CHRIS MOSCHOVITIS

CYBERSECURITY PROGRAM DEVELOPMENT FOR BUSINESS

THE ESSENTIAL PLANNING GUIDE

WILEY

CYBERSECURITY PROGRAM DEVELOPMENT FOR BUSINESS

CYBERSECURITY PROGRAM DEVELOPMENT FOR BUSINESS

THE ESSENTIAL PLANNING GUIDE

Chris Moschovitis

WILEY

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

Library of Congress Cataloging-in-Publication Data is Available:

ISBN 9781119429517 (Hardcover)
ISBN 9781119430056 (ePDF)
ISBN 9781119430001 (ePub)

Cover Design: Wiley
Cover Image: © phive2015/iStockphoto

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

CONTENTS

FOREWORD

If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained, you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.

— Sun Tzu, *The Art of War*

Who better to write a foreword for a cybersecurity book than a hacker? An "infamous hacktivist," as John Leyden called me five years back. After all, I'm the kind of person who, with help from this book, you will be prepared to defend yourself against!

I started out as a kid in the ghetto where I went into gang life and drug dealing. At some point I asked myself, "Do I follow in my father's footsteps, or do I find my own path in life?" I realized that living the fast life and being in the streets was only going to keep me there.

I wanted more.

I discovered the Internet at age 12. We're talking about a time when Google wasn't what it is today, and finding information online entailed going to forums, searching bulletin board system (BBS) archives, and relying on the likes of CompuServ, America Online (AOL), and Internet Relay Chat (IRC).

As I explored this world, I began to hear about certain mysterious figures who, like ancient sages, had a wealth of knowledge and experience that many Internet users lacked, but respected. I became attracted to the hacker ethic and lifestyle. Reading "The Hackers' Manifesto" cemented exactly what it was about being a hacker that I liked: that hacking was my decision, my choice, and no one could say otherwise.

I tried to reach out to hackers and join them. I was disappointed to learn these hackers belonged to invitation-only and private communities. It was impossible to speak to them. So, I made my own way. I chose a nom de guerre, "Sabu." As soon as I adopted this persona, I began to think differently, without boundaries.

To fully make the transition from Hector to Sabu required a lot of knowledge I didn't have. In short, I needed education. To compromise a server, I had to understand and be able to communicate with the underlying system, so I became a systems administrator of various UNIXes and POSIX systems. To write a proof-of-concept exploit for a vulnerability, I had to learn several programming languages, and so on.

As I slowly grew out of my awkward teenage years, I became more interested in the world from a geopolitical perspective, which attracted me to "hacktivism," where you combine hacker skills with activist causes. In the year 2000, I began hacktivist operations against governments around the world. I went from a curious hacker to a persistent threat to governments I did not agree with. That decision ultimately led to my downfall as a hacker and a hacktivist.

Just before my arrest, I had decided to leave the hacking world. All my experience as a hacker, security researcher, and systems administrator provided me a wealth of experience that I could now apply to any business—and I did. I became senior systems administrator for one of the biggest nonprofit technology-oriented organizations in New York City. Life was good, and every decision I made, including becoming a foster parent, was positive.

That's when I made my mistake and got back in the game. I unretired Sabu and reconnected with the hacktivist scene. It was 2010, the height of Anonymous and online hacktivism. I involved myself in the Arab Spring, shutting down government communications at the apex of the Tunisian revolution, as well as targeting federal contractors and media platforms. This was a time when cybersecurity was forever changed—from the tools and the scope of attacks to how hackers were organized, were funded, and acted. I knew our world would not be the same again.

I am not proud of that time. But when I realized how far I'd overstepped the line, it was too late.

I was arrested, and "Sabu" became infamous.

I had to accept the consequences of my actions and change my life for good. This meant leaving behind most of my friends, expanding my perspective, and realizing what really meant the most to me in life: my family.

My life offers you a glimpse into the hacker world. It's important for you to understand that we come from all walks of life, from privileged suburbs to the ghetto. We may be working in so-called legitimate jobs one day and hacking the next. Some do it for the thrill, whereas others still do it to support their causes—as in my case.

But hackers also hack for revenge and out of greed. The varied nature of hacker threats and motives means that cybersecurity is not easy. It requires dedication to preparedness, education, and constant vigilance.

Those three things, preparedness, education, and vigilance, are what Chris Moschovitis's book is all about. I first met Chris at ISACA CSX, and we quickly discovered that our thinking on cyberthreats and possible solutions was in alignment. Most important, I share with him the critical importance of being prepared, staying informed, thinking ahead, and remaining vigilant. Chris and I agree: This is the only path to cyber-resilience.

Like the choices I made in my life, the choices you make in your organization have the potential to change its path. The things you will learn in these pages will help you get ahead of the curve, become cyber-resilient, and be prepared for the next time you "meet" a hacker, who, unlike me, is not in retirement.

Hector "Sabu" Monsegur
Director of Assessment Services
Rhino Security Labs

PREFACE

"Enough already!"

This was the (only *half*-joking) reaction of a well-respected editor of a major publishing house when I suggested he produce yet another cybersecurity book. "Enough! You cybersecurity people have demoralized everyone so much that no one wants to hear, read, or talk about this any more. We're not publishing any more cybersecurity books! Done! Finished!"

I couldn't argue with him. He's right. Cybersecurity experts have done a wonderful job of terrorizing everyone about the threats while doing nothing by way of offering some hope, some light at the end of the tunnel. Every security discussion seems to boil down to the same, dire predictions of cyber-doom:

"It's not if, it's when!"
"There are only two kinds of companies:
Those that have been hacked and those that don't know it!"

Got it! We're all done for, thank you very much. Now what?

Something Completely Different

What if there was a book that put the whole cybersecurity thing into perspective, using simple, direct language? What if there were sections and chapters explaining what is going on, what the risks are, and what all the technobabble really means? And what if the book had a step-by-step, actionable approach on what you can do about all this? A book that aggregated the current best practices, put them in perspective, injected my experience and my own point of view, and how I applied all this across all our clients? All the while poking a little fun at ourselves, too?

I thought that this would be a great idea! And since I couldn't find any, I decided to write one.

Throughout my career, I've felt an attraction to science, technology, management, and governance, as well as a deep empathy for my clients' businesses. No matter what their industry, I understood their struggles, their anxieties, and what it means to make payroll no matter if it is for 10 employees or 5,000. I understood that I was their Rosetta stone—someone who could translate tech-speak to business-speak—and I felt the weight of that responsibility. My clients count on me and my recommendations. They are placing their trust

and their businesses in my hands. My recommendations and my opinions matter in ways far more impactful than just tech. They affect people, their jobs, and their privacy.

This is exactly why I wrote this book.

This book is for them and for you: a businessperson, either running your own business or responsible enough to need to know how to protect the one you're employed at—no matter the size. You don't want to be at the mercy of experts talking above your head and around you. You want to participate in the conversation; you want to know what you're getting into. You are also an individual concerned about your privacy. You are alarmed about all the stuff about cyberattacks, hackers, and the like bombarding you in the news, and you want to stop feeling helpless about it. You are also a pragmatist who knows you can't spend your day being terrorized into hiding, paralyzed with inaction, or crippled by the costs of compliance and cyber-protection.

This book will prepare you for all this, step by step. We'll develop your cybersecurity program together, using the information presented here as well as by reviewing case studies from different industries and businesses.

Speaking of case studies, we need a case study disclaimer. The case studies presented throughout this book are aggregated from our work and from the work of colleagues who were gracious enough to share their experiences, some as named contributors. As you would expect, all names, industries, and geographies have been changed to protect the anonymity of the clients. The goal has been to distill the essential lesson from each case while protecting the identity and respecting the privacy and confidentiality of every client. You will find these case studies sprinkled throughout the book, especially as we dive into the specifics of cybersecurity program development.

My original title for the book paraphrased the great Stanley Kubrick and his film, *Dr. Strangelove*. I was going to call it *How to Stop Worrying about Cybersecurity and Learn to Love the Hackers!* The wise people at Wiley talked some sense into me and changed it for the better, but my goal remains the same.

It is my hope that when you're done, you will stop worrying about cybersecurity and will have learned to love the hackers!

ABOUT THE AUTHOR

I was born in Athens, Greece. After high school I chose to come to the United States to study physics and computer science. I did that at The College at Brockport, in upstate New York. My years at Brockport were formative to me as a person, a scientist, and as a professional. Words for the gratitude and respect I have for the dedicated faculty that shaped my life can easily fill a couple of books, but that is for another time.

After graduating with my bachelor's degree in science, I became an instructor of computer science and a computer systems manager at the Stratford School in Rochester, New York. Following brief graduate work stints at the Rochester Institute of Technology and the University of Rochester, I moved to New York City to serve as the director of academic computing at the Pratt Institute. There, under the direction of the vice president of information technology (there were no "chief information officers" back then), I was responsible for the building and management of four computing centers of excellence, each focusing on a specific discipline (art, architecture, engineering, and information science). From there, I was recruited to be the vice president of information technology at the O'Connor Group, a real estate manager and developer in New York City. Then, in the middle of the Reagan Recession, I decided that there was no better time than the present to start my own company, which I did in 1989.

I have been running my own firm ever since, surrounded by partners and colleagues who teach me more and more every single day, and together we deliver a broad spectrum of IT consulting services. I have been privileged to partner with great clients, to engage in fantastic projects of business and technology transformation, and to collaborate with teams that push boundaries and develop incredible business solutions. I lived through the amazing advances in computer science that are now the stuff of lore: I was there during BitNet, sending email messages and watching the message hop from node to node. I was amazed at formatting the first 10MB hard disks of IBM's new personal computer. I've fed endless floppies in and out of the first Macs. I've built muscles carrying the Compaq "Portable," which was nicknamed "luggable" for good reason. I've carried pagers and cellphones the size of suitcases. I subscribed to CompuServe and AOL, and still have a working Hayes 14.4 modem.

Throughout it all, I have always been fascinated by security, privacy, and the protection of data. Even before "cybersecurity" was a word, I insisted that the sites we designed and managed implemented business-appropriate

computer security and disaster recovery. Maybe it was because George, a partner of mine at the time, was a computer virus collector (he still has them). Maybe, because I remain culturally Greek, naturally cautious and private. Whatever the reason, I always asked, "What happens if 'this' gets out?" or "How fast can we be back up and running?" Any of my consultants will tell you that even now, the first thing they are taught when they start working for me is that "not checking the backup is a career-ending mistake."

Following decades as a practitioner of both IT governance and cybersecurity management, I decided to make it official and joined Information Systems Audit and Control Association (ISACA), an independent, nonprofit, global association that was founded in 1969, engaging in "The development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems." Joining ISACA was one of the smartest things I ever did. Through ISACA, I got certified in two areas: one in IT governance, becoming Certified in Governance of Enterprise IT (CGEIT), and another in cybersecurity, becoming a Certified Information Security Manager (CISM). As of this writing, I am proud to have the highest scores in the New York chapter in both, as well as membership in the top 5 percent of those tested worldwide for CISM, and the top 10 percent for CGEIT.

ACKNOWLEDGMENTS

This book reflects a long, personal, and professional journey. Over the course of some 30 years in the industry, I have had the privilege to meet hundreds of professionals, experts, partners, clients, and vendors who have shaped my thinking, formed my experiences, and honed my expertise. From my original partner in the business, George Whelan, who religiously collected and kept live computer viruses on floppy disks, to instructors like Jay Ranade, who has forgotten more than I'll ever know, to clients who partnered with me, and staff who tirelessly worked to solve problems, I owe each one a debt of gratitude that no acknowledgment can do justice. I start, therefore, with an apology for my omissions. They are entirely my own.

First and foremost, I want to thank our clients, our true partners to success. Every day, we are honored and privileged to be your allies and to contribute to your success. We are humbled by all the things that you teach us every day. I would be remiss if I didn't single out the Hoffman family, Andrew, Mark, and Steve, who have been loyal supporters and mentors since I started the firm; the executive leadership at the 4As for defining and living into a true partnership of success; the founding partners at Allegaert Berger and Vogel, Chris, David, and Michael, for their trust in us, loyalty, and wise counsel through thick and thin; the president of the LaSalle Academy, Dr. Cathy Guerriero, and her team, for infusing us with creativity and vigor, and for taking the time to listen even when they are running at 1,000 mph; and finally, the leadership team at the Packer Collegiate Institute, Bruce Dennis, Elizabeth Winter, and Jim Anderson, for their trust, engagement, and reminding us how to be brave in the face of change.

In the same breath, I want to thank my own partners and associates, whose incredible expertise, loyalty, dedication, skills, empathy, and personal engagement make our clients' success possible. They are, alphabetically: Anna Murray, Atsushi Tatsuoka, Frank Murray, Greg Andrews, Haleigh Westwood, Jonathan Ongvano, Justin Schroeder, Leon Tchekmedyian, Pedro Garrett, Protus Miyogo, Sotos Antoniades, Steve Vance, Thomas Hussey, Yeimy Morel, and Zachary Tereska. Thank you for all you do, day and night, and thank you for allowing me to shut my door and write, write, write! Without your help, this book would still be on the drawing board.

Whenever there is a book, there is an editor and a publisher. I have been the luckiest of authors to have the best in both. First, my eternal gratitude to the amazing Hilary Poole, my editor, coauthor, and friend of countless years

and as many books. You are simply amazing. I refuse to go next to a keyboard unless I am reassured you'll edit the outcome. Thank you!

To everyone at John Wiley & Sons, one of the most professional and exceptional publishers in the world, and especially to my executive editor, Sheck Cho, captain and commander extraordinaire; Judy Howarth, manager of content enablement and operations; and my developmental editor, Christina Verigan. This book is as much yours as it is mine, and I am grateful for all your help, guidance, and support.

To all the cybersecurity and governance professionals around the world, working tirelessly in the field, in academia, in research institutions, in government agencies, and militaries, this book pales in comparison to your achievements every day. Without your endless efforts in breaking new ground, expanding and enhancing our scientific understanding, and guiding us through the turbulent and terrifying waters that cybersecurity is, we would be lost. Your work represents the lighthouse that helps us navigate, and if I aspire to anything, it is for this book to aid in reflecting your light, interpreting your guidance, and adding wind to the sails.

To the many international organizations that help all practitioners learn, hone, and apply their craft, as well as develop the frameworks we depend on, my gratitude for your ongoing contributions, tireless curation, and unending support. I must particularly single out $(ISC)^2$, CERT, ENISA, ISACA, ISECOM, ISO, ISSA, OECD, OWASP, and SANS, with my apologies for omitting the many other deserving organizations worldwide. My specific thanks to Dr. Christos K. Dimitriadis, chairman of the ISACA board of directors, and Matt Loeb, ISACA CEO, for their continuous support, and the ISACA New York chapter for making the chapter a home away from home for me and countless professionals in the New York metro area.

To the book's direct contributors and supporters, Anna Murray, F. Charlene Watson, Frank Downs, and Mark Thomas, thank you for allowing me to include your expertise and to share it with my audience. This book is richer and more useful because of your contributions. And to Mike Barlow, an early supporter and advocate for the book, as well as an accomplished writer in his own right, thank you for everything. Your guidance, advice, and support mean the world to me.

Finally, to Anna Murray, a name that keeps on repeating in these acknowledgments, but from where I sit, not enough! You are the most brilliant, expert, capable, tenacious, fierce, loving, accepting, and giving professional and writer I know! Every day I thank my lucky stars that brought you to my life as my partner in the business and my partner in life. You are, and always will be, the brightest star in the dark of night, guiding me home. Thank you.

CHAPTER 1
Understanding Risk

If you're reading this book, I'd hazard a guess that you've read some of the doom-and-gloom cybersecurity books out there as well. There are many, and many are great (see the bibliography for suggestions). What's more, I am sure you have had your fill of statistics. Dreadful statistics showing how cybercrime is increasing by the day. I'll include some of those, too, just to satisfy any morbid curiosity left in you, but they are essentially useless. By the time the ink is dry on these pages, the numbers have changed. For the worse.

A BRIEF SAMPLING OF DREAD

- Hacker Attack Rate: 39 Seconds

  Assistant Professor of Mechanical Engineering Michel Cukier at the A. James Clark School of Engineering conducted the study that profiled the actions of hackers using brute-force methods to gain access to a set of exposed computers. The results showed that the computers were attacked about 2,244 times per day.
- More than 33 percent of United States consumers have experienced a cyberattack.

  This was reported in a survey by Zogby Analytics commission for the Hartford Steam Boiler Inspection and Insurance Company (HSB), with the most likely victims being between 18 and 24 years old. Moreover, the associated incident costs ranged from $500 for 56 percent of the cases to between $1,000 and $5,000 for 23 percent of the cases.
- According to the "Internet Security Threat Report—Symantec 2017" (Volume 22, April 2017):

- It takes on average two minutes for an Internet of Things (IoT) device to get attacked.
- The average ransom amount for a ransomware attack went from $373 in 2014 to $1,077 in 2016.
- Over the last eight years, more than 7.1 billion identities have been stolen as a result of data breaches.
- In 2016, the United States was number one both in number of data breaches (1,023) and in identities stolen (791,820,040).

- According to the "2017 Data Breach Investigations Report" (Verizon):
  - 75 percent of the breaches are perpetrated by outsiders, versus 25 percent involving insiders.
  - 62 percent of breaches featured hacking, of which 81 percent leveraged stolen or weak passwords.
  - 66 percent of malware was installed through malicious email attachments.
  - 73 percent of the breaches were financially motivated; 21 percent were espionage-driven.
- According to the "Small Business Trends" website (https://smallbiztrends.com):
  - 43 percent of cyberattacks target small business.
  - Only 14 percent of small businesses rate their ability to mitigate cyberrisks vulnerabilities and attacks as highly effective.
  - 60 percent of small companies go out of business within six months of a cyberattack.
  - 48 percent of data security breaches are caused by acts of malicious intent. Human error or system failure account for the rest.
- According to Juniper Research's study titled "The Future of Cybercrime & Security: Financial and Corporate Threats & Mitigation" (Juniper Research, Ltd.):
  - Cybercrime is expected to cost businesses over $2 trillion by 2019.

  - Although North America has seen the lion's share of these breaches (60 percent in 2015), the proportion will level off as global digitization levels the playing field.
- According to "Cybersecurity Ventures' Predictions for 2017 through 2021":
  - The cost of cybercrime damages worldwide is estimated to be $6 trillion annually by 2021.
  - In 2016, the cybersecurity unemployment rate dropped to zero percent, and it is expected to remain at that level through 2021, with a projected job-to-skills shortfall of 1.5 million positions by 2019.
- ISACA's *2016 Cybersecurity Global Data Snapshot* lists social engineering, insider threats, and advanced persistent threats as the top-three threats facing organizations.
- According to Barkly Protects, Inc.:
  - One-third of the IT professionals surveyed by Barkly reported their security had been bypassed by a cyberattack in 2016.
  - 71 percent of organizations targeted with ransomware attacks were successfully infected.
  - Over half the organizations that suffered successful cyberattacks in 2016 are not making any changes to their cybersecurity posture in 2017, with budgetary constraints cited as the main block to improved cybersecurity.

How Much Is It Worth to You?

In the misty past, a person's most valuable possessions were things he could see: his castle, gold, tapestries, even his heirs! Their value was tied to their physical existence.

Today, the concept of *value* has expanded beyond tangibles to include intangibles such as data, intellectual property, and reputation. As a matter of fact, many intangibles hold more value than tangibles. Consider, which is more important: an artisanal pizza or the *recipe* for the artisanal pizza? It's no accident that the phase following the Industrial Revolution has been nicknamed the Information Revolution.

The rise of intangible valuables affects every individual as well as businesses of all sizes. These things of value that individuals and businesses create are—like all things of value—coveted by others and therefore warrant your protection. So, just like you would protect your valuable jewelry, you must protect your valuable data. It's a simple concept.

What is interesting in this analogy is the assumption that we all share a common understanding of what is *of value*. You certainly have no problem intuiting that a set of diamond earrings is valuable and should therefore be stored in a secure place. Which place and how secure? That, too, is straightforward to understand. We have an innate sense of value to guide us in these decisions—something that tells us that a $300 pair of earrings is safe in the jewelry box in the apartment while a $30,000 pair of earrings is best protected in a bank's safe deposit box. Easy to understand and easy to make a value judgment on.

We make these types of judgments every day, and we're very good at it. We understand what's of value, and we understand the risks to this value:

Earrings? Theft!
Property? Fire!

It ends up that we are very good at making complex risk management decisions on a daily basis. Who knew?

Risk! Not Just a Board Game

Consider this situation: It is 11:00 at night, and you just finished dinner with friends at your favorite restaurant. Walking to your car, you reach an intersection and see that the walk signal is red. You look left. You look right. You see a car down the block, shrug it off, and cross the street. No problem.

Now, let's change this scenario a little. Same story, only this time you are pushing a stroller with your baby in it. What's the decision now? Do you cross the street or wait for the signal to change? My bet is you wait.

We just stumbled on the concept of *risk acceptance*, which will prove to be of real importance in the pages that follow. The bottom line is that we all live with risk every single day of our lives. We constantly make decisions about risk and, when we're done evaluating, we take action signifying our acceptance of this risk.

In the example just suggested, in one case you accepted the risk that you can cross the street against the light, and in the other case, when you had your baby along, you did not. How does this translate to the cyberworld? In some cases, we accept the risk of having our information available out there (e.g., when using Facebook, Instagram, Swarm, and the like), and in others we do not (e.g., when we are using our credit card or revealing our medical records).

Studying risk is taking a trip down a fascinating, complex, and intricate labyrinth. It is hard-core science—involving complex mathematics, ethics, and philosophy—with potential life-and-death implications (e.g., the risk of reprisals when we attack a terrorist group, the risks that first responders take every day, etc.). This is certainly not a book to start you on this type of journey, although I have included a selected bibliography for you to consider at the back of this book. The purpose of this book is to expose you to some risk management and tech concepts so that we can develop a common language when discussing how to protect your things of value from cyber-based threats. With that in mind, let's start with a simple definition. What is risk?

Risk is the combination of the likelihood of an event and its impact.

What's the risk of a hurricane in Miami?

Well … how likely is it, and what will its impact be when it hits?

Why do you need know this? Because, for starters, the answer determines whether you want to move there, if you want to start a business there, if you want to send your kids to school there, and how much your insurance will cost you to protect you from this risk, and so on.

How can you determine the likelihood that a hurricane will strike Miami? You have tons and tons of statistical data that give you a good sense of the frequency of hurricanes hitting the area over the past couple of hundred years.

What's the impact? There is the cost of rebuilding, the cost of business losses, environmental damage, and the potential of loss of life, among many others. You get the picture. Who is good at keeping these types of statistics? Insurance companies. But this alone is not the complete picture. Let's fill in the blanks.

First, let's assume you have decided that you want to live in Miami. That's key. That decision (like the road-crossing example discussed earlier) implies some degree of risk acceptance out of the gate. You know that hurricanes strike Miami, yet you choose to live there. Fine. (Who am I to judge? I live in New York!)

But you're not simply living in Miami. Knowing that hurricanes may hit Miami, you have chosen to live in a "hardened" house, meaning a house that is as hurricane-proof as you *choose* to make it. Before buying the house, you did your research, compared options, and decided to buy a house that can withstand a Category 3 hurricane. That was your choice. It was a very important one: You didn't just choose any house. You chose to get a hardened one. This hardened option? That's a *control*. Controls act against risks. Your control was to buy a house that can withstand a Category 3 hurricane. That *mitigates* your risk: If a Category 3 storm hits, you are protected.