

Table of Contents

About the Author	ix
About the Technical Reviewer	xi
Acknowledgments	xiii
Introduction	xv
Chapter 1: The Significance of Incident Response	1
Why Does This Happen?.....	2
Strategy vs. Tactics	7
Changing the Culture	9
Summary.....	9
Chapter 2: Necessary Prerequisites	11
Establishing the Identify and Protect Functions.....	11
Defined Cybersecurity Program.....	12
How Does Each Program Support Incident Response?	15
Summary.....	16
Chapter 3: Incident Response Frameworks	17
NIST 800-61	18
Organizing a Computer Incident Response Capability.....	18
Handling an Incident.....	32
NIST CSF Implementations	33
Detection	34
Respond.....	37
Recover.....	40

TABLE OF CONTENTS

From Guidance to Program Implementation 41

- Policy 41
- Procedures 43
- Control Processes Implemented..... 43
- Measurement 44
- Management Actions..... 45

Summary..... 45

Chapter 4: Leadership, Teams, and Culture 47

- Leadership Qualities 47
 - Passion 48
 - Humility 48
 - Listening..... 50
 - Decisiveness..... 51
 - Emotional Intelligence 52
- Culture 53
 - How They Build Culture at Ohio State..... 53
- Alignment of the Team 57
- Prepare to Handle Incidents..... 57
- Facilitating Organizational Change 57
 - Kotter’s Eight-Step Change Model 58
 - Lewin’s Change Management Model 61
- Summary..... 64

Chapter 5: The Incident Response Strategy..... 65

- Purpose..... 65
- Scope 66
- Definitions..... 66
- How to Respond to Incidents 67
 - Incident Response Goals 67
 - Roles and Responsibilities..... 67

Triage.....	68
Escalation	68
Event and Response Phases.....	68
Summary.....	70
Chapter 6: Cyber Risks and the Attack Life Cycle	71
Documenting Cyber Risks	72
Threat Analysis	73
How Vulnerabilities Become Risks	74
Measuring Risk Severity.....	75
Review the Risk Assessment.....	77
The Mandiant Cyber Attack Life Cycle	78
Breaking Down the Life Cycle.....	79
How This Helps	82
Tie the Risk Assessment and Kill Chain	82
Targeting End Users.....	82
Targeting Web Applications	83
Summary.....	85
Chapter 7: Detection and Identification of Events	87
Building Detective Capabilities	88
Data Loss Protection.....	88
Implementing DLP	88
End Point Detection and Response.....	91
Analyzing Traffic	91
Security Incident and Event Management.....	92
Empowering End Users	93
Other Ways of Detecting and Identifying Events.....	94
Identification of Security Events	96
Summary.....	98

TABLE OF CONTENTS

- Chapter 8: Containment..... 99**
 - Indicators of Compromise..... 99
 - Containment Fundamentals 100
 - Choosing a Containment Strategy..... 101
 - Malware and Ransomware Outbreaks 101
 - Denial of Service 112
 - Lost Assets 112
 - Data Theft 113
 - Unauthorized Access and Misuse of Assets 114
 - Retaining Forensic Investigators..... 115
 - Executive Expectations 115
 - Summary..... 116

- Chapter 9: Eradication, Recovery, and Post-incident Review 117**
 - Removing the Attacker's Artifacts..... 117
 - Malware Artifacts 118
 - Rootkits 120
 - Vulnerability Scanning 121
 - Patching Vulnerabilities 121
 - Restoring Systems via Backups..... 121
 - Post-incident Review 121
 - Summary..... 123

- Chapter 10: Continuous Monitoring of Incident Response Program..... 125**
 - Components of Continuous Monitoring..... 126
 - The Organizational Tiers 127
 - How Continuous Monitoring Works 128
 - The Continuous Monitoring Strategy 128
 - Incorporating Continuous Monitoring into the NIST CSF Environment..... 130
 - What Are the Incident Response Risks? 130
 - Defining the Monitoring Strategy 132
 - Establishing and Implementing the Program 133

Analyzing Data and Reporting Findings.....	133
Responding to Findings.....	134
Reviewing and Updating the Monitoring Program.....	135
Summary.....	135
Chapter 11: Incident Response Story	137
Background.....	137
Initial Response.....	138
The Nightmare Begins	141
Blue Screen of Death.....	141
A Locked Database.....	141
All Is Quiet	142
The First Angry Call	144
The Second Incident Response.....	145
The CISO's Office.....	146
Log Files and a Revelation.....	146
End Point Detection and Response (EDR).....	147
Help Arrives	148
Lessons Learned	148
Summary.....	149
Chapter 12: This Is a Full-Time Job.....	151
Full-Time Effort Required.....	151
Building a Program	151
Leadership.....	152
Balancing the Incident Response Program Against Other Priorities.....	154
Developing a Battle Plan.....	154
Network Segmentation and Incident Response	154
Preplanning and Strategy Development.....	156
Identification.....	157
Containment	157
Eradication, Recovery, and Lessons Learned	158
Summary.....	159

TABLE OF CONTENTS

Appendix: NIST Cybersecurity Framework..... 161

- Identify: Asset Management..... 161
- Identify: Business Environment..... 162
- Identify: Governance 162
- Identify: Risk Assessment 163
- Identify: Risk Management 163
- Identify: Supply Chain Risk Management 164
- Protect: Access Control 165
- Protect: Awareness and Training..... 165
- Protect: Data Security 166
- Protect: Information Protection 166
- Protect: Maintenance 167
- Protect: Protective Technology..... 168
- Detect: Anomalies and Events..... 168
- Detect: Continuous Monitoring..... 169
- Detect: Detection Processes 169
- Respond: Response Planning..... 170
- Respond: Communications 170
- Respond: Analysis 170
- Respond: Mitigation 171
- Respond: Improvement 171
- Recover: Recovery Planning 172
- Recover: Improvements 172
- Recover: Communications 172

Index..... 173