

Managerial Guide for Handling Cyber-Terrorism and Information Warfare

Table of Contents

Preface	viii
----------------------	-------------

PART 1: FROM INFORMATION SECURITY TO CYBER-TERRORISM

Chapter 1: Information and Computer Security	1
<i>Definitions</i>	<i>2</i>
<i>Historical Security Brief.....</i>	<i>4</i>
<i>Implementing Information Security</i>	<i>10</i>
<i>Issues Requiring Attention</i>	<i>20</i>
<i>Conclusion</i>	<i>21</i>
<i>Bibliography.....</i>	<i>21</i>
 Chapter 2: The Nature of Terrorism.....	 24
<i>Definition of Terrorism.....</i>	<i>25</i>
<i>Primary Terrorism Drivers</i>	<i>27</i>
<i>Overview of Terrorist Acts.....</i>	<i>33</i>
<i>The Link between Terrorism and Information Technology</i>	<i>34</i>
<i>Prognosis on Terrorist Activities</i>	<i>35</i>
<i>Bibliography.....</i>	<i>37</i>
 Chapter 3: Cyber-Terrorism.....	 40
<i>Possible Terrorist Activities Against IT</i>	<i>41</i>
<i>Definition of Cyber-Terrorism and Information Warfare</i>	<i>43</i>

<i>Why Do Cyber-Terrorists Strike?</i>	44
<i>Correlations between Cyber and Corporeal Conflicts</i>	47
<i>Planning Security Systems: Overall Principles</i>	48
<i>Conclusion</i>	57
<i>Bibliography</i>	57

PART 2: ATTACKS AGAINST INFORMATION TECHNOLOGY

Chapter 4: Physical Security	61
<i>Issues in Physical Security</i>	64
<i>Advertising the Location</i>	65
<i>Securing the Perimeter</i>	67
<i>Protection of Equipment from External Disturbances</i>	75
<i>Theft of Equipment</i>	78
<i>Protection Against Eavesdropping</i>	79
<i>New Form of Attack</i>	81
<i>Retrieval of Information from Magnetic Media</i>	83
<i>Conclusion</i>	83
<i>Bibliography</i>	84
Chapter 5: Denial of Service Threat	85
<i>The Nature of DOS and DDOS Attacks</i>	86
<i>Mechanics of the DOS/DDOS Attacks</i>	88
<i>Conclusion</i>	94
<i>Bibliography</i>	95
Chapter 6: Web Defacements and Semantic Attacks	97
<i>Political Orientation</i>	99
<i>Protections</i>	102
<i>Conclusion</i>	103
<i>Bibliography</i>	104

Chapter 7: DNS Attacks..... 106
Launching an Attack..... 107
Handling DNS Attacks 108
Bibliography..... 109

Chapter 8: Routing Vulnerabilities 110
How to Eliminate Router Threats..... 114
Importance of Routing Vulnerabilities for Prevention..... 115
Bibliography..... 117

Chapter 9: Identity Stealing Attacks 119
Examples of Identity Theft Attacks 119
Conclusion 123
Bibliography..... 125

PART 3: HANDLING INFORMATION SECURITY ISSUES

Chapter 10: Identification, Authentication, and Access Control 129
A Question of Proper Identification..... 129
Key Definitions 131
Security of the Authentication Methods 132
Access Control 143
Monitoring System Access and Usage 155
Mobile Computing 157
Conclusion 160
Bibliography..... 160

Chapter 11: Personnel Security 163
Hiring New Staff..... 164
Security Duty During Employment 169
Terminating Employment..... 170

<i>Conclusion</i>	172
<i>Bibliography</i>	173
Chapter 12: Operations Management	175
<i>Operational Procedures and Responsibilities</i>	175
<i>System Planning and Acceptance</i>	177
<i>Protection Against Malicious Software</i>	179
<i>Housekeeping</i>	181
<i>Network Management</i>	182
<i>Media Handling and Security</i>	183
<i>Exchange of Information and Software</i>	186
<i>System Development and Maintenance</i>	187
<i>Compliance</i>	193
<i>Conclusion</i>	198
<i>Bibliography</i>	198
Chapter 13: Information Security Policy	199
<i>How to Generate an ISP</i>	202
<i>Example of Information Security Policy</i>	205
<i>Implementation of ISP</i>	209
<i>Conclusion</i>	210
<i>Bibliography</i>	211
Chapter 14: Business Continuity Management	213
<i>Business Continuity Management Process</i>	214
<i>Commentary</i>	220
<i>Bibliography</i>	220
Epilogue: Thoughts for the Future	222
About the Authors	226
Index	227