

# Contents

Author Biography .....	xv
Introduction.....	xvii

## **CHAPTER 1 What is Information Security? ..... 1**

Introduction.....	2
What is security? .....	3
When are we secure?.....	4
Alert! .....	4
Models for discussing security.....	5
The confidentiality, integrity, and availability triad.....	5
The Parkerian hexad.....	7
Alert! .....	8
Attacks .....	9
Types of attack payloads.....	9
Threats, vulnerabilities, and risk.....	11
Risk management .....	12
Incident response .....	16
Defense in depth.....	19
Layers.....	20
Information security in the real world .....	21
Summary .....	21
Exercises .....	22
References.....	22

## **CHAPTER 2 Identification and Authentication ..... 23**

Introduction.....	24
Identification.....	24
Who we claim to be .....	24
Identity verification .....	25
Falsifying identification.....	25
Authentication.....	26
Factors.....	26
Multifactor authentication .....	28
Mutual authentication.....	29
Passwords.....	30
Biometrics .....	31

Additional resources ..... 31  
    Hardware tokens ..... 34  
Alert! ..... 35  
Identification and authentication in the real world ..... 36  
Summary ..... 37  
Exercises ..... 37  
References ..... 38

**CHAPTER 3 Authorization and Access Control ..... 39**

Introduction ..... 40  
Authorization ..... 40  
    Principle of least privilege ..... 41  
Access control ..... 42  
    Access control lists ..... 43  
Alert! ..... 45  
    Capabilities ..... 47  
Alert! ..... 48  
Access control methodologies ..... 49  
    Access control models ..... 49  
    Physical access controls ..... 52  
Authorization and access control in the real world ..... 54  
Summary ..... 54  
Exercises ..... 55  
References ..... 56

**CHAPTER 4 Auditing and Accountability ..... 57**

Introduction ..... 57  
Accountability ..... 58  
    Security benefits of accountability ..... 60  
    How we accomplish accountability ..... 62  
Auditing ..... 62  
    What do we audit? ..... 63  
Alert! ..... 63  
    Logging ..... 64  
    Monitoring ..... 65  
    Assessments ..... 65  
Accountability and auditing in the real world ..... 66

Summary ..... 67  
 Exercises ..... 68  
 References..... 68

**CHAPTER 5 Cryptography ..... 69**

Introduction..... 70  
 History..... 70  
     Caesar cipher ..... 71  
     Cryptographic machines ..... 71  
 Additional resources ..... 75  
     Kerckhoffs’ principle..... 75  
 Modern cryptographic tools ..... 75  
     Symmetric versus asymmetric cryptography ..... 76  
     Hash functions ..... 79  
     Digital signatures ..... 80  
     Certificates ..... 80  
 Protecting data at rest, in motion, and in use ..... 81  
     Protecting data at rest..... 81  
 Alert! ..... 83  
     Protecting data in motion ..... 84  
     Protecting data in use ..... 85  
 Cryptography in the real world ..... 85  
 Summary ..... 86  
 Exercises ..... 87  
 References..... 87

**CHAPTER 6 Laws and Regulations ..... 89**

Introduction..... 89  
 Laws and regulations..... 90  
     US laws applicable to computing ..... 91  
     Laws outside of the United States..... 91  
 Compliance ..... 94  
     Regulatory compliance ..... 94  
     Industry compliance ..... 95  
 Privacy ..... 95  
     The concept of privacy..... 96  
     Privacy rights ..... 96  
     Privacy and business..... 98

Summary..... 98  
Questions..... 99  
References..... 99

**CHAPTER 7 Operations Security..... 101**

Introduction..... 102  
Alert!..... 102  
Origins of operations security ..... 102  
    Sun Tzu..... 103  
Additional resources ..... 103  
    George Washington ..... 103  
    Vietnam War..... 104  
    Business ..... 106  
    Interagency OPSEC support staff ..... 106  
The operations security process ..... 107  
    Identification of critical information..... 107  
    Analysis of threats ..... 107  
    Analysis of vulnerabilities..... 110  
    Assessment of risks ..... 110  
    Application of countermeasures..... 111  
Haas' Laws of operations security ..... 111  
    First law ..... 112  
    Second law..... 112  
    Third law..... 113  
Operations security in our personal lives..... 114  
Alert!..... 114  
Operations security in the real world..... 115  
Summary ..... 116  
Exercises ..... 117  
References..... 117

**CHAPTER 8 Human Element Security ..... 119**

Introduction..... 119  
Humans: the weak link..... 120  
Security awareness ..... 120  
    Protecting data ..... 121  
    Passwords..... 121  
    Social engineering ..... 122  
    Network usage ..... 125

Malware ..... 126  
 Personal equipment..... 126  
 Clean desk..... 127  
 Policy and regulatory knowledge..... 127  
 The security awareness and training program ..... 127  
     Effectively reaching users ..... 128  
 Summary ..... 128  
 Exercises ..... 129  
 References..... 129

**CHAPTER 9 Physical Security..... 131**

Introduction..... 132  
 Alert!..... 132  
 Additional resources ..... 133  
 Physical security controls..... 134  
     Deterrent ..... 134  
     Detective ..... 135  
     Preventive ..... 135  
     How we use physical access controls ..... 136  
 Protecting people ..... 136  
     Physical concerns for people..... 136  
     Safety ..... 137  
     Evacuation ..... 138  
     Administrative controls ..... 139  
 Protecting data ..... 140  
     Physical concerns for data..... 140  
     Availability ..... 141  
     Residual data..... 142  
     Backups..... 143  
 Protecting equipment..... 143  
     Physical concerns for equipment ..... 144  
 Note..... 144  
     Site selection..... 145  
     Securing access..... 146  
     Environmental conditions..... 146  
 Physical security in the real world..... 147  
 Summary ..... 148  
 Exercises ..... 149  
 References..... 149

<b>CHAPTER 10 Network Security .....</b>	<b>151</b>
Introduction.....	152
Protecting networks .....	152
Security in network design .....	153
Firewalls.....	153
Network intrusion detection systems .....	157
Protecting network traffic.....	158
The impact of intercepted data.....	158
Virtual private networks .....	159
Wireless network security .....	159
Secure protocols .....	160
Mobile device security .....	161
What is a mobile device? .....	161
Mobile device management .....	162
Bring your own device .....	162
Network security tools.....	163
Wireless .....	164
Port scanners.....	164
Packet sniffers.....	165
Alert! .....	165
Honeypots .....	165
Additional resources .....	167
Firewall tools .....	167
Network security in the real world .....	167
Summary .....	168
Exercises .....	168
References.....	169
<b>CHAPTER 11 Operating System Security .....</b>	<b>171</b>
Introduction.....	172
Operating system hardening.....	172
Remove all unnecessary software .....	173
Remove all unessential services.....	174
Alter default accounts.....	175
Apply the principle of least privilege .....	176
Perform updates .....	177
Turn on logging and auditing.....	178
Protecting against malware .....	178

Additional resources .....	179
Anti-malware tools .....	179
Executable space protection .....	180
Software firewalls and host intrusion detection.....	180
Software firewalls .....	181
Host intrusion detection.....	181
Operating system security tools .....	181
Scanners .....	182
Alert!.....	183
Vulnerability assessment tools .....	183
Exploit frameworks .....	183
Operating system security in the real world .....	185
Summary .....	185
Exercises .....	186
References.....	186
<b>CHAPTER 12 Application Security .....</b>	<b>189</b>
Introduction.....	190
The TJX breach .....	190
Software development vulnerabilities.....	191
Additional resources .....	191
Buffer overflows.....	192
Race conditions.....	192
Input validation attacks .....	193
Authentication attacks .....	193
Authorization attacks.....	194
Cryptographic attacks.....	194
Web security .....	195
Client-side attacks.....	195
Alert!.....	196
Server-side attacks.....	197
Database security.....	198
Protocol issues .....	199
Unauthenticated access.....	200
Arbitrary code execution .....	200
Privilege escalation.....	201
Additional resources .....	201
Application security tools.....	202

**xiv** Contents

Sniffers.....	202
Web application analysis tools.....	202
Alert!.....	203
Fuzzers.....	204
Application security in the real world .....	206
Summary.....	207
Exercises.....	208
References.....	208
Index .....	209