THE CODE OF HONOR

EMBRACING **ETHICS** IN **CYBERSECURITY**

PAUL J. MAURER AND ED SKOUDIS

The Code of Honor

The Code of Honor

Embracing Ethics in Cybersecurity

Paul J. Maurer
Ed Skoudis

WILEY

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

Published simultaneously in Canada and the United Kingdom.

ISBNs: 9781394275861 (hardback), 9781394275878 (ePDF), 9781394275885 (ePub)

Library of Congress Control Number: 2024935048

Cover image: © DNY59/Getty Images

Cover design: Wiley

Contents

Introduction: "Like Your Hair Is On Fire"

"*The Chinese use two brush strokes to write the word 'crisis.' One brush stroke stands for danger, the other for opportunity. In a crisis, be aware of the danger—but recognize the opportunity.*"

– President John F. Kennedy

Dear Reader,

You may not realize it yet, but we would like to humbly suggest to you that, metaphorically speaking, your hair is on fire—or at least you should be responding to the current state of the cybersecurity industry and its impact on the world with an alarmed sense of immediate concern. We assume you have opened these pages because you are a leader with cybersecurity responsibilities, a cybersecurity practitioner, or a student preparing for a role in this industry. Or, although you may have another role, perhaps cybersecurity is quickly becoming a critical concern in your daily work. Regardless of what brought you here, we are quite sure the challenges we address in these pages are more far-reaching and urgent than you may even realize right now.

The Code of Honor is the result of a journey we began several years ago to address an expanding ethical vacuum in our industry, where critical decisions are often made without regard to their ethical implications. At the same time, the weight and financial impact of our decision-making is rapidly increasing. As you will learn in the coming pages, the crossroads of cybersecurity and ethics aren't some philosophical "pie in the sky" discussion. Cybersecurity professionals hold a great deal of power and enormous levels of responsibility in the workplace and the broader economy. It is a high-pressure, fast-paced, and exciting field where ethical decision-making can make the difference between success and abject disaster, not only for your career but for your organization, customers, or constituents, and perhaps far beyond. The topics we explore in this book are integral to the daily operations of nearly every industry and are essential to the very stability of our modern world.

As the cybersecurity industry is changing at light speed, we must truly respond to the emergent ethical challenges with a level of "hair on fire" determination and precision. Our offering in *The Code of Honor* is a systematic and thoughtfully constructed program for building best practices regarding ethics in decision-making in the tech industry with a specific focus on cybersecurity. This book presents a concise, carefully designed, and timeless set of ethics that will engage everyone from C-suite leaders who work on the periphery of the cyber world to the most seasoned cybersecurity professionals and everyone in between.

We thought it best to begin by answering a few questions that will help you maximize your experience and effectively engage with the pages ahead.

How Should You Read This Book?

To craft this book, we spent a year thinking through and documenting various ethical dilemmas we've seen in the cybersecurity industry in our several decades, worth of experience as practitioners, leaders, and educators. From those discussions, we spent a great deal of time wrestling with each other to formulate a clear, short, valuable Cybersecurity Code of Honor to provide a framework for ethical decision-making for real-world cybersecurity leaders and practitioners. We then refined the code of honor by gathering input from dozens of friends and colleagues throughout the cybersecurity industry. We wrote this book to provide an in-depth tool that expands on the ideas of that code of honor, which is in Appendix A of the book.

The chapters are written in a specific sequence and are meant to be read in order. Every chapter supports a tenant of the code of honor. Each chapter is full of engaging stories, industry-specific illustrations, and practical, real-world applications designed to teach the essential foundational concepts behind this widely accepted code of ethics that is becoming an industry standard. The book is designed to be read individually or in a team or corporate setting. We highly encourage you to work through the lessons of each chapter with other professionals who can help you learn and grow.

Why Are There Two Authors but Only One Voice?

While "we" (Paul and Ed) contributed equally significantly to this product, we did not want to confuse the reader by writing with two different voices throughout these chapters. We chose to approach the important concepts in this book with one consistent voice to make the reading experience straightforward and ensure the content is front and center. On rare occasions, we will refer to specific experiences of Paul or Ed by name, but we will generally refer to our common and shared experiences as "we."

How Should You Approach the Critical Applications Case Studies?

Every chapter closes with a case study called "Critical Applications," designed to help you utilize the essential skills and concepts you have learned in that chapter and those before it. These case studies are meant to challenge you to consider the ethical implications of the choices we must make in our professional lives. While the names, companies, and details of these stories have been changed, they are based on real-world examples from across our industry that we have observed or advised our colleagues about.

Each case study can be used to facilitate lively small group discussion and debate in classrooms, corporate sessions, training exercises, or seminar settings. Not only are these studies powerful teaching tools for students and industry professionals, but they can also assist C-suite leaders

who need to better understand the scope of cybersecurity challenges, define their liability and responsibility, and think strategically about budget and hiring personnel necessary to protect their organizations. As you'll see later in this book, we think of cybersecurity ethical practices rather like muscles—the more you work them out, the stronger you'll get. Please use these "Critical Applications" scenarios at the end of each chapter as an exercise regimen for yourself and your team.

How Should You Use the Cybersecurity Code of Honor?

Our book closes with the Cybersecurity Code of Honor that is a singular universal code of ethics currently being adopted by cybersecurity practitioners and leaders around the world. The Cybersecurity Code of Honor was born out of research, interviews, and conversations with the world's leading experts in our field and can be applied to a wide range of ethical decisions you may confront in the cybersecurity industry. We recognize that various cybersecurity certification bodies and other related organizations have developed oaths and codes of honor for holders of those certs. We applaud their efforts and have reviewed each of them carefully as we formulated the Cybersecurity Code of Honor. We aim to build something applicable beyond individual cybersecurity certifications and even individual job roles—to create something useful as a framework throughout the cybersecurity world.

We have been humbled to witness the immediate impact the Cybersecurity Code of Honor has made across the industry. It is our hope it will also be adopted by you, your organization, or your school to help provide a singular lens through which best ethical practices in our field may be determined.

A Challenge to Make the World a Better Place

We have done our best to present the lessons about this system of cybersecurity ethics in a way that will engage everyone. It is our sincerest hope that this book can function as a comprehensive learning tool for students, cybersecurity professionals, and business leaders who have been desperately seeking a widely agreed-upon set of principles to guide their professional and personal ethical decisions. We believe that this book (and its corresponding code of honor) can be a catalyst for your career advancement, help enhance the security of your organization, and even fast-track your leadership teams' success. Ultimately, we challenge you to embrace the ethical standards and practices in this book for the world's greater good.

Sincerely,
Paul and Ed

CHAPTER

1

One Code to Rule Them All?

"The most important human endeavor is the striving for morality in our actions. Our inner balance and even our very existence depend on it. Only morality in our actions can give beauty and dignity to life."

– Albert Einstein

"The time is always right to do what is right."

– Dr. Martin Luther King Jr.

Cybercrime and cybersecurity should be among the foremost concerns of every industry, service, and every civic interest. Why? Cyber technology effectively runs the modern world from banking to healthcare, retail to

sanitation, and governance to modern warfare. Cybersecurity practitioners wield great power, are under intense pressure, work in a culture that is changing at warp speed, and often have profound responsibilities. The fast-paced environment of our industry can be a breeding ground for mistakes, misused authority, and even intentionally abused power. The unprecedented speed of innovation in the 21st century has left us without a clear system of ethics for this great economic and security threat of our age. We would be remiss if we didn't begin by sharing some statistics with you reflecting how cybersecurity and cybercrime impact the world as we write this book. While the numbers may read like an archeological time capsule by the time you read them, it is our way of pulling the "fire alarm" in the midst of an unfolding global crisis.

- According to research, an estimated 53.35 million U.S. citizens were affected by cybercrime just in the first half of 2022.[1]
- Ransomware attacks in 2022 cost global businesses an estimated $20 billion. As cybercriminals are becoming rapidly more advanced and targeting businesses that can pay higher ransom fees, experts believe that $20 billion will balloon to more than $30 billion just in the next year.[2]
- The average cost to an individual organization that has suffered a data breach in 2022 was $4.35 million.[3]
- This cyber arms race by the world's bad actors is also leading to increased security spending. According to a recent report, cybersecurity spending is expected to reach $172 billion by the close of 2022.

Every time we open our browser or news app to check the latest research, the proverbial fire presents its rapid spread in the news cycle of the day. Today's headline points out that "Crypto-hackers steal $3 Billion This Year," while another proclaims, "2025 will be the biggest year for Digital Heists!" Cyberattackers, through ransomware and other insidious schemes, have caused massive damage to banks, hospitals, schools, critical infrastructures, and more. And it seems to be only getting worse.

In Case You Are Wondering Why You Should Care

For those of you on the periphery of our industry or simply new to the job, it is important to know what you are risking if you choose to ignore this cybersecurity crisis (no matter how big or small your organization is). Even today, there are too many leaders who still don't fully understand the scope of impact that cyberattacks can have in our world. Here are just a few of the effects that cyberattacks can inflict upon you and your business:

- You may suffer damage to your computer systems. When malicious computer attackers target your business, they can damage or destroy data on those systems, and the cost to repair or rebuild them can be extremely high.
- Attackers can steal sensitive data from your business such as consumer information or even trade secrets, which can have a dramatic impact on your company's reputation and financial standing.

- A cyberattack can interrupt the services that your business provides and cause you to lose money, customers, and time.
- You can face legal consequences from a cyberattack. You and your business can be held accountable for damages to consumers.
- Being hit by a cyberattack can ruin your brand and your reputation, making it harder to attract and keep customers. It can negatively impact your business long after the immediate damages of an attack have been corrected.
- Finally, there is always cybercrime and identify theft's impact on real people. If cybercriminals steal consumer information from your systems, those customers will be put at risk, affecting your consumer retention, impacting stakeholder trust, and resulting in legal issues. Even more concerning are cyberattacks that break into healthcare systems, transportation, or other critical infrastructures, perhaps causing severe damage to life and limb.

Cybersecurity is no longer an issue that you can ignore. We would argue that your success as a business, a professional, and a leader could be tied to how seriously you address this problem. Experts are currently predicting that cybercrime will eclipse the gross domestic product (GDP) of the world's largest economies in the near future. While it may sound fantastical, we are here to tell you it is a stark and unnerving reality.

It's as if we are trying to put out this worldwide four-alarm fire with a water gun. Every day in the cybersecurity industry, we are fighting for the resources, staffing, education, and ethical framework to keep attackers at bay. While the global workforce in our industry stands at around 4.7 million workers, it is predicted that there will be an astounding 3.4 million cybersecurity worker *shortage* worldwide within a few years. Currently, we need 600,000 positions filled in the United States *alone*. As we struggle to keep up with the demand to fill positions, we also must be vigilant to find good candidates of reputable character who are committed to serving the greater good. If we fill open positions with people who lack the ethical framework and character to put it into real-world practice, we'll only make the problem worse—*much* worse.

This is a problem that touches the day-to-day operations of nearly every public and private entity. Yes, by the time you read these words, the numbers will be outdated, and unfortunately, the challenges will be way bigger. There is simply no evidence that these trends will reverse course in the near future. Technology will continue to dominate the business landscape and become ever more a part of all of life. We are not going to go backward from our online, on-demand, virtual world any time soon. And of course, we are not likely going to become less technologically advanced or cyber-integrated. Attackers are not going to give up. Cybercrime is too lucrative an industry.

Is there a way to stop or at least slow down the trend? Is there any hope?

Do We Need Ethics in Cybersecurity?

Yes. An ethical standard in cybersecurity is fundamental to its future. If you work in cybersecurity, your day-to-day job can feel like fighting fires. Your day can go from 0 to 100 with one email or intrusion alert, and you will often find yourself in high-stress situations that have serious consequences on your company and its customers or stakeholders. One of the realities of working in fast-paced, pressure-filled environments is the ever-present temptation to cut corners or take shortcuts. There is tremendous pressure on both practitioners and leadership in our line of work to make the *right* decisions because those choices can have far-reaching impacts on numerous individuals. We can better illustrate a few of the common ethical challenges with a story about two professionals who have been recently affected by cybercrime.

Sarah is the CEO of a midsize medical device engineering company that has been hit recently with a ransomware attack. It isn't long before her small security team identifies the entry point through a third-party IT service provider that is also used by several of her fiercest competitors. As her cybersecurity team rolls into response and investigation, the questions mount: Is the attacker truly connected to the service company, or is it just set up to appear that way? Does the CEO have a responsibility to alert her competitors of the potential breach? Do competitors have an advantage over Sarah during the downtime caused by the attack? Her firm designs medical devices for several healthcare organizations. Are there legal obligations to alert those entities of the attack? Do they have to alert their parent company, who