

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**

Copyright © 2020 by John Wiley & Sons, Inc., Indianapolis, Indiana

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

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at [www.wiley.com/go/permissions](http://www.wiley.com/go/permissions).

**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](http://booksupport.wiley.com). For more information about Wiley products, visit [www.wiley.com](http://www.wiley.com).

**Library of Congress Control Number:** 2020934806

**Trademarks:** Wiley and the Wiley logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries, and may not be used without written permission. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

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



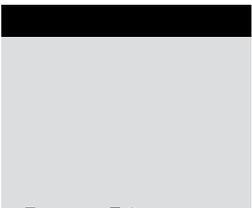
**Andrew Gorecki** is a cybersecurity professional with experience across various information technology and cybersecurity disciplines, including network and security engineering, data management, cybersecurity operations, and incident response.

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

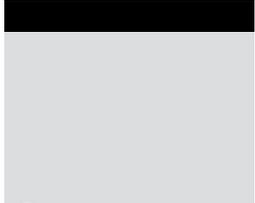




# Contents at a Glance

Foreword		xxiii
Introduction		xxv
<b>Chapter 1</b>	<b>Understanding the Bigger Picture</b>	<b>1</b>
<b>Chapter 2</b>	<b>Building a Cybersecurity Incident Response Team</b>	<b>51</b>
<b>Chapter 3</b>	<b>Technology Considerations in Cyber Breach Investigations</b>	<b>97</b>
<b>Chapter 4</b>	<b>Crafting an Incident Response Plan</b>	<b>143</b>
<b>Chapter 5</b>	<b>Investigating and Remediating Cyber Breaches</b>	<b>195</b>
<b>Chapter 6</b>	<b>Legal and Regulatory Considerations in Cyber Breach Response</b>	<b>243</b>
Index		281





# Contents

<b>Foreword</b>	<b>xxiii</b>
<b>Introduction</b>	<b>xxv</b>
<b>Chapter 1 Understanding the Bigger Picture</b>	<b>1</b>
Evolving Threat Landscape	2
Identifying Threat Actors	2
Cyberattack Lifecycle	4
Cyberattack Preparation Framework	5
Cyberattack Execution Framework	6
Defining Cyber Breach Response	8
Events, Alerts, Observations, Incidents, and Breaches	9
Events	9
Alerts	9
Observations	10
Incidents	10
Breaches	11
What Is Cyber Breach Response?	12
Identifying Drivers for Cyber Breach Response	13
Risk Management	13
Conducting Risk Management	13
Risk Assessment Process	14
Managing Residual Risk	17
Cyber Threat Intelligence	18
What Is Cyber Threat Intelligence?	18
Importance of Cyber Threat Intelligence	19
Laws and Regulations	20

- Compliance Considerations 20
- Compliance Requirements for Cyber Breach Response 21
- Changing Business Objectives 22
- Incorporating Cyber Breach Response into a Cybersecurity Program 23
  - Strategic Planning 23
  - Designing a Program 24
  - Implementing Program Components 25
  - Program Operations 26
  - Continual Improvement 27
- Strategy Development 27
  - Strategic Assessment 28
    - Gap Analysis 28
    - Maturity Assessment 30
  - Strategy Definition 32
    - Vision and Mission Statement 32
    - Goals and Objectives 33
    - Establishing Requirements 33
    - Defining a Target Operating Model 35
    - Developing a Business Case and Executive Alignment 35
  - Strategy Execution 37
    - Enacting an Incident Response Policy 37
    - Assigning an Incident Response Team 38
    - Creating an Incident Response Plan 38
    - Documenting Legal Requirements 38
- Roadmap Development 39
- Governance 40
  - Establishing Policies 40
    - Enterprise Security Policy 41
    - Issue-Specific Policies 41
  - Identifying Key Stakeholders 42
    - Executive Leadership 42
    - Project Steering Committee 42
    - Chief Information Security Officer 43
    - Stakeholders with Interest in Cyber Breach Response 43
  - Business Alignment 44
  - Continual Improvement 44
    - Necessity to Determine if the Program Is Effective 45
    - Changing Threat Landscape 45
    - Changing Business Objectives 45
- Summary 46
- Notes 47

<b>Chapter 2</b>	<b>Building a Cybersecurity Incident Response Team</b>	<b>51</b>
	Defining a CSIRT	51
	CSIRT History	52
	The Role of a CSIRT in the Enterprise	52
	Defining Incident Response Competencies and Functions	55
	Proactive Functions	55
	Developing and Maintaining Procedures	56
	Conducting Incident Response Exercises	56
	Assisting with Vulnerability Identification	57
	Deploying, Developing, and Tuning Tools	58
	Implementing Lessons Learned	59
	Reactive Functions	59
	Digital Forensics and Incident Response	59
	Cyber Threat Intelligence	60
	Malware Analysis	60
	Incident Management	61
	Creating an Incident Response Team	61
	Creating an Incident Response Mission Statement	62
	Choosing a Team Model	62
	Centralized Team Model	63
	Distributed Team Model	64
	Hybrid Team Model	65
	An Integrated Team	66
	Organizing an Incident Response Team	66
	Tiered Model	66
	Competency Model	68
	Hiring and Training Personnel	69
	Technical Skills	69
	Soft Skills	71
	Pros and Cons of Security Certifications	72
	Conducting Effective Interviews	73
	Retaining Incident Response Talent	74
	Establishing Authority	75
	Full Authority	75
	Shared Authority	76
	Indirect Authority	76
	No Authority	76
	Introducing an Incident Response Team to the Enterprise	77
	Enacting a CSIRT	78
	Defining a Coordination Model	78
	Communication Flow	80
	Incident Officer	80
	Incident Manager	81

- Assigning Roles and Responsibilities 82
  - Business Functions 82
    - Human Resources 82
    - Corporate Communications 83
    - Corporate Security 83
    - Finance 84
    - Other Business Functions 85
  - Legal and Compliance 85
    - Legal Counsel 85
    - Compliance Functions 86
  - Information Technology Functions 87
    - Technical Groups 87
    - Disaster Recovery 88
    - Outsourcing Partners and Vendors 89
  - Senior Management 89
- Working with Outsourcing Partners 90
  - Outsourcing Considerations 91
    - Proven Track Record of Success 91
    - Offered Services and Capabilities 91
    - Global Support 92
    - Skills and Experience 92
    - Outsourcing Costs and Pricing Models 92
  - Establishing Successful Relationships with Vendors 93
- Summary 94
- Notes 95

- Chapter 3 Technology Considerations in Cyber Breach Investigations 97**
  - Sourcing Technology 98
    - Comparing Commercial vs. Open Source Tools 98
      - Commercial Tools 98
      - Open Source Software 98
      - Other Considerations 99
    - Developing In-House Software Tools 100
    - Procuring Hardware 101
  - Acquiring Forensic Data 102
    - Forensic Acquisition 102
      - Order of Volatility 103
      - Disk Imaging 103
      - System Memory Acquisition 105
      - Tool Considerations 106
      - Forensic Acquisition Use Cases 107
    - Live Response 108
      - Live Response Considerations 109
      - Live Response Tools 109

Live Response Use Cases	112
Incident Response Investigations in Virtualized Environments	113
Traditional Virtualization	115
Cloud Computing	115
Forensic Acquisition	115
Log Management in Cloud Computing Environments	117
Leveraging Network Data in Investigations	118
Firewall Logs and Network Flows	118
Proxy Servers and Web Gateways	120
Full-Packet Capture	120
Identifying Forensic Evidence in Enterprise Technology Services	123
Domain Name System	123
Dynamic Host Configuration Protocol	125
Web Servers	125
Databases	126
Security Tools	127
Intrusion Detection and Prevention Systems	127
Web Application Firewalls	127
Data Loss Prevention Systems	128
Antivirus Software	128
Endpoint Detection and Response	129
Honeypots and Honeynets	129
Log Management	130
What Is Logging?	130
What Is Log Management?	132
Log Management Lifecycle	133
Collection and Storage	134
Agent-Based vs. Agentless Collection	134
Log Management Architectures	135
Managing Logs with a SIEM	137
What Is SIEM?	138
SIEM Considerations	139
Summary	140
Notes	141
<b>Chapter 4    Crafting an Incident Response Plan</b>	<b>143</b>
Incident Response Lifecycle	143
Preparing for an Incident	144
Detecting and Analyzing Incidents	145
Detection and Triage	146
Analyzing Incidents	146
Containment, Eradication, and Recovery	147
Containing a Breach	147

- Eradicating a Threat Actor 148
- Recovering Business Operations 149
- Post-Incident Activities 149
- Understanding Incident Management 150
  - Identifying Process Components 151
    - Defining a Process 151
    - Process Controls 153
    - Process Enablers 155
  - Process Interfaces 155
  - Roles and Responsibilities 158
  - Service Levels 159
- Incident Management Workflow 160
  - Sources of Incident Notifications 160
  - Incident Classification and Documentation 162
    - Incident Categorization 163
    - Severity Assignment 163
    - Capturing Incident Information 167
  - Incident Escalations 169
    - Hierarchical Escalations 169
    - Functional Escalation 169
  - Creating and Managing Tasks 169
  - Major Incidents 170
  - Incident Closure 171
- Crafting an Incident Response Playbook 171
  - Playbook Overview 171
  - Identifying Workflow Components 173
    - Detection 173
    - Analysis 174
    - Containment and Eradication 176
    - Recovery 176
    - Other Workflow Components 177
- Post-Incident Evaluation 177
  - Vulnerability Management 177
    - Purpose and Objectives 178
    - Vulnerability Management Lifecycle 178
    - Integrating Vulnerability Management and Risk Management 180
  - Lessons Learned 180
    - Lessons-Learned Process Components 181
    - Conducting a Lessons-Learned Meeting 183
- Continual Improvement 184
  - Continual Improvement Principles 184
    - The Deming Cycle 184
    - DIKW Hierarchy 185

The Seven-Step Improvement Process	187
Step 1: Define a Vision for Improvement	188
Step 2: Define Metrics	188
Step 3: Collect Data	189
Step 4: Process Data	190
Step 5: Analyze Information	191
Step 6: Assess Findings and Create Plan	191
Step 7: Implement the plan	192
Summary	192
Notes	193

<b>Chapter 5</b>	<b>Investigating and Remediating Cyber Breaches</b>	<b>195</b>
	Investigating Incidents	196
	Determine Objectives	197
	Acquire and Preserve Data	198
	Perform Analysis	200
	Contain and Eradicate	202
	Conducting Analysis	202
	Digital Forensics	203
	Digital Forensics Disciplines	203
	Timeline Analysis	205
	Other Considerations in Digital Forensics	206
	Cyber Threat Intelligence	207
	Cyber Threat Intelligence Lifecycle	208
	Identifying Attacker Activity with Cyber Threat Intelligence	209
	Categorizing Indicators	212
	Malware Analysis	214
	Classifying Malware	214
	Static Analysis	216
	Dynamic Analysis	217
	Malware Analysis and Cyber Threat Intelligence	217
	Threat Hunting	218
	Prerequisites to Threat Hunting	218
	Threat Hunting Lifecycle	219
	Reporting	221
	Evidence Types	223
	System Artifacts	223
	Persistent Artifacts	223
	Volatile Artifacts	225
	Network Artifacts	226
	Security Alerts	227
	Remediating Incidents	228
	Remediation Process	229

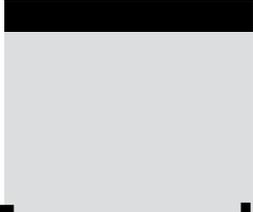
- Establishing a Remediation Team 230
  - Remediation Lead 231
  - Remediation Owner 232
- Remediation Planning 233
  - Business Considerations 233
  - Technology Considerations 234
  - Logistics 235
  - Assessing Readiness 235
  - Consequences of Alerting the Attacker 236
  - Developing an Execution Plan 237
- Containment and Eradication 238
  - Containment 238
  - Eradication 239
- Monitoring for Attacker Activity 240
- Summary 241
- Notes 242

**Chapter 6 Legal and Regulatory Considerations in Cyber Breach Response 243**

- Understanding Breaches from a Legal Perspective 244
  - Laws, Regulations, and Standards 244
    - United States 245
    - European Union 246
    - Standards 246
    - Materiality in Financial Disclosure 247
  - Cyber Attribution 248
    - Motive, Opportunity, Means 248
    - Attributing a Cyber Attack 249
  - Engaging Law Enforcement 251
  - Cyber Insurance 252
- Collecting Digital Evidence 252
  - What Is Digital Evidence? 253
  - Digital Evidence Lifecycle 253
    - Information Governance 254
    - Identification 254
    - Preservation 255
    - Collection 255
    - Processing 255
    - Reviewing 256
    - Analysis 256
    - Production 257
    - Presentation 258
- Admissibility of Digital Evidence 258
  - Federal Rules of Evidence 258
  - Types of Evidence 260

Direct Evidence	260
Circumstantial Evidence	260
Admission of Digital Evidence in Court	261
Evidence Rules	261
Hearsay Rule	261
Business Records Exemption Rule	262
Best Evidence	262
Working with Legal Counsel	263
Attorney-Client Privilege	263
Attorney Work-Product	264
Non-testifying Expert Privilege	264
Litigation Hold	265
Establishing a Chain of Custody	265
What Is a Chain of Custody?	266
Establishing a Defensible Protocol	266
Traditional Forensic Acquisition	267
Live Response and Logical Acquisition	268
Documenting a Defensible Protocol	269
Documentation	269
Accuracy	270
Auditability and Reproducibility	270
Collection Methods	270
Data Privacy and Cyber Breach Investigations	271
What Is Data Privacy?	271
Handling Personal Data During Investigations	272
Enacting a Policy to Support Investigations	272
Cyber Breach Investigations and GDPR	273
Data Processing and Cyber Breach Investigations	274
Establishing a Lawful Basis for the Processing of	
Personal Data	275
Territorial Transfer of Personal Data	276
Summary	277
Notes	278
<b>Index</b>	<b>281</b>





## 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.<sup>1</sup>

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.<sup>2</sup>

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.<sup>3</sup>

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.<sup>4</sup> 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.<sup>5</sup>

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