Managing Risk and Information Security

Protect to Enable

Malcolm Harkins

Apress open

Managing Risk and Information Security: Protect to Enable

Malcolm Harkins

ISBN-13 (pbk): 978-1-4302-5113-2

ISBN-13 (electronic): 978-1-4302-5114-9

President and Publisher: Paul Manning
Lead Editors: Jeffrey Pepper (Apress); Stuart Douglas (Intel)
Coordinating Editor: Jill Balzano
Cover Designer: Anna Ishchenko

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.

For information on translations, please e-mail rights@apress.com, or visit www.apress.com.

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.

Foreword

Newly promoted CISOs rapidly realize that the scope of the position they have taken on is often beyond what they have been prepared for. The nature of securing an enterprise is daunting and overwhelming. There are no simple checklists or roadmaps for success. Many of the technical security skills a CISO has acquired during the early portion of his or her career may provide a "sixth sense" or intuition, but technical expertise alone does not prepare the CISO for the business and leadership challenges required for success.

The Dunning-Kruger effect "is a cognitive bias in which unskilled individuals suffer from illusory superiority, mistakenly rating their ability much higher than average" (Wikipedia). Successful CISOs generally realize and admit to themselves how much they don't know. In my career, I have met many senior security professionals and have noticed a common set of traits among those who are successful.

They generally exhibit a strong sense of curiosity, the ability to be self-aware, the ability to "think evil" (like the adversary), and have strong communication and critical thinking skills. They are open to new ideas, they invite debate, and they are adaptive in their thinking and positions when new information is presented. They develop leadership skills and build structures that enable balance. They also recognize talent and surround themselves with teams of capable security technologists who are the true experts. Excellent security leaders have learned that risk is not black-and-white and that balance needs to be applied. They are empathic and likeable. My friend Malcolm meets all these criteria.

In ***Managing Risk and Information Security: Protect to Enable***, he distills the hard-acquired knowledge he has learned through his career as a business and security leader into a concise framework that enables CISOs to cut through the chaos of securing the enterprise. Absorb the lessons in this book and enrich them by continuing to experiment and innovate. Threats, organizational dynamics, and technology are constantly evolving and we as security professionals must apply the lessons outlined here and continuously adapt ourselves to the challenge.

—Patrick Heim
Chief Trust Officer
Salesforce.com, Inc.

Contents at a Glance

Contents

About the Author

Malcolm Harkins is vice president of the Information Technology Group, Chief Information Security Officer (CISO) and general manager of Information Risk and Security. The group is responsible for managing the risk, controls, privacy, security, and other related compliance activities for all of Intel's information assets.

Before becoming Intel's first CISO, Harkins held roles in Finance, Procurement, and Operations. He has managed IT benchmarking efforts and Sarbanes-Oxley systems compliance efforts. Before moving into IT, Harkins acted as the profit-and-loss manager for the Flash Product Group at Intel; he was the general manager of Enterprise Capabilities, responsible for the delivery and support of Intel's Finance and HR systems; and he worked in an Intel business venture focusing on e-commerce hosting.

Harkins previously taught at the CIO Institute at the UCLA Anderson School of Business and he was an adjunct faculty member at Susquehanna University in 2009. In 2010, he received the award for excellence in the field of security at the RSA Conference. He was recognized by *Computerworld* magazine as one of the top 100 Information Technology Leaders for 2012. In addition, (ISC)2 recognized Malcolm in 2012 with the Information Security Leadership Award.

Harkins 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.

Preface

Many organizations failed to survive the information technology revolution. Many more will not survive the current wave of technology-driven innovation—and the threats and vulnerabilities that come with it.

To thrive in complex, highly-connected global markets, organizations need bold business strategies that use technology to achieve competitive advantage. The enterprise information risk and security team can either hinder these strategies or help drive them. Effectively managing information risk and security, without hindering the organization's ability to move quickly, will be key to business survival. That is why, three years ago, I changed the mission of Intel's information risk and security team to "*Protect to Enable*." It is also why I am writing this book.

In January of 2002 I was hired to run a program called Security and Business Continuity. This program was created after the events of 9/11 and the Code Red/Nimda viruses during the summer of 2001. It was primarily focused on the availability risk concerns at that time. I had no technical security background but had been with Intel close to 10 years in a variety of business-related positions that were mostly in finance. It became apparent to me in those first few months as I was learning that the world was going to start dramatically changing and a "perfect storm" of risk was beginning to brew. The following picture is what I put together to explain that to my manager, Intel's CIO, and anyone who would listen to me.

In February of 2004, I left this program since we were mostly done with the effort to deal with the availability risks. I left to run our system's Sarbanes-Oxley compliance efforts. My finance background, the variety of business roles I had previously held, and my time being around IT for so many years as well as the effort I had led in 2002 and 2003 made it a natural fit. But I had something else haunting me, which was this picture. I wasn't haunted by the fear of the risks that could occur, but rather it fueled my sense of curiosity and triggered in me a passion to figure out how to navigate this storm of risk. So in 2005, once our initial SOX compliance efforts were complete, I went back to information security but with a drive and desire to try to link all the main elements of information risk, security, control, and compliance activities together to deal with this spiral of risk. So for the past 7 years, this has been my quest. In this book, I will cover many things I have learned in the 11 years that I have been managing various aspects of information risk and security, at Intel. I will share ways to think about risk, ways to look at governance. I will explore internal and external partnerships for information sharing and collaboration that can make a difference. I will share the examples of things we have done within Intel and things we are looking to do to better manage our risks and enable our IT users. Finally, I will look to the future as well as share my perspectives on the skills required for the 21st-century CISO.

Managing Risk and Information Security: Protect to Enable 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.

Acknowledgments

This book is dedicated to my family: my father, John; my mother, Mary; my children Colin, Evan, and Erin; and the woman who completes me—my wife, Kim.

In developing this book, I received help from many people within Intel Corporation and throughout the industry.

Special thanks to Mike Faden—our discussions, and his questions seeking clarity from me, brought this book to life. Thanks also to Ilene Aginsky, who encouraged me to start the book, and to Elaine Rainbolt, who has provided considerable help along the way.

I also wish to thank all those in Intel's information risk and security team. Without their skills and passion, I would not have learned so much during the past 11 years. It is because of them that I have been able to execute my role and write this book. Many individuals contributed time, energy, and expertise—either to me, helping me grow my knowledge over the years; directly to the book; or to the creation of other documents that I used as source materials. The following deserve special thanks: Brian Willis, Kim Owen, Steve Mancini, Dennis Morgan, Jerzy Rub, Esteban Gutierrez, Rob Evered, Matt Rosenquist, Tim Casey, Toby Kohlenberg, Jeff Boerio, Alan Ross, Tarun Viswanathan, Matt White, Michael Sparks, Eran Birk, Bill Cahill, Stacy Purcell, Tim Verrall, Todd Butler, Stuart Tyler, Amir Itzhaki, Carol Kasten, Perry Olson, Mary Rossell, Marie Steinmetz, Fawn Taylor, Grant Babb, Eamonn Sheeran, and Dave Munsey.

Other experts who have helped me to learn and grow include the members of the Bay Area CSO Council and Executive Security Action Forum, the members and staff of the Information Risk Executive Council, and participants in the Evanta CISO Executive Summits. In particular, I'd like to acknowledge peers who act as trusted sounding boards for ideas, for me and for others in the industry: Patrick Heim, Dave Cullinane, Justin Somani, Gary Terrell, Larry Brock, Mark Weatherford, Brett Whalin, Joshua Davis, Dennis Brixius, Preston Wood, Anne Kuhns, Roland Cloutier, and John Stewart.

Finally, I wish to thank Intel's past CIOs who challenged and inspired me, and took risks by placing me in roles I wasn't ready for: Carlene Ellis, Louis Burns, Doug Busch, John Johnson, and Diane Bryant.