

# CONTENTS IN DETAIL

<b>ACKNOWLEDGMENTS</b>	<b>xvii</b>
------------------------	-------------

<b>INTRODUCTION</b>	<b>xix</b>
---------------------	------------

Who Should Read This Book and Why . . . . .	xx
What's in This Book . . . . .	xxi
The Book's Scope . . . . .	xxii

## **PART I: THE TABLETOP EXERCISE PROCESS 1**

### **1 WHY PERFORM TABLETOP EXERCISES? 3**

Reasons to Conduct a Tabletop Exercise . . . . .	4
Improve Incident Response Team Collaboration. . . . .	4
Clarify Team Roles and Responsibilities . . . . .	4
Assess the Impact of Process Changes . . . . .	5
Reduce the Cost of Data Breaches. . . . .	6
Improve Security Awareness . . . . .	8
Explore Key Questions. . . . .	9
Prepare Senior Leadership for an Incident . . . . .	9
Align with Industry Standards . . . . .	10
Fulfill Contractual Requirements . . . . .	11
Examine a Recent Cybersecurity Incident . . . . .	12
Identify and Prioritize Risks . . . . .	12
Advantages of Tabletops over Other Security Exercises. . . . .	13
Low Cost and High Return on Investment . . . . .	13
Efficiency . . . . .	14
No Operational Disruption . . . . .	14
What Tabletop Exercises Can Test . . . . .	15
The Potential Impact of Current Threats . . . . .	16
The Sufficiency of the Information Security Budget . . . . .	17
Information Sharing Protocols for IoCs . . . . .	18
Gaps in the Incident Response Plan . . . . .	19
The Efficacy of Processes and Procedures . . . . .	19
Compliance with Notification Requirements . . . . .	20
Residual Risk After Corrective Actions . . . . .	21
Summary . . . . .	21
Questions . . . . .	21

### **2 PLANNING THE TABLETOP EXERCISE 23**

Securing Executive Sponsor Support. . . . .	24
Choosing an Appropriate Executive Sponsor . . . . .	24
Outlining the Executive Sponsor's Responsibilities . . . . .	25

Defining the Exercise’s Goals and Objectives . . . . .	26
Rehearsing the Incident Response Plan . . . . .	27
Understanding Organizational Incident Response Roles . . . . .	27
Assessing Vendor Response . . . . .	27
Evaluating Communication Processes . . . . .	28
Senior-Level vs. Operational-Level Exercises . . . . .	28
Determining Who Should Participate . . . . .	29
External Vendors . . . . .	30
Legal Support . . . . .	32
The Development Team . . . . .	33
Logistical Considerations . . . . .	36
Hosting Remote vs. In-Person Exercises . . . . .	36
Determining the Duration . . . . .	37
Choosing a Date and Time . . . . .	37
Securing a Facility . . . . .	38
Setting the Tone . . . . .	40
Notifying and Preparing Exercise Attendees . . . . .	41
The Executive Checkpoint . . . . .	41
The Initial Email Notification . . . . .	42
Calendar Invitations . . . . .	43
The Discussion Session . . . . .	43
Informal Touchpoints . . . . .	44
The Final Reminder . . . . .	44
Scenario Confidentiality . . . . .	45
Opposition from Invitees . . . . .	46
Outsourcing Tabletop Exercises . . . . .	47
Summary . . . . .	48
Questions . . . . .	49

### 3

## THE DEVELOPMENT PROCESS: WHERE THE RUBBER MEETS THE ROAD

51

Choosing a Topic . . . . .	52
Consult Your Business Impact Analysis . . . . .	52
Confer with the Executive Sponsor . . . . .	53
Leverage Other Resources for Inspiration . . . . .	53
Developing the Scenario . . . . .	53
Characteristics of an Effective Scenario . . . . .	53
Sources of Inspiration for Your Scenario . . . . .	57
Introducing Injects . . . . .	59
Simulate Time Constraints . . . . .	61
Direct Focus . . . . .	62
Balance Clarity and Conciseness . . . . .	63
Designing the Exercise Storyboard . . . . .	63
Considering the Scenario Escalation Pace . . . . .	67
Crafting Your Ground Truth Document . . . . .	68
Add Details and Expected Outcomes . . . . .	69
Maintain Realism . . . . .	70
Align with Objectives . . . . .	70

Creating the Presentation Deck . . . . .	73
Introductions . . . . .	74
The Preamble . . . . .	74
Injects and Exercise Discussions . . . . .	78
The Debrief . . . . .	80
Inviting Feedback . . . . .	80
Summary . . . . .	80
Questions . . . . .	80

**4**  
**FACILITATING A SUCCESSFUL TABLETOP EXERCISE** **83**

The Facilitator’s Role . . . . .	83
Tabletop Management Tasks . . . . .	85
Assigning a Scribe . . . . .	85
Adding a Co-facilitator . . . . .	86
Inviting a Guest Presenter . . . . .	86
Prewriting Questions . . . . .	87
Exercise Tools and Tactics . . . . .	88
A Writing Board . . . . .	88
Polling Software . . . . .	88
Remote Presentation Software . . . . .	91
Multimedia Aids . . . . .	92
Attendee Tasks and Breakout Groups . . . . .	93
Recording Devices and Software . . . . .	94
Making the Most of the Exercise Space . . . . .	94
Maximize the Conference Room Layout . . . . .	94
Work the Room to Boost Engagement . . . . .	95
Communication Tips . . . . .	96
Monitor Physiological Responses . . . . .	96
Set Up Backchannels . . . . .	96
Check in with Senior Attendees . . . . .	97
Manage Conversation Hogs . . . . .	97
Forge Interpersonal Connections . . . . .	98
Consider the Question Structure . . . . .	99
Pay Attention to Nonverbal Communication . . . . .	100
Practice Cultural Awareness . . . . .	100
Identify Sensitive Topics Beforehand . . . . .	101
Summary . . . . .	101
Questions . . . . .	102

**5**  
**ACTING ON WHAT YOU’VE LEARNED: EVALUATION AND NEXT STEPS** **103**

Evaluation Requirements and Restrictions . . . . .	103
Choosing an Evaluator . . . . .	104
Evaluation Methods . . . . .	105
Performing a Debrief . . . . .	105
Sending a Survey . . . . .	106

Reporting Conventions . . . . .	107
Statement of Completion . . . . .	107
Full Report . . . . .	108
Follow-up Activities . . . . .	111
Assess the Incident Response Plan . . . . .	112
Catalog and Update Other Documentation and Processes . . . . .	112
Conduct Follow-up Tabletop Exercises . . . . .	113
Implement a Formal Tabletop Exercise Program . . . . .	113
Communicate High-Level Exercise Findings . . . . .	114
Identify and Analyze Trends . . . . .	114
Summary . . . . .	115
Questions . . . . .	115

## **PART II: EXAMPLE SCENARIOS 117**

### **6 ENGAGING A TECHNICAL AUDIENCE 119**

A Widespread Phishing Campaign . . . . .	120
The Scenario . . . . .	120
Possible Modifications . . . . .	123
Ransomware Affecting File Servers (the Technical Version) . . . . .	123
The Scenario . . . . .	124
Possible Modifications . . . . .	126
A Malware Outbreak via a Zero-Day Vulnerability . . . . .	126
The Scenario . . . . .	126
Possible Modifications . . . . .	130
A Supply Chain Compromise . . . . .	130
The Scenario . . . . .	130
Possible Modifications . . . . .	133

### **7 ENGAGING AN EXECUTIVE AUDIENCE 135**

Ransomware Affecting File Servers (the Senior-Level Version) . . . . .	136
The Scenario . . . . .	136
Possible Modifications . . . . .	138
A Dark Web Data Discovery . . . . .	138
The Scenario . . . . .	138
Possible Modifications . . . . .	140
A Distributed Denial-of-Service Attack . . . . .	141
The Scenario . . . . .	141
Possible Modifications . . . . .	143

### **8 ENGAGING THE BUSINESS 145**

A Physical Security Breach . . . . .	145
The Scenario . . . . .	146
Possible Modifications . . . . .	148

A Social Media Compromise . . . . . 148  
    The Scenario . . . . . 149  
    Possible Modifications . . . . . 152  
An Insider Threat . . . . . 152  
    The Scenario . . . . . 152  
    Possible Modifications . . . . . 155

**APPENDIX: REPORTING TEMPLATES 157**

**INDEX 165**