CYBERSECURITY FOR EXECUTIVES

A Practical Guide

Gregory J. Touhill and C. Joseph Touhill

AIChE
The Global Home of Chemical Engineers

WILEY

CYBERSECURITY FOR EXECUTIVES

A Practical Guide

Gregory J. Touhill

C. Joseph Touhill

AIChE

WILEY

Library of Congress Cataloging-in-Publication Data

Touhill, Gregory J.
Cybersecurity for executives : a practical guide / by Gregory J. Touhill and C. Joseph Touhill.
pages cm
Includes bibliographical references and index.
ISBN 978-1-118-88814-8 (cloth)
1. Computer networks–Security measures. I. Touhill, C. J., 1938– II. Title.
TK5105.59.T67 2014
658.4′78–dc23

2014002691

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

To our wives and children

FOREWORD

I always have thought of myself as a savvy businessman. I worked for or served on the boards of some of the best known and most successful companies in the world. Additionally, I started several companies, beginning small and growing them into successful enterprises. I've been CEO of a New York Stock Exchange member firm and a board member of 20 publicly owned companies. I believed that I had a pretty good handle on how technology benefits the management of businesses of all sizes. In fact, I prided myself at being an early adopter of computers, incorporating them into my businesses where they quickly became indispensable to our operations. Computers enabled us to be more productive and efficient, improving the value proposition of our businesses.

I'll be the first to admit that I am not an expert on computers. Like other senior executives, I recognize their great value and look for opportunities to improve my businesses through automation. As computers became more integral to our businesses, I developed a healthy respect for those who understood the mysteries that lurked within that box. While I liked to fiddle with my computer from time to time, I never deluded myself into believing I was a "computer expert." When I needed help, I went to the professionals.

I saw the explosion of innovative technology in the 1990s, and took the advances pretty much in stride, but then something alarming happened. At first it was an annoyance, but as time went on, a scary scenario. Reports of "hackers" penetrating businesses to steal consumer's personal and financial information started appearing in the newspapers. First it was just isolated attacks, often accomplished by insiders with an axe to grind. But the reports kept coming from all business sectors with increasingly negative effects, including interruptions to operations, expensive lawsuits, and regulatory fines. The computer systems that my colleagues and I had installed to improve our productivity and efficiency were now under threat, or siege by hackers.

Obviously all businesses today heavily rely on computers. Most cannot operate in today's highly competitive markets without trusted, timely, and accurate information. That's why it is very important for executives to have a solid understanding of the emerging role of "cybersecurity" as a prime mechanism to control and manage risk. Like many executives, I needed to become smarter and better versed on cybersecurity quickly.

I was fortunate to be introduced to Greg Touhill by my friend John Maluda, a Telos Corporation director. John told me that Greg was retiring from the U.S. Air Force where he was the general in charge of cybersecurity and information technology for one of the nation's ten combat commands. John told me that Greg was an expert on cybersecurity

and led his team to the Rowlett Award, which is given to the organization that has the best cyber defense in the Department of Defense. After a long and distinguished military career, Greg was taking his experience as a CIO and cybersecurity professional to the business world.

Greg joined the Corporate Director's Group, an organization I founded, on John's recommendation and quickly earned his Professional Director certification. His transition from the battlefield to the boardroom has been smooth and transparent as he possesses not only the leadership skills typical of generals, but he also has mastered business principles and maintains his technical certifications in cybersecurity. He now is a highly successful consultant and an adjunct professor at Washington University in St. Louis teaching (of course) cybersecurity.

Cybersecurity is a hot topic among the Corporate Director's Group members and executives in general. While at a recent CDG seminar on cybersecurity, Greg told me that he was in the process of writing a book for people like me. He said it would be entitled, *Cybersecurity for Executives: A Practical Guide*. I told Greg that I couldn't wait to get my hands on it as most writing on cybersecurity is focused on simply scaring people or is written in technical jargon that is nearly undecipherable to the common person. Greg assured me that not only would I understand the message of his book but also I would be able to put it to very practical use immediately.

I am delighted that Greg and his father Joe, a long-time executive, CEO, and board member, wrote this book. It was an easy read; in fact at times I found it hard to put down. They present the material with clarity, humor, and flair. When I finished the draft he gave me, I said, "Greg, I believe you have a real winner here! Executives and directors ought to read this book!"

I meant what I said. I believe this book ought to be the Cybersecurity Bible on every executive's desk. It lays out what the threat to business is from unscrupulous intruders; it frames the problem in terms of risk management; it tells you how to build an appropriate corporate strategy to deal with attempts to steal or alter data and information; it sets out in detail the policies and procedures you need to protect your organizations; and it tells you what changes you need to make with software, hardware, and personnel to make your plan work. It also tells you how to measure the success of your defenses. Additionally, it addresses unique threats to critical infrastructure. Until I read the book, I didn't realize that there are many legal requirements and responsibilities that must be complied with if you are hacked.

There are two chapters that really resonated for me. The first is Chapter 9. In fact, I anticipate some readers may skip to that chapter first for obvious reasons. But if you do, please go back and read from the beginning. You will be glad you did. The formulation of the Disaster Recovery and Business Continuity Plan and the steps called for in implementation are worth the price of the book. When you are hacked (and most experts, including the Touhills, believe that everyone will be sometime), read the chapter carefully and go down the list of recommendations carefully.

The last Chapter 10 had special meaning to me, on several levels. First, I have served on numerous boards of all types over the years—public and private companies, and hospitals and charitable organizations. To me successful programs happen only when you have a fully informed and fully engaged board. Second, I believe the

creative setting of the chapter captures the essence of most board meetings I attend. I was fascinated, for instance, by the story of the Kilcawley Chemical Corporation. An eye opener.

In summary, this is a terrific, important and well-written book by experts. I believe it will be your standard reference, as well, when you encounter tricky cybersecurity issues. Read it carefully and use it well.

Clint Allen
A.C. Allen & Company
Needham, MA

PREFACE

Cybersecurity is the deliberate synergy of technologies, processes, and practices to protect information and the networks, computer systems and appliances, and programs used to collect, process, store, and transport that information from attack, damage, and unauthorized access.

Brigadier General Gregory J. Touhill,
United States Air Force (retired)

As my retirement from the United States Air Force was nearing, I contemplated what I would do in my next career. The Air Force had prepared me well to serve in a number of senior executive roles in the private sector. As I went through the excellent transition class the Air Force offers its departing Airmen, I looked at my resume and saw a lot of opportunity. I have extensive leadership and management experience in electronics, telecommunications, software development, finance, program management, information technology, and cybersecurity. I commanded at the squadron, group, and wing levels. I managed the Air Force's US $22B information technology budget at the Pentagon. I served as a diplomat when I was the defense attaché to the State of Kuwait during our nation's crucial transition from Iraq. I was the base commander (equivalent to a chief executive officer) of Keesler Air Force Base, with an annual budget of US $1.3B and 12,000 personnel under my command. I have been a chief information officer (CIO) several times and maintain my technical certifications as a certified information systems security professional (CISSP). In my last assignment as the United States Transportation Command CIO, my team and I were recognized by the National Security Agency with the 2013 Rowlett Award for the best Information Assurance Program in the United States Department of Defense. As my military career came to its conclusion, I was well prepared to do many different things yet I was confronted by a new problem: choosing what to do next.

I did not have to wait too long to find my answer. While I was still in uniform, I had countless discussions with the CEOs and CIOs that my units did business with over how they protected and secured *my* information. I was keenly aware that my information needed to be protected from inadvertent disclosure to those who didn't have "a need to know." One of my duties was to make sure our partners properly protected our military information. I found that more often than not I ended up educating many of our business partners on how to protect *our* vital information, how to implement best practices in cybersecurity, how to educate their work force, how to audit for cybersecurity compliance, and how to create a culture with cybersecurity in mind. As I entered

the business world, I found that nearly every business executive I talked with was eager to discuss with me their information technology and concerns over how to secure their information. They found my information technology and cybersecurity experience was valuable to helping them protect their information and competitive advantage. Several of them even suggested that I write a book about cybersecurity. My second career as an information technology and cybersecurity consultant was born.

While it surprises many executives in the private/commercial sector, the Air Force already had given me an excellent foundation in business because in many respects it is managed much like a major corporation and, as a general officer, I rose to one of its senior executive positions. Nonetheless, before I left military service, I recognized that I needed to expand my knowledge of contemporary business practices, terminology, and procedures. I joined the Corporate Directors Group, a public company director education organization, where I earned my Professional Director certification and was introduced to Clint Allen, the group's president. Clint is a highly experienced senior executive and board member who has been a great source of knowledge and advice as I made the transition from the military. When I told him that I was thinking of writing this book, not only was he encouraging, but also he wanted to know when I'd get it done as he said he was so eager to read it. His enthusiasm and interest in educating executives on cybersecurity issues inspired me to invest in this writing effort. He was equally generous in volunteering to write the foreword.

While I had great credentials and experience in information technology and cybersecurity, I knew that I needed an expert in business to complement my technical skills. I did not have to look far and turned to my father, Dr. Joe Touhill, who, in addition to being a renowned technologist, is a highly successful CEO, board member, and senior executive. His experience in creating and managing companies, both large and small, was invaluable in filling any gaps in my resume. He has been a corporate officer for 41 years, 29 years of which he has been a CEO. Additionally, he has had extensive board and high-level committee experience. For example, he has been on the board of directors or a trustee of a hospital, a regional MRI facility, a publicly traded bank where he was chairman for several years, a municipal authority, and a major engineering certification organization. He also served on advisory committees for a leading technological university. In other words, he has been around and has an in-depth knowledge and understanding of what executives need and want.

As we did while writing our first book, *Commercialization of Innovative Technologies: Bringing Good Ideas to the Marketplace*, in this book we collaborated over long distances through the countless emails and phone calls, synchronizing our research, outlines, text, and edits. During the first writing effort, I was deployed to Iraq, Afghanistan, and throughout the Middle East for a year, so my father had to patiently wait for my contributions, which I worked on during my increasingly rare off-duty time. This time was different as we were able to talk several times during the day and exchange manuscripts in near real time, permitting us to partner extremely well. My dad's extensive business experience was critical as we focused on the business aspects of cybersecurity rather than jumping into the trap taken by others of being too enamored by the information technology itself. *Our position is that information technology is a tool used by businesses to create value and that cybersecurity is about risk management.*

As we prepared to write this book, we recognized that the Internet has become a powerful ecosystem teaming with data and a myriad of practical and very helpful applications. In fact, it is said that every day in today's so-called "Cyber Age" the human race generates more data than all recorded history before 2003. All that data is being mined to uncover your shopping habits, what web sites you tend to visit, with whom you associate, your recreational and political interests, where you like to travel, and how you spend your money. The Cyber Age has spawned a whole new industry just to collect, collate, and analyze "Big Data." However, "Big Data" equates to "Big Money" which in turn attracts people who seek to gain access to your information or may act in a manner that adversely affects your business.

Some people use terms like hackers and cyber terrorists to describe these people. We prefer to use a term commonly used by most cybersecurity professionals: *bad actors*. A wide variety of individuals can adversely affect your business using information technologies. Some act in a malevolent manner while others cause damage inadvertently. Successful cybersecurity programs protect against all threats, providing businesses and individuals the resiliency to maintain the confidentiality, integrity, and availability of their information. Therefore, when we refer to bad actors, we refer to anyone who is acting in a manner adverse to your business and its information.

Our analysis led us to conclude that your information, especially that which is proprietary, is the lifeblood of your business and your information technology systems have become the circulatory system that keeps your business healthy and vibrant. Regrettably, the same information technology that delivers competitive advantage to businesses also presents serious threats if not managed closely and well. Your information needs to be secure for your business to survive. Unfortunately, we find many executives view cybersecurity as an unnecessary cost and a topic solely for their information technology staffs. We believe this is a mistake.

Think about your business.

- As an executive, how long can you do your job without access to information technology?[1] How long can your business survive without a trusted, stable, and reliable information technology system?[2]
- Can your financial team operate without access to sensitive information? What if their information is tainted?
- How about your production facilities? What do they do if the electricity shuts off? Can they continue to operate? What if their supervisory control and data systems, which are the control units that operate machinery, are corrupted and the machines don't work properly?

[1] For purposes of this book, we define "executive" thusly: an executive is someone who has administrative and managerial responsibility for a shareholder-owned business, or a publicly-owned organization committed to the protection and promotion of the health, welfare, and safety of its constituents.

[2] Also for purposes of this book, we will use the word "business" in its broadest sense. "Business" can mean any operation or organization falling under the purview of an executive as previously defined above.

- What if your competitors have access to all of your company research? In addition to the risk that others may use your plans to field your desired product and bring it to market before you, others may decide maliciously to poison your information and sabotage your plans so you deliver a flawed product to market instead.
- What if your shareholders and potential investors lose confidence in your business because of your company's inability to safeguard its information and systems?

For many years, information technology was the always valued, often derided, and frequently misunderstood part of a company's business. Corporate executives appreciated the ability of information technology to enhance business operations through its capacity to manipulate information with ever-increasing speed and precision. Yet, for many corporate executives, information technology was the realm of the "geeks"; those technical wizards who appear more enamored with the technology than the bottom-line that drives the business. Indeed, for most businesses, information technology has been considered an important supporting arm of the business, but rarely a key component.

Perhaps because information technology has been considered a supporting role to the business, many corporate executives delegated much of the oversight and many of the decisions regarding information technology to their information technology department heads. However, as businesses became more and more dependent on information technology, the stakes of a failure involving information and the information system magnified in importance to where a single failure could be an existential event that could doom a company. The stakes are so high that the security of the company can no longer be entrusted to the "geeks" in the server room. That is why we believe our book will fill the need of executives to understand fully the cybersecurity risks they will encounter within the context of management and mitigation.

We contend that cybersecurity is about risk management. It is about protecting shareholders and their business, maintaining competitive advantage, and protecting assets. It is not just about computer technology. Rather, it is a multidisciplinary approach to managing risk; a principal concern of executives.

If you are looking for a book that will make you a technical expert, we certainly can help there, yet most corporate executives don't need to be a technical expert to make good decisions. They need to understand their business and its needs. They especially need to understand the risks their business faces and determine best courses of action to take to mitigate risks. They need to understand the value of their information as much as the value of their inventory and manage both with effectiveness, efficiency, and security. They need to know how to build and sustain great teams composed of the right talent and motivation to best posture the company for success. They need to lead people to perform at peak levels and continuously seek to innovate and improve the business. They need to be able to create an environment where they can gather the right information from the right sources at the right time to make the right decisions.

This book will help and guide you to do that.

Remember, this book will not make you a cybersecurity expert. Instead, we seek to make you *Cyber-Aware* and prepared to make the key decisions to make your business better, and effectively manage the risks inherent in the Cyber Age.

As you read this book, please carefully consider the following:

Cybersecurity is not just a technical issue, it is a business imperative.

While we have done our best to eliminate redundancies, you may see some information that may appear more than once in the book. There are several reasons that this information may be presented in multiple areas. Firstly, because some concepts, such as cybersecurity insurance, transcend many of the key themes of the book, they are discussed within the context of the appropriate sections. Secondly, we recognize that many readers will use the content of the book as reference material as they adjust their cybersecurity programs. We anticipate they may use individual chapters to address pressing concerns. As such, we have included all relevant subject matter that enables the chapters to serve as stand-alone references. Thirdly, there are some items of interest that are so important that they bear repeating for emphasis.

We hope that you find our work informative and valuable. We recognize that cybersecurity is a multi-disciplinary subject, replete with its own idioms, acronyms, and phrases. As such, we include a glossary of terms and an appendix to help add clarity to some of the concepts discussed in the text.[3] Unless attributed to other sources, the work, and any errors we and our editors did not catch in the many reviews leading to publication, are ours and ours alone.

We look forward to hearing your feedback. Please feel free to write us at cyber@touhill.com.

Gregory J. Touhill
Jamison, Pennsylvania
December 2013

[3] These will help you to communicate with the "computer aficionados" without being snowed.

ACKNOWLEDGMENTS

We would like to thank our reviewers, including Aaron Call, Chief Information Security Officer for IO.com; Sean Kern of the National Defense University's Cybersecurity and Information Technology cadre; Sekhar Prabhakar, founder and Chief Executive Officer of CEdge Software Consultants; and Jack Zaloudek, Program Director for Information Management and Cybersecurity at Washington University in St. Louis. Their insightful comments, suggestions, and encouragement were invaluable and made this a better book. Many thanks for your sage advice and investment in your precious time.

We also would like to thank Clint Allen, who contributed the foreword for this book. His enthusiasm and interest in educating executives on cybersecurity issues inspired us to invest in this writing effort. Thank you for your encouragement and the foreword's kind words.

Kate McKay of STM Publishing Services was instrumental in launching this book. She provided great advice throughout the publication process. Thank you for your assistance and counsel.

Finally, we also would like to thank Andrew M. Touhill for his contributions to this book. He was instrumental in assisting us with research, editing, and contributed the glossary of terms. His crisp edits and critical analysis helped us reduce and (hopefully) avoid ramblings, worthless opinions, and errors. Thank you Drew for your great work. With your help, this truly is a father and son and grandson effort.

CONTENTS