ANDREW GORECKI

CYBER BREACH RESPONSE THAT ACTUALLY WORKS

ORGANIZATIONAL APPROACH TO MANAGING RESIDUAL RISK

WILEY

Cyber Breach Response That Actually Works

Cyber Breach Response That Actually Works

Organizational Approach to Managing Residual Risk

Andrew Gorecki

WILEY

Published simultaneously in Canada

ISBN: 978-1-119-67932-5
ISBN: 978-1-119-67935-6 (ebk)
ISBN: 978-1-119-67931-8 (ebk)

Manufactured in the United States of America

Limit of Liability/Disclaimer of Warranty: The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Web site is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or website may provide or recommendations it may make. Further, readers should be aware that Internet websites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services please contact our Customer Care Department within the United States at (877) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at booksupport.wiley.com. For more information about Wiley products, visit www.wiley.com.

Library of Congress Control Number: 2020934806

The author has written this book as an individual, not as an IBM employee, and the writings in this book are his own and do not necessarily represent IBM's positions, strategies, or opinions. IBM does not sponsor or endorse this book.

About the Author

Andrew Gorecki is a cybersecurity professional with experience across various information technology and cybersecurity disciplines, including network and security engineering, data management, cybersecurity operations, and incident response.

Andrew has provided cybersecurity consulting services across various industry sectors in the United States, the United Kingdom, and other European countries. Andrew developed a strong interest in incident response while working as a cybersecurity consultant in the U.K. Following his interest, Andrew joined the X-Force Incident Response and Intelligence Services (X-Force IRIS) competency of IBM Security in the U.S. to work in incident response full-time.

As of this writing, Andrew manages a team of incident response consultants within X-Force IRIS. In addition to his managerial responsibilities, Andrew leads investigations into large-scale breaches for Fortune 500 organizations and consults on building and optimizing incident response programs.

Andrew takes a holistic approach to incident response by focusing on the end-to-end business process, facilitating cross-functional engagements, and helping clients build capabilities based on sound risk management principles.

About the Technical Editors

Adam Brand has spent most of his career focused on helping organizations improve their security programs. Over the years, he has also helped untangle complex malware found in breaches, led breach response efforts, and identified unknown attackers through threat hunting engagements. At the time of writing, Adam is a Managing Director with a large consulting firm in the cybersecurity strategy and governance group.

Adam has worked with dozens of clients throughout his career on both proactive and reactive cybersecurity projects. While he can and often does delve into the technical details, his key to success is often helping position technical challenges or information in ways nontechnical executives can understand in order to take action.

An active public speaker and security community participant, Adam has spoken at dozens of industry conferences over the years. Furthermore, Adam has developed an active interest in skillsets focused on medical device security, and currently works with both device manufacturers and healthcare providers to help improve patient safety.

Rhodes Gregory Taylor-Broun is a security operations center and computer incident response professional with decades of hands-on experience and several industry certifications. Greg holds the SANS Advanced Penetration Testing and Exploit Writing (GXPN), SANS Certified Intrusion Analyst (GCIA), and Certified Information Systems Security Professional (CISSP) certifications. He has worked on a wide variety of information security incidents and high-profile data breaches, and he brings real-world, hands-on experience to bear when working in the field. Greg calls San Diego home with his wife and daughter, where he runs a meetup for digital forensicators and incident responders, sharing his knowledge freely with the community.

Acknowledgments

Writing this book has been both hard and rewarding. I am grateful to everyone who contributed to this book and made it possible. I want to thank my colleagues and friends for their invaluable contributions, especially Kurt Rohrbacher, Warren Stramiello, Matthew Sullivan, Pavle Culum, Markus Schober, Phil Harrold, Chris Sperry, Matt DeFir, John Dwyer, and David Porco.

I also want to thank Himanshu Wickramasinghe, who introduced me to cybersecurity, mentored me over the last several years, and guided me on the consulting path.

A very special thanks to Adam Brand and Greg Taylor for reviewing the book and providing valuable suggestions, as well as the Wiley team, especially Gary Schwartz and Jim Minatel.

Finally, this book would not be possible without the support of my wife Marie. I want to thank her for support, encouragement, and sacrifices that allowed me to make this book a reality!

— Andrew Gorecki

Contents at a Glance

Contents

Foreword

It is often said that air traffic controllers have the most stressful job in the world. Being able to coordinate the safe takeoff and landing of dozens of commercial airliners, each carrying hundreds of passengers per day, all while dealing with a myriad of externalities, including the weather, ground control, controlled and noncontrolled airspaces, regulators like the FAA, flight crews, and airport operators, must seem like an impossible task. That is why in the United States, air traffic controllers must undergo a series of background checks and psychological exams, a rigorous training program, and certification testing, all before they ever set foot in a control tower.

If air traffic controllers have the most stressful job, cybersecurity incident responders might be a close second. As an incident responder, you're responsible for performing technical forensic investigations of highly complex environments as well as ensuring that the response team is maintaining its composure and working toward a common goal of mapping the full extent of attacker activity and eliminating their access to the network. It requires producing answers to questions that do not have an easy answer. It demands a deep level of technical knowledge in addition to a militaristic ability to lead a team toward a common objective. A responder must also consider the potential ramifications of a breach that may only surface much further down the line and take measures to protect the organization involved in the scenario, however improbable, that events unfold in such a way. It is part art form, part science.

When I interview people for incident responder positions, I often ask candidates to describe a situation where they were able to thrive under adverse conditions, because they will absolutely find themselves in an even more difficult position as an incident responder. During a cybersecurity breach, stress levels are at their peak, people fear for their jobs and for the survival of their business, and in some circumstances, even fear for the physical safety of the general public. Attacks against critical infrastructure are not unheard of and seem to become even more prevalent as time goes on. In addition to the high-stress environment, financial budgets and higher-level business objectives undermine every step of the process. If you're not prepared to have the CEO of a Fortune 500 company channel his or her anger and frustration by yelling at you, you might not be cut out for the job. It is for these reasons that most incident responders do not stay in the field for very long. They move on to other roles and apply their experience in a proactive way to prevent organizations from experiencing their worst day. A responder with 10 years of experience is considered a relic.

All of this helps to explain why I always believed that there was no manual for how to do incident response, no textbook you could give to an inexperienced responder that tells them everything they need to know to be able to respond to incidents. The cybersecurity industry does not have a standard training curriculum and testing process to admit new entrants into the field, like the aviation industry has for air traffic controllers. Incident response is one of those things that you can truly learn only by doing, and you can only succeed after you have failed several times. It is baptism by fire, and the anointed need no other teacher.

That's why this book is so ambitious—it is an attempt to bring order to an inherently chaotic process. Over the past several years that Andrew and I have worked together, I have learned that he has a knack for reading complex situations, digesting critical information, and building structure around the process that allows various elements to operate more efficiently. Most responders get so "into the weeds" in trying to solve the immediate problem that they don't have either the time or the ability to step back and consider the bigger picture. Andrew has taken his experience and engineered a framework for doing incident response more effectively. Take his advice and run with it—and if even one paragraph of this book helps your organization avoid the worst-case scenario in a cybersecurity incident, you'll know who to thank.

—Kurt Rohrbacher

Introduction

Cybersecurity has taken the media by storm in recent years, and cyberattacks are now headline news, from destructive ransomware attacks that impact manufacturing plants to data breaches that involve Fortune 500 companies.

Organizations have experienced notable disruptive cyberattacks in recent years. A ransomware attack on a global shipping company, A. P. Møller – Mærsk, wiped out their entire IT infrastructure across 600 sites in 130 countries. As a result of the cyberattack, Maersk had to rebuild their entire infrastructure in a heroic effort over 10 days. The total losses are estimated to have cost Mærsk up to $300 million.[1]

The National Health Service (NHS) in the U.K. incurred a cost of £92 million ($120 million) as a result of the WannaCry ransomware outbreak in June 2017. The cyberattack also resulted in the cancellation of 19,000 appointments.[2]

There are also numerous examples of data breaches resulting in significant financial losses, damage to brand reputation, and fines imposed by regulators. One of the most significant data breaches in recent years was the Equifax breach that led to the disclosure of personal data of 145 million U.S. consumers, including Social Security numbers, credit card information, addresses, and birth dates.[3]

As businesses and other organizations increase their digital footprint and online presence, the need to secure their information assets is more critical than ever before. The Ponemon Institute's Cost of a Data Breach Study (2019) determined an average cost of a data breach across various industries was $3.92 million.[4] Furthermore, the World Economic Forum identifies cyberattacks as the fifth top risk in terms of likelihood and the seventh top risk in terms of impact.[5]

Many organizations are increasingly concerned about their exposure to cyberattacks. Businesses exist to generate value for their shareholders, and cyberattacks ultimately impact the bottom line. Even nonprofit organizations can suffer severe financial consequences as the result of a cyberattack.

In my consulting engagements, I have observed that cyber risk has become a frequent topic of board-level conversations, and enterprises increasingly perceive exposure to cyberattacks as a business issue. To address cyber risk, organizations build information security programs to protect critical assets and reduce risk to an acceptable level. As residual risk is inevitable, incident response is a critical control in the risk management process that allows organizations to address the aftermath of an incident, reduce the impact of a cyberattack, and restore the affected assets to a fully operational state.

An effective cyber breach response program is like a fire department. Organizations design a set of capabilities based on their needs and requirements, build an incident response team, acquire the necessary technology, and operationalize those capabilities. When the inevitable happens, the affected stakeholders can call the fire department, who might be able to extinguish the fire before the real damage is done, or at least reduce the amount of damage.

The benefits of developing an effective cyber breach response program include the following:

Minimize the impact of cyberattacks. The sooner an organization detects and responds to a cyberattack, the lesser the impact to business operations, brand reputation, and financial standing.

Decrease the cost of response. Effective incident response helps organizations decrease the overall attacker dwell time on their network, leading to a decreased cost of response. *Dwell time* is the time a threat actor remains on your network from the initial compromise to eradication.

Prevent enterprisewide incidents. Undetected intrusions can swiftly progress into enterprisewide incidents within weeks. The response effort is usually proportional to the time an attacker dwells on the network. Furthermore, enterprisewide incidents usually require disruptive remediation and can impact the bottom line of the victim organization.

Improve security posture. Incident response is an iterative process, with evaluation being one of its core components. The lessons-learned outcome can help organizations improve their policies, controls, and the incident response process itself. This approach ultimately leads to an enhanced security posture and cyber resilience.

Ensure compliance. Specific regulations and standards require organizations to have incident response capabilities, including an incident response plan.

Enhance service quality. Information technology is a business enabler, and its mission is to provide value to the business. The role of information security, on the other hand, is to protect that value. By building incident response capabilities, organizations can minimize the impact of cyberattacks on their services and core business functions, leading to overall better service quality to internal and external clients.

Who Should Read This Book

I have written this book for anyone who is looking for an authoritative source of information on building and managing a cyber breach response program, including senior cybersecurity managers and chief information security officers (CISOs).

This book is also a valuable source of information for executive leaders, business and technology professionals, legal counsel, risk managers, and other stakeholders who have an active interest in cyber breach response in their organizations or who are planning to transition into a career in this field.

In this book, I explain cyber breach response concepts in a clear, concise, and technology-agnostic language that anyone with a grasp of fundamental cybersecurity and risk management concepts can understand.

How This Book Is Organized

I organized this book into six chapters that provide a comprehensive discussion of various topics relating to cyber breach response. I designed the book to serve both as a guide for building cyber breach response programs from scratch and as a reference guide for organizations that strive to grow and evolve their capabilities. Although the book consists of progressive chapters, each chapter provides stand-alone content that the reader can reference. Where appropriate, I also direct the reader to other chapters for specific information.

Chapter 1: Understanding the Bigger Picture This chapter defines cyber breach response and discusses foundational concepts. It starts with a brief overview of the threat landscape and discusses drivers for cyber breach response and their role within an overall cybersecurity program. A discussion of the critical building blocks of a sound cyber breach response strategy concludes this chapter.

Chapter 2: Building a Cybersecurity Incident Response Team Chapter 2 discusses the various considerations that organizations need to take into account when building an incident response team. The topics in this chapter include incident response competencies and functions, team models, skills, the hiring and retaining of talent, and cross-functional team development. A brief discussion on outsourcing considerations concludes this chapter.

Chapter 3: Technology Considerations in Cyber Breach Investigations This chapter focuses on building the technical capabilities necessary to support incident response investigations. The chapter starts with a discussion on general considerations for sourcing incident response technology. Then it progresses into a discussion on data acquisition in on-premises and virtualized environments, including cloud computing. The final two sections discuss sources of network data and log management solutions.

Chapter 4: Crafting an Incident Response Plan Chapter 4 starts with a discussion on the incident response lifecycle. Then it dives into various incident management concepts before concluding with a discussion on post-incident activities and continual improvement.

Chapter 5: Investigating and Remediating Cyber Breaches This chapter takes an in-depth look at a methodology that incident responders employ during investigations. It discusses topics such as digital forensics and data analysis, cyber threat intelligence, malware analysis, threat hunting, and reporting. This chapter also discusses evidence types before concluding with a discussion on remediating cyber breaches.

Chapter 6: Legal and Regulatory Considerations in Cyber Breach Response Chapter 6 discusses how the legal and regulatory landscape impacts cyber breach investigations. It goes in-depth