CONTENTS

List of figures viii
Author ix
Foreword x
Acknowledgements xi
Glossary xii
Useful websites xvi
Preface xviii

INTRODUCTION 1
Incident response 2
Digital forensics 4
Why both? 6
Hands-on 6
How this book fits in 7

PART 1 INCIDENT RESPONSE 9

1. UNDERSTANDING INFORMATION SECURITY INCIDENTS 11
What is an information security incident? 11
Types of incident 12
Detecting security incidents 19
Why do security incidents happen? 25
Summary 27

2. BEFORE THE INCIDENT 28
Building the incident response playbook 28
Testing the playbook 34
Incident planning and compliance 37
Forensic readiness 38
Summary 39

3. THE INCIDENT RESPONSE PROCESS 40
Identification 41
Containment 52
Eradication 57
Recovery 59
Summary 59

4. THINGS TO AVOID DURING INCIDENT RESPONSE 60
Eradication and preservation 61
An incident from an incident 67
The blame game 69
It's not over until it's over 70
Summary 70

5. AFTER THE INCIDENT 71
Post mortem 71
Quantify the impact 76
Forensics 79
Summary 79

6. THE BUSINESS OF INCIDENT RESPONSE 81
Request for proposal 81
The power of PR 84
Mergers and acquisitions 87
Escape the technical bubble 87
Incident response service providers 88
Summary 90

PART 2 DIGITAL FORENSICS 91

7. INTRODUCING THE DIGITAL FORENSICS INVESTIGATION 93
The investigator 94
Forensics fundamentals 96
Arriving at an investigation 100
Investigative process 100
Summary 104

8. THE LAWS AND ETHICS OF DIGITAL FORENSICS 105
Crimes without borders 105
Laws applicable to forensics 107
Ethical considerations 115
Summary 116

9. DIGITAL FORENSICS TOOLS 117
Grab bag 117
Forensic hardware 120
Forensic software 124
Summary 128

10. EVIDENCE ACQUISITION BASICS 129
The hard disk drive 129
Removable media 134
Processing disk images 135
File systems 136
Operating systems 139
Files 143

Analysis of artefacts 144
Summary 146

11. **CAPTURING A MOVING TARGET** **147**
Incident response and digital forensics 147
Live acquisition drivers 148
Live acquisition technique 152
Order of volatility 152
Network forensics 155
Summary 158

12. **MEMORY FORENSICS** **160**
Understanding memory devices 160
Capturing 164
Analysis 166
Summary 168

13. **CLOUD FORENSICS** **169**
Cloud computing terminology 169
Acquisition in the cloud 171
Container forensics 177
Forensics in the cloud? 178
Summary 178

14. **MOBILE DEVICE FORENSICS** **179**
Mobile phone terminology 179
Seizing mobile devices 182
Acquisition types and tools 184
Smartphones 186
Summary 188

15. **REPORTING AND PRESENTING YOUR FINDINGS** **189**
Layout and content 190
Audience 194
Summary 195

16. **THE HUMAN ELEMENTS OF AN INVESTIGATION** **196**
Victims 196
Perpetrators 201
Investigators 203
Summary 204

Index 205