George K. Kostopoulos

CYBERSPACE and CYBERSECURITY

SKN006774

CRC P
Taylor & Fra

005.8
K86

CYBERSPACE and CYBERSECURITY

George K. Kostopoulos

THƯ VIỆN TRƯỜNG ĐHSPKT
SKN 006774

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **Informa** business

Contents

Foreword xi

Preface xiii

About the Author xvii

1 Vulnerabilities in Information Systems **1**

Introduction 1

Measuring Vulnerability 4

Avoiding Vulnerabilities through Secure Coding 6

Mistakes Can Be Good 10

Threats Classification 11

Threat Modeling Process 11

Security Starts at Home 13

Security in Applications 14

International Awareness 15

Exercises 16

2 Vulnerabilities in the Organization **19**

Introduction 19

Common Organizational Vulnerabilities 20

Access Authorization and Authentication 21

Human Factors 24

Security Services 25

External Technologies 26

Wireless Networks 27

Bluetooth 28

Passive Vulnerabilities 29

Active Vulnerabilities 29

Precautions 29

Wireless Fidelity 30

Wi-Fi Precautions at Home 32

Wi-Fi Precautions at the Hotspot 34

Wi-Fi Precautions at the Enterprise 35

Worldwide Interoperability Microwave Access 36

WiMAX Features 36

Cloud Computing 38

Exercises 42

3 **Risks in Information Systems Infrastructure 45**

Introduction 45

Risks in Hardware 46

Risks in Software 49

Risks in People 52

Risks in Laptops 53

Risks in Cyberspace 54

Risk Insurance in Cyberspace 56

Exercises 58

4 **Secure Information Systems 61**

Introduction 61

Assets Identification 62

Assets Communication 64

Assets Storage 66

Resource Access Control Facility 68

Securing the Email Communications 69

Email Server Side 69

Email Client Side 70

Information Security Management 70

Exercises 73

5 **Cybersecurity and the CIO 79**

Introduction 79

CIO: Personality 80

Trust and Ethics 80

Communication and Intelligence 81

Leadership and Entrepreneurship 81

Courage and Limitations 81

CIO: Education 82

University Degrees 82

Certifications 82

CIO: Experience 82

CIO: Responsibilities 83

Data Backup and Archiving 85

Culture of Security 85

Cyber Training 86

Contingency Plans 87

Liability 87

CIO: Information Security 87

Internal Information Security Components 87

Access Control—Electronic 87

Access Control—Physical 88

Cyber Policies 88

Cyber Awareness and Training 89

Training 89

Business Continuity 90

CIO: The Changing Role 91

Exercises 91

6 Building a Secure Organization 93

Introduction 93

Business Continuity Planning 94

Business Impact Analysis (BIA) 96

Business Recovery Strategy (BRS) 96

Drafting of the BCP 97

Testing of the BCP 97

Training in BCP Implementation 98

BCP Performance Indicators 98

System Access Control 98

System Development and Maintenance 100

Physical and Environmental Security 101

Compliance 101

Personnel Security 103

Security Organization 104

Computer and Network Management 104

Asset Classification and Control 104

Security Policy 105

Exercises 106

7 Cyberspace Intrusions 109

Introduction 109

IDPS Configuration 110

Sensors 111

Processor 113

Consoles 113

Network 114

IDPS Capabilities 114

Information Acquisition 115

Information Loggings 115

Detection Techniques 115

Prevention Actions 117

IDPS Management 117

Implementation 117
Step One: Features 118
Step Two: Architecture 118
Step Three: Installation 118
Step Four: Testing 119
Step Five: Activation 119
Operation 120
Maintenance 120
IDPS Classification 121
Host-Based IDPS 122
Network-Based IDPS 124
Network Behavior Analysis System 124
Wireless IDPS 125
IDPS Comparison 128
Exercises 129

8 Cyberspace Defense 131
Introduction 131
File Protection Applications 131
File Backup 131
Disaster Recovery 133
History Deletion 133
Shredding and Wiping 135
File Undelete 135
File Encryption 135
Loggers 136
Anti-Loggers 137
PC Performance Applications 137
Registry Repair 138
Anti-Rootkits 138
Antivirus 139
Junk Files 139
Fragmentation 140
Protection Tools 140
Security Analyzer 140
Password Analyzer 142
Firewalls 143
Packet-Level Filtering 145
Circuit-Level Filtering 145
Application-Level Gateway 145
Email Protection 146
Exercises 147

9 Cyberspace and the Law **151**
Introduction 151
International Laws 152
Europe 152
United Nations 153
North Atlantic Treaty Organization 153
INTERPOL 155
Impediments to Cyber Law Enforcement 156
Cyber-Related Laws in the United States 156
Commercial Privacy Bill of Rights Act of 2011 157
Cybersecurity Act of 2010 159
Federal Information Security Management Act of 2002 161
USA PATRIOT Act of 2001 162
Communications Assistance for Law Enforcement Act of 1994 163
Computer Security Act of 1987 165
Privacy Act of 1974 165
Cybercrime 166
Trends in Cyber Abuse 167
Combating Cybercrime 167
Exercises 170

10 Cyber Warfare and Homeland Security **175**
Introduction 175
Cyber Warfare 176
Cyber Weapons Convention 180
Cyber Terrorism 181
Cyber Espionage 183
Homeland Security 185
National Cyber Security Division 185
Cybersecurity Preparedness 186
Challenges 187
Distributed Defense 188
Countermeasures 189
Cyber Defense Ecosystem 190
Cybersecurity Training 191
Cyber Simulation and Exercises 191
Exercises 195

References **199**

Index **211**

Information Technology / Security & Auditing

... a timely read, and even more so, a trusted resource ... covers a great deal of ground very well and its tutorial and comprehensive checklist style pulls even the risk discussions together in an understandable and educational manner that reinforces awareness to the critical attributes found within this manmade domain. ... each individual chapter deals with an important and realistic aspect of cybersecurity together with the vulnerabilities and risks. Together, the chapters provide a first-rate overview of this exceedingly complex topic, a perspective that has equally horizontal as well as vertical implications, and will keep the reader cognizant of the interrelationships among the disparate disciplines making up cyberspace.

—Riley Repko, CEO, Trusted Cyber Solutions LLC & Senior Research Fellow,
Virginia Tech University

Based on related courses and research on the cyber environment in Europe, the United States, and Asia, ***Cyberspace and Cybersecurity*** supplies complete coverage of cyberspace and cybersecurity. It not only emphasizes technologies but also pays close attention to human factors and organizational perspectives.

Detailing guidelines for quantifying and measuring vulnerabilities, the book also explains how to avoid these vulnerabilities through secure coding. It covers organizational-related vulnerabilities, including access authorization, user authentication, and human factors in information security. Providing readers with the understanding required to build a secure enterprise, block intrusions, and handle delicate legal and ethical issues, the text:

- Examines the risks inherent in information system components, namely, hardware, software, and people
- Explains why asset identification should be the cornerstone of any information security strategy
- Identifies the traits a CIO must have to address cybersecurity challenges
- Describes how to ensure business continuity in the event of adverse incidents, including acts of nature
- Considers intrusion detection and prevention systems (IDPS), focusing on configurations, capabilities, selection, management, and deployment

Explaining how to secure a computer against malware and cyber attacks, the text's wide-ranging coverage includes security analyzers, firewalls, antivirus software, file shredding, file encryption, and anti-loggers. It reviews international and U.S. federal laws and legal initiatives aimed at providing a legal infrastructure for what transpires over the Internet. The book concludes by examining the role of the U.S. Department of Homeland Security in our country's cyber preparedness.

Exercises with solutions, updated references, electronic presentations, evaluation criteria for projects, guidelines to project preparations, and teaching suggestions are available upon qualified course adoption.

CRC Press
Taylor & Francis Group
an informa business
www.crcpress.com

6000 Broken Sound Parkway, NW
Suite 300, Boca Raton, FL 33487
711 Third Avenue
New York, NY 10017
2 Park Square, Milton Park
Abingdon, Oxon OX14 4RN, UK

K14391
ISBN: 978-1-4665-0133-1
90000
9 781466 501331

www.crcpress.com