CHRIS MOSCHOVITIS

PRIVACY, REGULATIONS, AND CYBERSECURITY

THE ESSENTIAL BUSINESS GUIDE

WILEY

Table of Contents

List of Tables

List of Illustrations

PRIVACY, REGULATIONS, AND CYBERSECURITY

THE ESSENTIAL BUSINESS 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 9781119658740 (hardback)
ISBN 9781119660118 (ePub)
ISBN 9781119660149 (ePDF)

Cover image: © Yuichiro Chino / Getty Images, © dem10 / Getty Images
Cover design: Wiley

FOREWORD

You will never do anything in this world without courage. It is the greatest quality of the mind, next to honor.
—Aristotle

Businesses today are faced with increasing demands for privacy protections, ever-more complex regulations, and ongoing cybersecurity challenges that place heavy demands on scarce resources. During these difficult times it is important that we have the courage to proactively deal with these imperatives. This book is an essential tool for any business executive who needs to orchestrate the "handshake" between privacy, security, and ongoing regulations. Oh yes, and courage.

A few years ago, I returned to one of my passions—security—when I took over as the leader of a business in the eastern US. These last three years have been challenging but exciting, and I have seen an unprecedented level of interest by business executives in privacy and security. I have made more board presentations and been in more meetings with the C-suite on these topics in the last three years than the ten years before that combined. When I was appointed to the board of the ISACA (Information Systems Audit and Controls Association), I was thrilled at the opportunity to make significant change in the security profession. But I expected too much too soon, and the board's message after my first presentation was clear: "We need more research on the concept of information security management and how security is viewed by executives before we make any investments."

It was early in the new millennium, and security was becoming a topic of conversation in the executive suite.

Even though the first CISO had been appointed at Citi in 1995, the body of knowledge for security was defined by technical and product-specific certifications with no frameworks to support organizations, and privacy regulations such as GDPR were still just a distant thought.

At that time, I had made my recommendation to the board of the ISACA to drive the setting of “common body of knowledge” of the future CISO. I had a strong belief that there was wider acceptance of the role and its importance in protecting the organization.

Maybe it was a turning point, but several events came together early in the new millennium to reinforce this belief. “I LOVE YOU” infected millions of computers, followed by the first criminal conviction of a hacker, the widespread disruption caused by denial-of-service attacks on Microsoft systems (and Bill Gates's decree that Microsoft products would embed security as part of the product), and a series of other high-profile hacks. This was exacerbated by the financial collapse of Enron and its impact on the trust in the US economic system. Regulation followed with the Sarbanes-Oxley Act and many others around the globe. It was a new world, and the continued regulation around security and privacy gained momentum.

That year I became chairman of the board of ISACA, and the new body of knowledge accompanied by a certification (CISM) was launched. The founding group was made up of four dedicated CISOs, and the certification is still the standard for security management professionals.

Which brings me back to my good friend Chris, with whom I have formed a terrific bond over mutual interests. Fine food and wine and a connection as first-generation Greeks cemented our friendship. Recently, we discussed and debated many topics, including the need for those executives who understand security risks to transform that

knowledge into action around privacy and security around regulation.

I have found Chris's intellectual curiosity and sense of humor to be both compelling and engaging. These traits are a perfect vehicle to take the reader on this journey, from the fundamentals of privacy to the ongoing regulatory pressures and how companies can be better prepared at the executive level to tackle these changes.

Chris is able to interpret complex principles and distill them into a natural flow, where the reader is taken on a journey. In Homer's *Odyssey*, Circe warned Odysseus of the impending perils so that he would be prepared. Likewise, Chris's book prepares the executive to be aware of the perils and opportunities ahead and provides a roadmap on how to act with courage as security and privacy regulations continue to proliferate.

Be prepared and do the right thing and not just because of regulation—do it for your customers, employees, shareholders, and everyone who places trust in you and your company. Use the step-by-step approach from this book, so you and your company can be ready for whatever challenges the future might hold.

It is time to act, and with this guide in hand, you are well on your journey.

Marios Damianides
Cyber Security Leader, Ernst & Young LLP
Chair of the Board, ISACA (2003–2005)

PREFACE

“What? I've been working like this all my life! Now, you're telling me that I have to be GDP…umm…GD-whatever compliant?”

My friend and client, an immigration attorney from way back when “immigration” was not a dirty word, was angry. Her practice had been very successful over the years, dealing with all sorts of immigration issues across continents. The problem is that she is doing business with citizens of the European Union (EU). Worse, she has a partner in Athens, Greece, an EU-member country.

Fabulous! She must comply with the General Data Protection Regulation of the EU, better known by its acronym, GDPR. For those of you blissfully unaware of GDPR, it is a law passed by the European Union in 2016. It has far-reaching consequences to businesses worldwide, including yours!

If you are a businessperson who, like my friend, has no idea where to begin with GDPR, then this book is for you! It is the sequel to *Cybersecurity Program Development for Business: The Essential Planning Guide* (Wiley, 2018), and just like that book, this one is designed with you, a businessperson, in mind. In *Cybersecurity*, my goal was to give you enough information so that you wouldn't be at the mercy of experts talking over your head and around your business when it came to cybersecurity. In its introduction, I wrote:

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?

The goal, approach, and style remain the same—only this time, the aim is to transform your hard-earned cybersecurity awareness into one that is privacy-centric and regulation-aware. If you're one of the many businesspeople out there who are new to all this, just starting to confront the new cyberwar realities, concerned about yours and your business' privacy, and worried that some regulation will descend to levy God knows what kind of fine, then you're in luck!

This book will guide you through all this step-by-step, section-by-section: privacy, regulations, and cybersecurity. We'll work through the basics together, as well as reviewing case studies and examples of best practices across different industries and different size companies.

Just like in the first book, which I will be referencing frequently, especially in Part Three, we need a case-study disclaimer: The case studies and examples presented throughout both books are aggregated from my own work and from the work of many colleagues who were gracious enough to share their experiences. As you would expect, all names, industries, and geographies have been changed to protect the anonymity of these clients. In some of the cases, multiple problems were combined into one. In

others, many assignments were broken out into a single one. 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.

There is a fundamental difference, though, between the first book and this one. The first book dealt strictly with the practical and pragmatic design of a cybersecurity program with the goal of protecting your business. This book synthesizes two distinct, diverse, and complex segments into a privacy-first and regulation-focused cybersecurity program. If you already have a cybersecurity program in place, then this book will help you hone what's already there into a privacy-centric and regulation-compliant cybersecurity program.

If you don't have a cybersecurity program in place, then… where have you been?

Nevertheless, I am glad you're with us now! This is your opportunity to start building a cybersecurity program from the bottom up that, from inception, will be privacy- and regulation-compliant-focused.

One more thing before we dive right in: Just as it is important to understand what this book is, and who it is for, it is equally important to know what it is not. This is especially true since we will be dealing with topics that are at once scholarly, legal, and technical in nature. This book is not intended to be an academic analysis, a legal brief, or a technical how-to manual, although it will borrow and reflect work from all these disciplines. If you're looking for the latest scholarly book on privacy, an in-depth legal treatment of the California Consumer Privacy Act, or how to configure your firewall, this book is not for you!

This book is intended as a practical, pragmatic, and actionable business guide for people across industries and

business sizes who need to understand what all this talk about privacy really means, what the effect of all these laws and regulations are, and how to put it all together in a cybersecurity program to protect what's of value to them.

It relies heavily on the outstanding work of numerous scholars, lawyers, and information technology and cybersecurity professionals, without whom it would not have been possible to write it. You will find a detailed bibliography of sources at the end of the book, and I urge you to use it and dig deeper as you see fit.

For me, each one of these topics, and especially privacy, represent fascinating areas of study. Privacy and cybersecurity force us to confront questions of how we as people manage difficult, complex concepts and how we translate those concepts into actionable laws and ways of doing business.

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 State University of New York, 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 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 10 MB 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 cell phones 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 Whelan, 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 IASCA, I got certified in three areas: First in cybersecurity, becoming a Certified Information Security Manager (CISM), then in IT governance, becoming Certified in Governance of Enterprise IT (CGEIT), and finally as a Certified Data Privacy Solutions Engineer (CDPSE).

Not one to stand still, and always fascinated by the beauty in complexity, I decided in 2018 to study privacy and its implications on our society, business, and systems. I subsequently joined the International Association of Privacy Professionals (IAPP). Just like ISACA, the IAPP is an incredible community of privacy experts that have dedicated their life to the study and implementation of sound privacy principles. I found a welcome home there and endless resources to help me in my journey that has led me here, to this book, that I am humbled to share with you.

I am privileged to be able to continue my journey, running my firm tmg-emedia, inc., and to be surrounded by incredible professionals, clients, and friends that teach me the value of hard work, dedication, and love every day.

ACKNOWLEDGMENTS

Every book is a labor of love. This one is no different. After I finished my first baby, *Cybersecurity Program Development for Business: The Essential Planning Guide,* I knew I wanted to write a second, one specifically focused on Privacy. The initial idea was unformed but persistent. Privacy intrigued me. The “P” word was used practically daily; legislators were passing laws pretending to preserve it while businesspeople were at a loss about what to do with it.

I was clear from the beginning that I did not want to write a scholarly treatment on privacy. Better-equipped scholars of many stripes have produced, and continue to produce, great works on the subject. My approach was to be similar to the first book: What do we need to know on privacy so that we can be informed as citizens and enabled as professionals? More to a pragmatic point, how does all this privacy legislation affect our capacity to design and deliver an effective cybersecurity program?

To answer all these questions, I came up with the format for this book. It would have three distinct parts: one on privacy; one on regulations, worldwide; and one on privacy-centric cybersecurity program development. The latter would be based on the previous book but enhanced by our understanding of privacy, not just as a concept but as a set of concrete regulatory requirements. The result is in your hands!

Books are never solitary efforts. Yes, the image of the writer toiling away at her desk day-in, day-out is true, but the author brings a universe of people to paper. Same with me. Over the course of 31-plus years in the information

technology 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. Their influence is reflected in the pages that follow. They wrote the book with me.

From my original partner in the business, George Whelan, who religiously collected and kept live computer viruses on floppy disks, to instructors such as 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.

Still, I must start somewhere, and the right place to start is with an apology for my omissions. They are entirely my own.

Next, I want to acknowledge a debt of gratitude to my clients, my true partners to success. Every day, I am honored and privileged to be your ally and to contribute to your goals. I am constantly humbled by all the things that you teach me 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 31 years ago; the founding partners at Allegaert Berger and Vogel, Chris, David, and Michael, for their trust in me, their loyalty, and wise counsel through thick and thin; the amazing team at Kapitus for teaching me and my team how to jump onto a rushing freight train; and to Vigdis Eriksen at Eriksen Translations for her trust in us and for her feedback that makes us better every day!

In the same breath, I want to thank my own partners and associates, whose incredible expertise, loyalty, dedication, skills, empathy, and personal engagement make my and our clients' success possible. They are, alphabetically: Anna

Murray, Atsushi Tatsuoka, Danielle Chianese, Doel Rodriguez, Frank Murray, Greg Andrews, James Rich, Justin Schroeder, Leon Tchekmedyian, Pedro Garrett, Thomas Hussey, Tyler Raineri, and Yeimy Morel. Thank you for the privilege of working with you, for all you do, day and night, and for allowing me to shut my door and write, write, write! You made this possible!

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 one-and-only, walk-on-water-on-her-bad-days, amazing Hilary Poole, my editor, coauthor, and friend of countless years and just as many books. Hilary, you are amazing! I absolutely refuse to go next to a keyboard unless I am reassured that you'll edit the outcome. Thank you!

Deepest thanks 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 and Susan Cerra, the project's managing editor! This book is as much yours as it is mine, and I am grateful for all your help, guidance, and support.

To all the privacy, 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. I cannot emphasize this enough: Without your endless efforts in breaking new ground, expanding and enhancing our scientific understanding, and guiding us through the maze, we would be lost. All your works represent the lighthouses 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 CERT, ENISA, IAPP, ISACA, $(ISC)^2$, ISECOM, ISO, ISSA, NIST, NSA, OECD, OWASP, and SANS, with my apologies for omitting the many other deserving organizations worldwide. My specific thanks to IAPP and ISACA for their continuous support and endless resources. The ISACA New York chapter remains a home away from home for me and countless professionals in the New York metro area.

To the many friends who supported me in so many ways, through encouragement, advice, and love: Jeanne Frank, I know you're watching from Heaven! You were right about the book! Alex and Mari, Richie and Charlene, Sherryl, Sotos, Dimitris and Koralia, and last but not least, Madina, my princess Indira, and my prince Kamron: I don't know what I did to deserve any of you, but I can't imagine life without you! Thank you!

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 person, amazing professional, and talented 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!

PART ONE
Privacy

What man art thou that, thus bescreened in night, so stumblest on my counsel?
—William Shakespeare, *Romeo and Juliet*

CHAPTER 1
Understanding Privacy

Bene vixit, bene qui latuit.
—Ovid*, Tristia*

In case your Latin is rusty, Ovid's quote above translates to: “To live well is to live concealed.” My interpretation is different: “To live well is to live in privacy.”

But let's not get ahead of ourselves here. What, exactly, is *privacy*? What does it mean? What do we understand when we describe something as “private”?

Do we mean *secret?* Is something private also secret? Certainly, the reverse is not true: we can have many secrets that are not private! They may be secrets of others, secret negotiations, secret deals, and so on.

Do we mean *personal?* Is it data coupled with our personhood? If so, is all personal data private? What about our name? Are there degrees of privacy?

Defining privacy has puzzled minds far greater than mine, and the definitions for privacy have been just as grand and diverse. Let's start with our perennial friends at Merriam-Webster. They define privacy as:

1. a: the quality or state of being apart from company or observation: SECLUSION

   b: freedom from unauthorized intrusion

2. a: SECRECY

   b: a private matter: SECRET

3. archaic: a place of seclusion

The *Oxford English Dictionary*, on the other hand, defines privacy as:

1. A state in which one is not observed or disturbed by other people.

   1.1 The state of being free from public attention.

And, one of my favorites, Wiktionary's definition, covers all the bases, albeit sometimes cyclically:

1. The state of being secluded from the presence, sight, or knowledge of others.
2. Freedom from unwanted or undue disturbance of one's private life.
3. Freedom from damaging publicity, public scrutiny, surveillance, and disclosure of personal information, usually by a government or a private organization.
4. (obsolete) A place of seclusion.
5. (obsolete, law) A relationship between parties seen as being a result of their mutual interest or participation in a given transaction, contract, etc.; Privity.
6. (obsolete) Secrecy.
7. (obsolete) A private matter; a secret.

Not to be left out, of course, is the legal definition of privacy. *Black's Law Dictionary* defines privacy as:

The right that determines the nonintervention of secret surveillance and the protection of an individual's information. It is split into 4 categories:

1. Physical: An imposition whereby another individual is restricted from experiencing an individual or a situation;
2. Decisional: The imposition of a restriction that is exclusive to an entity;
3. Informational: The prevention of searching for unknown information; and
4. Dispositional: The prevention of attempts made to get to know the state of mind of an individual.

It's worthwhile to pay attention to those four categories: physical, decisional, informational, and dispositional. We'll be returning to those in more detail when we take on the meanings of privacy for your business.

It's not that I have something to hide,

I have nothing I want you to see.

—Amanda Seyfried

Definitions of privacy have evolved over time, and our understanding of the concept is constantly changing. Therefore, it would be naive to assume that Privacy with a capital P can be rendered via a legal definition, complex or not, or a dictionary entry.

Privacy has been, and remains, the subject of rigorous academic study. Anthropology, sociology, psychology, history, and other disciplines have been looking into the