organizations make. We need to make sure that the opportunities are as clearly defined as the obligations to mitigate risk, so that our organizations make the right decisions. And we need to take equal responsibility for the outcomes of those choices, as opposed to abdicating that responsibility solely to the business. Once the choice is made, we must transition out of the debate about what is right and focus on taking the right actions—on making tomorrow better than today.

We can think of this as doing what's right. We can think of it as protecting our customers and partners and keeping our markets healthy for everyone. No matter what motivates us, thoughtfully building systems to support a culture of genuine responsibility for privacy and security is not only good corporate responsibility; it is also good for

business. For computing to continue to improve the world we live in rather than endanger it, it needs to be trustworthy. And for that trust to be deliverable, we need to ensure the data we enter into our computers is both secure and private. As an organization, we demonstrate and build trust through our approach to solving these cyber-risk challenges.

In the preface of the first edition, I said "*Managing Risk and Information Security* is a journey, but there is no finish line. Our approach to managing information risk must continue to evolve as rapidly as the pace of business and technology change. My hope is that people will read this book and begin their own journey."

I still firmly believe what I said then. But I also believe that, as General George Marshall once said, "The only way human beings can win a war is to prevent it." We are at war against adversaries who wish to harm the users of technology. But there is also a battle among those responsible for protecting security and privacy. On one side are organizations that would like to continue on the current path because they profit from the insecurity of computing, or that approach the duty of care with a bias towards limiting liability rather than protecting their customers. On the other side are those who believe that our role is to generate trust. We do that by protecting to enable people and businesses. It's a hard road; I know, because I experience it every day. But we shouldn't back away from something just because it is hard. We need to plant our feet and stand firm. The only question is where we plant our feet.