Additional praise for *Cyber Threat! How to Manage the Growing Risk of Cyber Attacks*

“Don Ulsch has written a provocative and informative book that is a must-read for all board members. You cannot protect against risks you are not aware of, and, although at times his message is scary, Don certainly lays out the cyber risks companies face.”

—Debra Squires-Lee, Partner, Sherin and Lodgen, LLP

“Don Ulsch’s new book is a passionate, sincere, and thorough analysis of the problem of cyber attacks, in all of its aspects. The Introduction title, “What Every Current and Future Senior Executive Must Know about the Cyber Threat,” summarizes perfectly the vast content of Don’s book. One does not have to be a senior executive in order to understand, appreciate, and enjoy Don’s book. A must-read, definitely.”

—Dimitris Zografopoulos, PhD, Legal Auditor at Hellenic Data Protection Authority, Member of DAPIX Working Group on Information Exchange and Data Protection–Council of European Union

“Don Ulsch provides a great summary of the threats that companies face in cyberspace. It is only with awareness of the real threats that organizations face that executives can take the appropriate actions to protect their companies.”

—Ira Winkler, President, Secure Mentem

“As a CISO and enterprise risk professional, I found the topics covered insightful and well-timed. Cyber threat spreads fire to the risk landscape and gives a realistic, useful, and fact-based education for the senior-level executive.”

—Nikk Gilbert, CISSP, CISM, Vice President and Chief Information Security Officer,

“The time to hide from the cyber threat is over, thanks to this book: a useful tool to protect your corporation, your family, and yourself from a cyber attack. Another example of Don’s wisdom.”

—Manuel González Alonso, former Spanish Police Chief Inspector, Security Chief, Criminologist, Detective, and current Chief Executive Officer in “DARTE Investigación Privada”

“The loss of security around our most valued information has become an enormous drain on our national resources and is disruptive to our everyday lives. The source of risks is not always what they appear to be. Mr. Ulsch’s sage advice and counsel helps each of us who handle or manage important information limit our exposure and loss of information.”

—Danny Miller, System Chief Information Security Officer, Office of the Chief Information Officer, the Texas A&M University System
“Don has dedicated his professional career to researching and educating various industry groups about cyber security, and he is truly a global expert. Don clearly explains cyber security threats originating from sources domestic and foreign, how cyber attacks are perpetrated, and why organized crime, terrorist organizations, and some countries are winning the cyber war. *Cyber Threat!* alerts readers as to how and why electronic information is at risk and provides solutions on how to protect this information.”

—Thomas Alger, Director of Risk Management, Mass Development

“Don has given the information security community a very insightful book, which will assist us in navigating an increasingly turbulent, pervasive, ever-evolving cybersecurity landscape, by providing an abundance of essential knowledge. *Cyber Threat!* answers the pertinent questions that all CISOs should be asking in the year 2014. If you are looking for some of the missing pieces to the global information security puzzle or simply want to understand the current cybersecurity reality to which we must awaken each morning, then *Cyber Threat* is a must-read.”

—Bob Ganim, Chief Information Security Officer, Global Investment Management Firm

“This easy-to-read, yet highly informative, book exposes the frightening truth about the growing risk of the increasingly sophisticated cyber attacks that threaten businesses today. Written in a snappy, nontechnical style, the author explains key facts and policy considerations using engaging stories and illustrative anecdotes. Throughout the book, the reader is presented with sensible recommendations and enterprise governance strategies to deal with these threats. This is an essential read for corporate executives and members of boards of directors.”

—David R. Wilson, Esq., President, Gateway Associates

“*Cyber Threat!* clearly sets the scene for today’s challenges in this arena. Don addresses the global threat environment head-on and then discusses essential ways to protect intellectual property, infrastructure, and corporate reputation. It is a must-read for all IT security and compliance professionals.”

—David A. Wilkinson, The Bellwether Group, Inc.

“The corporate board room is under attack from many sides, the most concerning of which is the threat of cyber crimes. Don Ulsch is uniquely qualified to provide effective protection techniques to ensure that the integrity of corporate information is maintained at the highest level. This book is a must-read for all levels of management in both the private and public sector.”

—Donald P. Hart, Esq., Nantucket, Massachusetts

“We’ve embarked on the ‘Internet of things’ without a clear understanding of what it will mean to our digital and personal lives. Don gives us the undeniable facts that every board member and corporate executive should read. You can’t ignore the truth after you read this book.”

—Patricia Titus, Vice President and Chief Information Security Officer, Freddie Mac
Cyber Threat!
The Wiley Corporate F&A series provides information, tools, and insights to corporate professionals responsible for issues affecting the profitability of their company, from accounting and finance to internal controls and performance management.

Founded in 1807, John Wiley & Sons is the oldest independent publishing company in the United States. With offices in North America, Europe, Asia, and Australia, Wiley is globally committed to developing and marketing print and electronic products and services for our customers’ professional and personal knowledge and understanding.
Cyber Threat!

How to Manage the Growing Risk of Cyber Attacks

N. MacDonnell Ulsch

Wiley
To my wife, Susan Shea Ulsch, my mother, Evelyn Frankenberg Houck, my brother, Phillip Ulsch, and his wife, Josie, my daughter, Jeanne McCabe, and Kenneth Brown. Around them, and their own growing families, my own universe revolves. To Joseph and Margaret Frankenberg, and N. M. Ulsch Sr. And to those in our family who fought overseas for the enduring liberty we enjoy years after their sacrifice: N. M. Ulsch Jr., Edward Frankenberg, Joseph Frankenberg, and Archie Shea.
Contents

Foreword xi
Preface xv
Acknowledgments xvii

Introduction: What Every Current and Future Senior Executive Must Know about the Cyber Threat: A Perfect Digital Storm Is Forming 1

- What Factors Create a Perfect Storm? 2
- Increasingly Sophisticated Attacks 8
- Mobile Devices at Higher Risk 9
- Sometimes Security Just Doesn’t Take Hold 9
- It Wasn’t Always Like This 10
- Without a Bang 11
- A Board Issue 12
- The Cyber Frankenstein Cometh 13
- Defining Success 14
- Notes 15

PART I: THE CYBER THREAT TO THE CORPORATE BRAND: HOW IT WILL IMPACT YOUR COMPANY

Chapter 1: The Rise of Cyber Organized Crime and Its Global Impact 19

- Is Nothing Sacred? 23
- The Liberty Reserve Case: Money Laundering in the Digital Age 24
- The Corruption Factor 27
- Information Threat, Physical Threat 32
- Notes 33
Chapter 2: The Emergence of the Cyber Nation-State and Technology Espionage: Red China Rising and Its Global Cyber Theft Strategy 35

A Case of Cyber Espionage Conspiracy? 43
According to the Select Committee . . . 54
Notes 55

Chapter 3: Cyber Al Qaeda Poses a Threat to Critical Infrastructure 57

A Disabled America 59
A New Age: Inspiring Terrorists and Terrorism 62
A Call Heard Vaguely 64
Attack upon Attack, No Peace in Sight 67
Notes 68

PART II: CORPORATE VULNERABILITIES IN THE DIGITAL SOCIETY: PREPARE TO DEFEND YOURSELF AND YOUR BRAND

Chapter 4: What Is the True Cost of a Cyber Attack? 71

Cyber Attack Detection Sometimes Takes Years 74
One of the First Questions: “How Much Will This Cost?” 76
A Few Common Cost Factors 77
What about Unreported Breaches? 78
Cyber Attacks Result in a Wider Impact: The Community 81
Notes 83

Chapter 5: U.S. Cyber Public Policy: Don’t Rely on It to Protect the Brand 85

No Guarantees with This Executive Order 88
Government-Industry Cooperation: No Silver Bullet 91
The Challenge of Defining Cyber Public Policy 92
Cold War II: The Cyber Chapter 93
Is There a Silver Lining in an Attack? 97
Notes 102
Chapter 6: Four Trends Driving Cyber Breaches and Increasing Corporate Risk: Technological, Cultural, Economic, and Geopolitical Shifts

Technology Trend 104
Loss of Situational Awareness: Distraction 107
Culture 108
Technology Is a Double-Edged Sword 109
Notes 112

Chapter 7: Social Media and Digital Protest

Social Media: A Tool for Disruption, a Model for Change 116
The Hacker Group Anonymous 117
Anarchaos: In the Image of Anonymous 125
Notes 126

PART III: PROTECTING THE BRAND: ACTIONS EXECUTIVE MANAGEMENT MUST TAKE TO REDUCE CYBER RISK

Chapter 8: Managing the Brand When the Worst Occurs

Be Prepared 132

Chapter 9: Managing the Big Risk: Third-Party Vendors

Background Investigation Suggestions to Improve Process 149
Risk-Reinforced Service Level Agreements 154
Clouds Fill the Horizon 166
Notes 169

Chapter 10: Creating Executive Cyber Risk Councils

The Goal of the Executive Cyber Risk Council 175
Who Should Be Included in the Executive Risk Council? 176

Chapter 11: Early Warnings: Something Bad Is on the Way

Technical Signals Are There—But You’ve Got to Look 187
Know Who’s Inside the Enterprise 190
What a Web We Weave . . . When Surfing 192

About the Author 197

Index 199
Foreword

Like a red morn that even betokened, Wreck to
the seaman, tempest to the field, Sorrow to the
shepherds, woe unto the birds, Gusts and foul
flaws to herdsmen and to herds.

—Shakespeare, Venus and Adonis (1593)

It has been some time since you have read and studied Shakespeare,
let me offer another version of the warning in the epigraph:

Red sky in the morning—Sailors take warning.

—Author, unknown

Don Ulsch has once again, in his most recent book, clearly explained the
cyber threat risks. This threat became crystal clear to me, when, as U.S.
Attorney for the District of Massachusetts, I was approached by a U.S.–based
Fortune 150 company that was being extorted by an organized crime syndi-
cate, operating with impunity, in an eastern European country. The demand:
cash. The risk for the company: the loss of years of product research and
development and hundreds of millions of dollars of future revenue.

Frustratingly, the organized crime syndicate operated in a place beyond
the reach of our federal government resources. The lessons I learned during
that investigation were the great and growing cyber risks faced by U.S.
companies and the limited abilities of our government to protect those
companies and their shareholders from this harm. It is morning in corporate America, and many are facing a red sky.

Notwithstanding this real and escalating harm that costs our government, consumers, and the private sector billions in losses, far too many executives continue to ignore the “perfect storm” we are facing.

Louis Pasteur once said, “Chance favors the prepared mind.” Don Ulsch explains how chance also favors the prepared company.

When Thomas Alva Edison said “Genius is 1% inspiration and 99% perspiration,” his idea of perspiration was hard work, not worry. To be successful in protecting a company’s assets from today’s threats requires 99 percent preparation and 1 percent perspiration. For those executives who view their companies as less than 99 percent prepared, Don Ulsch’s book is just the right prescription. And like the early sailor viewing the sunset, the benefits for those prepared executives will be a “red sky at night—and the executives delight.”

—Michael Sullivan
Partner
Ashcroft Law Firm
Kansas City, Missouri
WHERE TO begin? Start with the fundamental assertion that we are at war, a cyber war. The topic is expansive and seems to become more inclusive every day as the word “cyber” enters almost every aspect of our lives. “Cyber” is becoming so familiar to us now that we passively accept anything associated with it. We don’t always appreciate that, but it is true, and it becomes truer with every new day and Internet-enabled device. We don’t see all of these devices, either. From laptops and smartphones and tablets to automobiles to refrigerators, cockpits, and smart homes, we are connected. The utilities that power our inventions and domiciles are connected. Hospitals are connected. Retail stores, insurance companies, defense contractors, automobile manufacturers are connected, too, as are chemical manufacturers, agriculture, and government. It seems like everyone is connected to everything, and all is connected to or by the Internet.

And that’s great—or so it seems. But the bad actors of the world, from organized criminals to narcotics traffickers to identity thieves to traffickers of humans, sex, illegal arms, and even weapons of mass destruction, have also found a cyber stage upon which to perform.

This book is about three defined issues. First is the cyber threat. Growing worse by the day, it is omnipresent, diversified, giving the word “cyber” a bad reputation. Cyber love, cyber kindness, cyber humility, cyber goodness, cyber cheer—these terms are vastly outgunned by other cyber-ish terms. Cyber war, cyber terror, cyber bullying, cyber fraud, cyber spying, cyber crime come to mind.

Second is the notion of vulnerability. What makes us vulnerable, and what increases this vulnerability? Things like social media contribute to this state of vulnerability. So does mobility, a culture of information on demand, anywhere, anytime, and on any device. It seems the more information-rich and information-device diverse we become, the more vulnerable we become. Somewhat insidiously, the more vulnerable we become, the less we may
realize it. Why? Because we are so intimately familiar with all things cyber. Cyber haunts the backstory of most everything we do. It is invisible. Only its symbols are seemingly magically visible. Its commonness instills if not a sense of trust, then one of virtual indifference. As with a colorful toy, we are mesmerized with cyber things, even if the word is never uttered. Games, maps, menus, books, movies, lectures, newspapers, magazines, and just about everything else is digital.

The third undertaking is what enterprises can do to help offset the threats by addressing vulnerabilities. Interestingly enough, governments are trying to reduce the threats through public policy, regulation, security guidelines, and frameworks. However, there is no escaping the fact that every organization must face these issues, with or without input and insight from the government. These are not assignable risks. This book examines some of the things organizations, from government to public and private enterprises, should do to prepare for what many consider to be an inevitable breach. No organization is helpless. Far from it. The issue isn’t that there’s nothing to do, that we’re totally defenseless. It’s more that the synaptic charges that are supposed to get through to the boards lose thrust and intensity along the way.

Ralph Waldo Emerson once wrote that nothing great ever happens without enthusiasm. One of the great things that can be done in the face of the powerful cyber threat is simply to accept it, confront it head-on, and commit to managing the risks it conveys. There is an opportunity to generate enthusiasm about managing the cyber threat, about mitigating the risks it poses.

Divided into three parts, this book conveys the message that “security” and “technology” are two words that every board director must embrace, because these two words result in two other words that the board understands all too well: “risk impact.” Part I examines the cyber threat in its many forms. Part II takes a look at the vulnerabilities common to companies, while Part III provides strategies for more effectively controlling the risks associated with cyber attacks.

This book hopes to instill that enthusiasm by discussing the threat, examining the vulnerabilities, and embracing change that leads to more resilience and resistance to the threat. But one thing is certain: Cyber crime is like any other crime. It isn’t going away. Just the opposite seems true. And a cyber war defines war. No war in the future will take place without this dimension. We live in a digital universe, for better or worse. Make no mistake. We need to manage the cyber element of our universe so that it does not manage us. The greatest risk is in failing to meet this threat.
Acknowledgments

While one person may be responsible for actually writing a book, it is by no means a solitary pursuit. Certainly that was the case with Cyber Threat! My thinking about the evolution of the asymmetric cyber threat has been shaped by many people whose opinions and perspectives I respect. While we do not always agree on every issue, I do believe that the big cyber threat picture is coming clearly into focus and that we agree on many aspects of the problem and the solutions. Unhesitatingly, I would say that without their contributions, this book would not have been possible. In many ways this is a race against time, a race to close the gaps before the digital barbarians get through the gate. On that we all agree. Whatever deficiencies this volume may suffer are the fault of the author, not those who generously contributed their time and expertise.

The cyber threat is not just a computer or technology issue. It is a fundamental business and industry issue, comprised of technology and human behavior. It is a problem that has leached into virtually every dimension and aspect of life. As a threat, it packs a powerful blow. Balancing the threat against the necessity of all things cyber is a delicate exercise. As they say, it’s complicated. It also requires many vantage points. I have been fortunate in receiving many perspectives on the subject.

Writing a book is a family affair, and this one was no exception. All we have is time, and how we spend it matters. I felt this was an important subject, and so did my family, and it was therefore worth the commitment. This book would not have been possible without the love and support of my family.

First, a special thanks to my wife, Susan, who is a tireless researcher and constant editor who continuously challenges assumptions and supported this effort from day one. My mother, Evelyn Houck, also encouraged the effort and supported it in many ways. My brother, Phillip, of the Maverick Insurance Agency, provided special insight on cyber insurance and risk. Kenneth Brown, an adviser at ZeroPoint Risk Research where I worked for nearly five years,
proved to be a strong sounding board about banking, the economy, and risk management.

Michael J. Sullivan of the Ashcroft Sullivan LLC law firm deserves special thanks, and not only for contributing the foreword of this book. Mike has dedicated much of his career to public service and personifies what it means to serve, most recently as the U.S. attorney for the District of Massachusetts and as director of the Bureau of Alcohol, Tobacco, Firearms and Explosives. He has prosecuted war criminals, terrorists, and cyber criminals, among others. Mike dedicated his invaluable time in discussing the issues examined in this book. Working with Mike are an exemplary group of professionals, including former U.S. assistant attorney Brian J. Leske, attorney Ellen Giblin, attorney Amy Barry, and Michelle Reilly, who are always professional, resourceful, and supportive and who have contributed selflessly. I also want to thank former U.S. attorney general John Ashcroft, David Ayers, and Paul Garrett of the Ashcroft Group LLC.

Ken Mortensen, former associate deputy attorney general, spent many hours with me at the Patriot Diner discussing transnational organized crime, privacy, and many other cyber threat issues. I would also like to express my gratitude to Thomas Garruba for his insights. A number of executives at Boston Private Bank and Trust Company were generous with their time and expertise, including Chief Risk Officer Timothy MacDonald, Rich Byron, attorney Victoria Kane, William Kane, Christine Cioffi, and Tiffany DeMontier.

My sincerest thanks to attorneys Heather Egan Sussman of the Boston office of McDermott, Emery & Will LLP, and attorneys Jennifer Geeter and Jon Dabney of the Washington, D.C., office. All have been a pleasure to work with, often under trying circumstances, and all three are exceptional.

I owe special gratitude to my former ZeroPoint Risk Research partners and colleagues Lorie Skolski, Gerard Kane, Steve Grosso, and former FBI special agent and security executive Joseph DeSalvo. They were always unwavering in their support and are dedicated professionals for whom I have exceptional regard.

To former Boston police commissioner Edward F. Davis, thank you. Catapulted into the national spotlight during the Boston Marathon terrorist bombing in 2013, he was a tireless figure when it seemed Boston was under siege.

Attorneys William “Bill” Rogers, John F. Bradley, and Peter J. Caruso of Prince Lobel Tye LLP in Boston have been generous with their time and expertise, as has former federal prosecutor Joseph M. Burton, managing partner of the San Francisco office of Duane Morris LLP, and Eduard Goodman of ID
Theft 911. Dr. Lothar Determann, an attorney at Baker & McKenzie LLP, has been very helpful, and I appreciate his expertise and efforts. I extend my thanks to Holly Chase, a bank regulator and expert in financial institution risk, and to Elton Hill, who retired recently from the Federal Reserve. I also want to acknowledge Kevin Hamel, who leads the privacy and security initiative at COCC.

For many years I have been associated with the National Security Institute. Thank you to my NSI colleagues Stephen Burns, David Marston, and the late Edward Hymoff. Much of what I know about security I learned at NSI. It was Ed, formerly with the forerunner of the Central Intelligence Agency, the Office of Strategic Services, who one day a number of years ago, while I was teaching at Boston University, said, “There are a couple of former military guys I’d like you to meet.” It was Dave and Steve. A great American and national treasure also serves on the advisory board of the National Security Institute, four-star General Earl Anderson, U.S. Marine Corps (Retired), the youngest active-duty Marine ever promoted to the rank of general. He is also the former assistant commandant of the Marine Corps. At this writing he is 94 years old. Semper Fi, General.

For their invaluable contributions over the years I would like to thank attorney David R. Wilson, John Cassella, Thomas Barrett, and Colonel James Bullion, U.S. Army (Retired). Colonel Bullion served two tours in Iraq and has spent a great deal of time in Afghanistan with the Department of Defense, where understanding the nature of threats and responding accordingly is essential to survival.

Retired Marine Corps officers and National Security Agency veterans Ed Lucke and Jeffrey Zimmerman have long been colleagues whose experiences also shaped my appreciation of threat and risk. Dr. Larry Ponemon and Susan Jayson of the Ponemon Institute have been very supportive, encouraging, and generous with their research. I would like to thank Jerry Archer, Jim Malatesta, Jin Kim, Richard Crawford, Phill Bakker, Joe Judge, Jeffrey Bamberger, Dr. Angelo Tosi, and John Rostern for their observations and support over the years. Thank you also to Thomas Wagner for your advice and counsel.

Anthony Kimery, executive editor of Homeland Security Today, has been extremely helpful and insightful and always supportive. Thank you, Christopher Pierson, for your studied perspective on privacy, and Tom Alger. Andy Briney of TechTarget is always helpful, and I have appreciated his counsel and observations through the years. I also want to acknowledge Kathleen Richards and Eric Parizo of TechTarget, as well as Eileen Feretic of Baseline magazine.
Thank you, Elizabeth C. and T. Brooks Fitzsimmons.

To Brian Powers, David Mechanic, Dennis Huaman, Maryalice Decamp, Brian Kelly, Chris Winn, Christo Ovcharov, Paul Rozek, Beth Healy, David Welch, Captain G. Mark Hardy, U.S. Navy (Retired), attorney Annemarie McAvoy of Fordham University Law School, Gary Foster, and Dr. Jack Kerivan, thank you for your continuous support and encouragement. Michael Fountain and Mike Weir, thank you.

Also deserving of thanks are Thomas E. Samoluk, attorney, executive, and author, whose commentary on certain subjects has proved spine-stirring, Anne Marie Graceffa, and David Rawlings. Dan Swartwood of the Ponemon Institute and president of the Society for the Policing of the Cyberspace, thank you for your insights. Debra Squires-Lee of Sherin Lodgen LLP is deserving of thanks. John Colucci of the McLane law firm, thanks for your frequent counsel. I appreciate the contribution of Nicola Crawford of i-Risk Europe Ltd. Much appreciation to Nikk Gilbert, CISO of CUNA Mutual, and Naheed Bleecker for their continuing support. To Kevin Hamel, vice president of security at COCC, thank you for your observations and support. To Eileen Turcotte, thank you.

I want to extend my appreciation to Neil Doherty and to attorney Scott Kannry for their always interesting observations regarding privacy and risk.

To David Wilkinson and Karen E. Antons of the Bellwether Group Inc., and M. J. Vaidya, an adjunct professor at New York University and Americas CISO at General Motors, your support is appreciated. Thank you, Constantine Karbaliotis, for your expert counsel, and to Catherine A. Allen and Robin Slade of the Santa Fe Group.

Tomas Filipiak served overseas as an officer in the U.S. Army as an information security professional and understands the cyber threat and its life and death implications in a combat zone. I appreciate his observations. To Matthew Lion, Erin Weber, Sanjay Deo of 24by7 Security LLC, and Clay Moegenberg, I appreciate your always interesting perspective and support. Insurance executive and privacy and security specialist John Graham of Zurich North America was very helpful, as always, and my appreciation goes also to Jim Randall, who is head of global cyber security for Zurich. Danny Miller, system CISO of the Texas A&M University System, was very helpful.

Much of the effort to protect consumers in the United States against the cyber threat is undertaken by states. None is more deserving of mention than the Commonwealth of Massachusetts. Leading this effort are Barbara Anthony, undersecretary of the Office of Consumer Affairs and Business Regulation, and
her exceptional team, including Deputy General Counsel Joanne Campo, Julian W. Smith, and Maureen Tobin—thanks for your good work and leadership.

My appreciation is also extended to Paul D’Ambrosio, MD, Andrew DiLernia, MD, and Karyn M. Connolly.

Benjamin Dubuc traveled to China to teach English after graduating from the University of New Hampshire and kept in touch on the cyber threat there, which was greatly appreciated.

Stacey Rivera, my editor at John Wiley & Sons, has proved to be more than patient and exceptionally competent, and I want to thank her for making this book better than it otherwise would have been.

Maintaining integrity in the enterprise is the job of everyone, but the actions of those security, compliance, and privacy officers are vital. Thanks to those whose battle every day is to defend against the cyber threat.

Last but not least, there are others who deserve thanks but their identities will have to remain confidential, as they continue to work behind the scenes in the interest of law enforcement and national security. You know who you are, and I appreciate your work, as do many others.