CYBERCRIME AND BUSINESS

Strategies for Global Corporate Security

Sanford L. Moskowitz

B H

Cybercrime and Business

Strategies for Global Corporate Security

Sanford L. Moskowitz

Butterworth-Heinemann
An imprint of Elsevier

Butterworth-Heinemann is an imprint of Elsevier
The Boulevard, Langford Lane, Kidlington, Oxford OX5 1GB, United Kingdom
50 Hampshire Street, 5th Floor, Cambridge, MA 02139, United States

© 2017 Elsevier Inc. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system, without permission in writing from the publisher. Details on how to seek permission, further information about the Publisher's permissions policies and our arrangements with organizations such as the Copyright Clearance Center and the Copyright Licensing Agency, can be found at our website: www.elsevier.com/permissions.

This book and the individual contributions contained in it are protected under copyright by the Publisher (other than as may be noted herein).

Notices
Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods, professional practices, or medical treatment may become necessary.

Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information, methods, compounds, or experiments described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

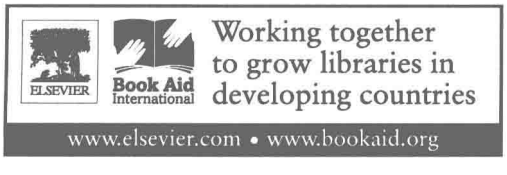
To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

Library of Congress Cataloging-in-Publication Data
A catalog record for this book is available from the Library of Congress

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

ISBN: 978-0-12-800353-4

For information on all Butterworth-Heinemann publications visit our website at https://www.elsevier.com/books-and-journals



Publisher: Candice Janco
Acquisition Editor: Sara Scott
Editorial Project Manager: Hilary Carr
Production Project Manager: Punithavathy Govindaradjane
Cover Designer: Mark Rogers

Typeset by SPi Global, India

To my sister and brothers, Albert, Carol, and Martin, with love

此为试读,需要完整PDF请访问: www.ertongbook.com

Preface

As I write this, the US Congress and America's intelligence agencies are beginning to investigate Russian influence in this country's 2016 election. At the center of these enquiries, of course, is the issue of cybercrime, specifically, Russian hacking of the Democratic National Committee (DNC) and the emails of officials associated with Hillary Clinton's campaign. While this episode has major implications related to integrity of the American electoral system and US-Russian geopolitics, it may also be viewed over time by historians as a watershed in the evolution of global cybercrime. This one incident has brought to the attention of the world the potential impact that a cyberattack can have on the affairs of state. If we consider the DNC a business—which in a very real sense it is—and the people who work for it its employees, then it also reminds us of the powerful damage that cybercrime inflicts on 21st-century organizations in the USA and, by extension, the world at large.

Cybercrime in the second decade of the 21st century appears to have reached a tipping point. That it will continue to be a rapidly growing problem for business and governments seems now inevitable. It is clearly now a fact of life and an unstoppable force that is closely intertwined with so many aspects of our existence, from public policy and national security to the everyday transactions—financial, political, social—that define and shape our roles as citizens, consumers, and members of a global society.

This book focuses in on one aspect of the cybercrime revolution: its troubled relationship to the American and international business community. To be sure, as early as the 1990s, business has been a major target of hackers who over the years, have impressed the world with amazingly daring cyber heists against some of the biggest and most resourceful corporations. Through the stealing of trade secrets, intellectual property, and, even more damaging, personal information of millions of unwitting customers, these perpetrators have inflicted unprecedented damage against consumers, businesses, and national economies. Organizations are only just beginning to wake up to the growing and implacable dangers that they face from hackers worldwide. It seems then

the right time to take a good, hard look at how and why cybercriminals have been so successful in their hunting of digital swag across such a wide swath of the corporate landscape. A basic question that we ask in the chapters to follow is why companies, even those with abundant resources and fine-tuned strategic sense, have found themselves so open and defenseless against the wiles and strategies of the hacking community. In posing this question, we are, at the same time, also asking something else: what are the assortment of cyber-related risks that different companies face as they evolve, and what are the digital threats attached to the various strategies companies tend to select in order to grow?

There has of course been quite a bit of print dedicated to such areas of cybercrime as the technology involved—what digital methods perpetrators use to infiltrate companies, what technology potential victims turn to in effort to protect themselves—and public policy and regulations of different countries—what policies, laws, and regulations governments employ to fight cybercrime and how effective these are.[a] This book, however, gives its attention over to other, less well-known terrain of cybercrime: the relationship between organizational (and inter-organizational) structures and the patterns of cybercriminal activity. Cybercriminals are a highly motivated—as well as technically adept—and quite flexible criminal community. They have come to understand (as many of more upstanding actors on the other side of the law have not) that no one approach to a cyberattack "fits all." Companies of varying sizes working with diverse constellations of associates, and pursuing divergent strategies must be approached differently and on their own terms if the cybercriminal hopes to carry out successful forays. Each company, then, has its own unique "cyberattack profile"—how hackers invade it—depending on that organization's internal structure, size, suppliers, markets, and so forth, and on the types of strategies—mergers, acquisitions, joint venturing, franchising, licensing, etc.—that it uses to expand its operations within its own country and globally. By fleshing out these different attack patterns, we are also revealing to potential victims the risks that they face by growing in certain directions and by adopting one strategic route over another to realize this growth.

This book relies extensively on case studies that have occurred over the last two decades to create these cybercrime risk profiles over two critical dimensions: firm size and corporate strategy. The bottom line in these chapters is that cybercrime can no longer be treated as a side issue by corporate leaders, a once-in-a-while threat to be dealt with reactively and in an at-the-moment, ad-hoc manner by middle managers and IT departments. C-suite executives must take the reins of leadership and understand that they can no longer design their

[a]For a review and analysis of policy and regulations as related to global cybercrime, see [1].

long-term strategic plans without serious consideration of how these plans will affect their fortunes at the hands of clever and determined cyber-thieves. An organization may target a strategic vision that makes sense when it comes to supply, production, and market conditions, but fail miserably—and fatally—in dealing with the onslaught of digital crime that afflicts its house. Strategic policies must begin to be informed by, and designed with, the brutal reality of cybercrime as it is now playing out in the first half of the 21st century.

Moreover, society itself, and not just the corporation, must clearly understand (as we shall see in the following pages) that cybercrime against business takes a very severe toll on a nation as a whole. As cybercrime swells in a country, that nation's economic growth, productivity, employment, innovation, and overall competitiveness plummet. Cybercrime is thus a parasite that feeds on a country's energy and creativity, and sucks the lifeblood from its commercial activity. Social institutions must move to the fore to help limit the power of cybercriminals. Universities must expand the content of their business courses to include teaching future executives how to handle cybercriminal threats at the corporate level, particularly how to incorporate the risks of cybercrime into strategic decision-making; governments at the national and international level need to enact strict laws and regulations against cybercrime and industrial espionage so that businesses have protection against cybercriminals and the confidence to create long-term strategic plans; professional societies must work with universities and governments to set up training workshops for corporate executives for creating and carrying out strategic planning that minimizes the risks for firms from cyber terrorism, piracy, and industrial espionage.

The chapters that follow show clearly the ability of cybercriminals to "add colors to the chameleon"—that is, to adapt their approaches, methods, and tactics to fit each type of firm and its particular strategic vision. These adaptations to types of firm and their strategies on the part of cybercriminals define the variety of cyber-risk profiles faced today by corporate leadership. Following an introductory chapter that presents a general overview of the relationship between cybercrime and business both in the USA and globally, we discuss the various ways in which cyberattacks take place within different types of companies: startups, spinoffs, small and medium-sized enterprises (SMEs), and large, diversified organizations. The remainder of the book puts the spotlight on the major strategies open to businesses that wish to expand their operations and shows how cybercriminals shape their attacks to meet the particular requirements of each strategic plan. The concluding chapter compares and contrasts the cyber-risk profiles for companies that (1) are at different stages in their evolutionary cycle and (2) adopt a particular strategic direction for corporate expansion. In doing so, the chapter expounds on the strategic implications of these risk patterns for companies. It alerts top-level executives of the cyber obstacles that await them when pursuing one or another direction for their firm

and, by so doing, how to avoid—or at least minimize the risks inherent in—such dangers. It further cautions that their continued refusal to take on the mantle of leadership when it comes to fighting cybercrime now comes at an increasingly steep price and, in this digital age, can only play havoc with the future of their companies and with the economic well-being of the countries within which they reside.

Reference

[1] Clough J. Principles of cybercrime. Cambridge, UK: Cambridge University Press; 2010 [chapters 1–6].

Acknowledgments

I received great encouragement and help during the course of writing this book from many academic colleagues and industry contacts with expertise in industrial espionage and cybercrime. They regularly provided me with useful information and insights, including leading me to helpful sources and suggestions for case study analysis. They were very patient with me and with my constant barrage of questions and "devil's advocate" positions and arguments.

I do want to especially thank my two research assistants, Sabrina Schultz and Ingrid Pfefferle, for their very valuable contributions to this book. More than any others, they served in the trenches with me during the writing stages. Sabrina was a tireless researcher who contributed extremely useful perspectives on a number of the case studies in this book. Sabrina found and brilliantly analyzed some of the less well-known cases that added immeasurably to this book. She also provided outstanding analysis and insights into the relevance of globalization and geopolitical trends on cybercrime in the USA and internationally. I incorporated many of her insights into these chapters. Ingrid also needs to be recognized for her important contributions. This book made superb use of her abilities as a researcher, editor and critic. She produced excellent case study analysis, especially when it came to those instances that involved cybercrimes committed against the larger companies, such as Target. She also had very definite ideas about what should be included (and not included) in this book, and how certain ideas should be expressed and developed. I found Ingrid's comments immensely useful as I set about writing up my chapters.

Finally, I want to thank Brian Romer, Senior Acquisitions Editor at Elsevier/Butterworth-Heinemann, for coming to me with the idea for this project and guiding me through the proposal stage. This book would not have happened without him. I must also acknowledge the patience and great work of my editors at Butterworth Heinemann—Hilary Carr and Punithavathy Govindaradjane—throughout the course of this project. I am not sure I would have ever completed this book if it were not for Hilary in particular urging me forward and her continued confidence in my work even as I struggled with completing chapters in a timely manner.

此为试读,需要完整PDF请访问: www.ertongbook.com

Contents

此为试读,需要完整PDF请访问: www.ertongbook.com