



Table of Contents

Introduction	1
Part I - Securing The Infrastructure	3
1 How to Deal with Real World Infrastructure Security Threats	8
1.1 Introduction	8
1.2 Why Infrastructure Failure?	10
1.3 Remedies	10
1.3.1 Put the Users, First	10
1.3.2 Asset Protection and Resilience	11
1.3.3 Consider External Systems are Insecure	11
1.3.4 Providing Audit Information to Consumers	11

1.3.5	Both Users and Process Need Authentication	12
1.4	References	12
2	What Are Monitoring and Access-Control Systems	15
2.1	Introduction	15
2.2	What is Access Control and Monitoring System?	16
2.2.1	Various Types of Access Control	16
2.3	Overview of Infrastructure Security	17
2.4	Three Important Practices to Strengthen Cybersecurity	18
2.4.1	Combine Cybersecurity with AI and Machine Learning	18
2.4.2	Enhance Visibility	18
2.4.3	Increase Preparation Planning	19
2.5	Access Control	19
2.5.1	What is Access Control?	19
2.5.2	Various Access Control Systems	20
2.6	Security Policy	22
2.7	Physical Security Controls	24
2.7.1	Introduction to Physical Security	24
2.7.2	Physical Security Controls	24
2.7.3	Locks and Keys	26
2.8	Standard key-locking Deadbolt	28
2.8.1	Types of Deadbolts	29
2.9	Solenoid-operated Deadbolt Locks	30
2.10	Cipher Locks	32
2.11	Access-control Gates	34
2.12	Sliding Gates	35
2.12.1	Automatic Sliding Gate	36
2.12.2	Characteristics of Sliding Gate	36
2.13	Swinging Gates	37
2.14	Control Relays	39
2.14.1	Classification of Relay	41
2.15	Authentication Systems	42
2.15.1	Methods	42
2.15.2	Authentication Factors	43
2.15.3	Single-factor Authentication	44
2.15.4	Multi-factor Authentication	44
2.15.5	Strong Authentication	44
2.16	Magnetic Stripe Reader	45

2.16.1	Definition of Magnetic Stripe Reader	45
2.17	Smart Cards	46
2.17.1	The Meaning of the Smart Card	46
2.17.2	Advantages	47
2.17.3	Types of Smart Cards	47
2.18	RFID Badges	48
2.18.1	Introduction to RFID Badges	48
2.18.2	Methods and Materials	48
2.18.3	How is the RFID System Managed?	48
2.18.4	RFID System Components	49
2.19	Biometric Scanners	49
2.19.1	Types of Biometric Authentication Scanner	50
2.20	2Remote Access Monitoring	51
2.21	Opened-and Closed-condition Monitoring	53
2.22	Automated Access Control Systems	54
2.22.1	Automated Access Control Systems Information	54
2.22.2	Topologies of an Access Control System	56
2.22.3	Models of Access Controls	56
2.23	References	57
3	Brief about Video Surveillance Systems	61
3.1	Introduction	61
3.2	What is a Video Surveillance System?	62
3.3	Types of Video Surveillance Systems	62
3.4	Background of Video Surveillance Systems	64
3.5	Uses of Video Surveillance Systems	64
3.5.1	Industries & Offices	64
3.5.2	Traffic Monitoring	65
3.5.3	Sporting Events	66
3.5.4	Monitor Employees	66
3.5.5	ATM & Banks	66
3.5.6	Schools & Colleges	67
3.6	Criticism of Video Surveillance Systems	67
3.7	Market for Video Surveillance Systems	67
3.8	Video Surveillance around the World	68
3.8.1	London	68
3.8.2	Beijing	69
3.8.3	Chicago	69

3.8.4	New York	70
3.8.5	Chongqing, China	70
3.9	Factors to Consider While Selecting Your Video Surveillance System	71
3.9.1	How many Cameras You Need	71
3.9.2	Where to Install the Cameras	71
3.9.3	Various Attributes of the Surveillance System	71
3.9.4	Frame Rate	71
3.10	References	72
4	Brief about Intrusion Detection and Reporting Systems	74
4.1	Intrusion Detection Systems	74
4.1.1	Types of IDS (Intrusion Detection Systems)	75
4.2	Security Controllers	77
4.3	Wi-Fi Security	77
4.4	Sensors	80
4.4.1	What are Sensors?	80
4.4.2	Classification of Sensors	81
4.4.3	Types of Sensors	81
4.4.4	Factors to Consider while Choosing the Right Sensor	83
4.5	Vehicle Detection Sensors	84
4.6	Fire Detection Sensors	85
4.7	Fire Alarms and Detection Methods	86
4.7.1	Types of Flame Detectors	87
4.7.2	Other Fireplace Alarms	89
4.8	Output Devices	90
4.8.1	Reasons for having an Output Device	90
4.8.2	Various Output Devices	91
4.9	References	91
Part II - Securing Local Hosts		94
5	Localhost Security in the Real World	102
5.1	Introduction	102
5.2	Security Challenges	108
5.2.1	Active Attacks	108
5.2.2	Passive Attacks	111

5.3	Other Security Challenges	112
5.3.1	Computer Virus	112
5.3.2	Rogue Security Software	113
5.3.3	Trojan Horse	114
5.3.4	Adware and Spyware	115
5.3.5	Computer Worms	115
5.3.6	Denial-of-Service (DOS) and Distributed-DOS (DDOS) Attack	116
5.3.7	Phishing	117
5.3.8	Rootkit	117
5.3.9	SQL Injection Attack	118
5.3.10	Man in the Middle Attacks	119
5.4	Device Security Scenario 1 - Home Environment	120
5.5	Device Security Scenario 2 - Office Environment	123
5.6	Summary	125
5.7	References	127
6	Everything You should Know about Securing Devices	130
6.1	Introduction	130
6.2	Explanation of a Device	131
6.3	How to Secure Your Devices?	132
6.3.1	Layers of Security	132
6.3.2	What We have to Do?	134
6.4	Network Security	135
6.4.1	Operating Systems	135
6.4.2	Remote Access	136
6.4.3	Remote Access Technology	137
6.4.4	SSL VPN Technology	138
6.4.5	Wireless Access Control	139
6.5	Securing Host Devices	140
6.6	Securing Internet Applications	141
6.7	Types of Network Security	142
6.7.1	Gateway Security	142
6.7.2	Identity Management	143
6.7.3	Firewalls for Web Application	145
6.7.4	Virtual Private Networks	145
6.7.5	Antivirus	146
6.7.6	Data Loss Prevention	146

6.7.7	Email Security	146
6.7.8	Intrusion Detection System	146
6.8	Internal Security	148
6.9	Endpoint Devices	149
6.10	Transport Layer Security (TSL)	150
6.11	Managing Endpoint Devices	151
6.12	Cloud Security	152
6.12.1	Challenges in Cloud Computing	153
6.13	Significance of Cybersecurity	155
6.14	References	155

7 Details on How to Protect the Inner Perimeter 158

7.1	The Inner Perimeter	158
7.1.1	Firewalls	158
7.1.2	Border Routers	159
7.1.3	De-militarized Zones	160
7.1.4	Intrusion Detection Systems (IDS)	160
7.1.5	Intrusion Prevention System	161
7.2	Inner Perimeter Requirements	162
7.3	Inner Perimeter Guidelines	162
7.4	Connectivity and Mobility	163
7.4.1	Connectivity of LAN Systems	163
7.4.2	Wireless Connectivity	164
7.4.3	VPN Connectivity	165
7.4.4	Device Ports	166
7.5	Operating System Security Choices	167
7.6	Local Administrative Tools	167
7.6.1	User Authentication	167
7.6.2	User Accounts	168
7.6.3	Backing Up and Restoring Data	169
7.6.4	Account Policies	169
7.6.5	File Systems	170
7.6.6	Network Services	170
7.6.7	System Patches	171
7.6.8	Operating System Minimization	172
7.6.9	Logging and Monitoring	172
7.6.10	System Integrity	173
7.7	Operating System Security Tools	173

7.8	Implementing Data Encryption	173
7.8.1	Damages and Breach of Data	174
7.8.2	The Importance of being Encrypted	175
7.8.3	What is Encryption?	175
7.8.4	Choosing What to Encrypt	175
7.8.5	Data States	176
7.9	Points for Implementing a Successful Data Encryption Strategy	177
7.10	References	179
8	Everything Related to Protecting Remote Access	181
8.1	Introduction	181
8.2	RDP Brute-force Attacks and RDP Credentials for Trade	182
8.3	Securing against RDP Compromise Risk	182
8.4	How to Protect Local Devices?	183
8.4.1	Physical Safety	184
8.4.2	Authentication	184
8.4.3	Software for Anti-malware	184
8.4.4	Robust Protocols	184
8.4.5	Firewall	185
8.5	Secure Connection	185
8.5.1	What does Secure Connection mean?	185
8.5.2	Six Precious Tips for Applying Secure Connections when Online	185
8.6	Usual Settings	187
8.7	Implementing a Firewall	187
8.7.1	What Firewalls Do?	187
8.7.2	What kind of Firewall is the Best?	187
8.7.3	How to Configure a Firewall?	188
8.8	How to Install and Use Anti-malware Software?	189
8.8.1	Working of Anti-malware	189
8.8.2	How to Install Malwarebytes Anti-malware	190
8.8.3	How to Use Malwarebytes Anti-malware in your PC	196
8.9	Removing Unnecessary Software	199
8.9.1	Control Panel	199
8.9.2	Windows Explorer	200
8.9.3	Free Uninstallers	200
8.9.4	Malware Scanners	200

8.10	Disabling Non-essential Services	200
8.11	Disable Unwanted OS Default Features	201
8.12	Keep Your Web Browser Secured	206
8.12.1	Configure Security of Your Browser and Privacy Settings	207
8.12.2	Keep Updated Browser	207
8.12.3	Sign Up for Warnings	208
8.12.4	Be Careful while Installing Plug-ins	208
8.12.5	Install AV	208
8.12.6	Install Safety Plug-ins	208
8.13	Install All the Updates and Patches	209
8.13.1	Types of Updates	209
8.13.2	What are Patches?	209
8.13.3	Why Patch Your PCs and Servers Early and Often	210
8.14	Requiring Strong Passwords	211
8.14.1	Information Sharing and Safety Issues	211
8.14.2	Important points of Password Safety	212
8.14.3	Importance of a Powerful Password	212
8.15	Use Various Local Protection Tools	212
8.15.1	Local Firewalls	212
8.15.2	Host-based Intrusion Detection Method	213
8.15.3	Browser Security Alternatives	213
8.15.4	Antivirus/Anti-malware Tools	213
8.15.5	Software Versions having Recent Updates and Patches	213
8.16	Software-based Local Firewalls	214
8.17	Use Various Tools for Local Intrusion Detection	215
8.17.1	NIDS (Network-based Intrusion Detection System)	215
8.17.2	HIDS (Host-based Intrusion Detection System)	215
8.17.3	Signature Detection	216
8.17.4	Anomaly Detection	216
8.17.5	OSSEC	217
8.17.6	OpenWIPS-NG	217
8.17.7	Suricata	217
8.17.8	Bro IDS	218
8.18	Profile-based Anomaly Detection Systems	218
8.19	Threshold-based Anomaly Detection Systems	218
8.19.1	Introduction of Anomaly Detection	218

8.19.2	What are Anomalies Detection?	219
8.19.3	Techniques of Anomaly Detection	220
8.20	How to Configure Browser Security?	221
8.20.1	Introduction of Configuring Browser Options	221
8.20.2	Solution for Internet Explorer	221
8.20.3	Google Chrome Browser Solution	224
8.21	Configuring Security Levels	227
8.22	Configuring Script Support	228
8.23	Fight and Prevent Malicious Software	230
8.23.1	Definition of Malicious Code	230
8.23.2	Wherewith can You Defend Yourself toward Malicious Code?	231
8.23.3	Whereby make Yourself Improve if You Display a Sufferer of Malicious Code?	233
8.24	Using Antivirus programs	233
8.24.1	Introduction of Using Antivirus Programs	233
8.24.2	Advantages of Antivirus Programs	235
8.24.3	Disadvantages of Antivirus Programs	236
8.25	Using Antispyware	236
8.25.1	What is Spyware?	236
8.25.2	The Aim of Antispyware	237
8.25.3	Protection from Antispyware	237
8.25.4	Beware of Unsafe Imposters	237
8.25.5	Limitations of the Rule	238
8.25.6	In New Market	239
8.26	Hardening Operating Systems	239
8.26.1	Introduction of Hardening Operating System	239
8.26.2	Systems Hardening has Nine Best Methods	240
8.26.3	Advantages of Systems Hardening	242
8.27	Service Packs	242
8.27.1	Introduction of Service Packs	242
8.27.2	What Service Pack Perform Should	243
8.27.3	Do I Manage the Latest Service Pack?	244
8.28	Patches	244
8.28.1	Introduction of Patch	244
8.28.2	Connecting Patches	245
8.28.3	Details of Patch	245

8.29	Updates	246
8.29.1	Introduction of Updates	246
8.30	Brief about Application Software Security	247
8.30.1	Introduction of Application Software Security	247
8.30.2	How Important is Application Software Security?	248
8.30.3	Application Security Tools	248
8.31	Software Exploitation	249
8.31.1	Introduction of Software Exploitation	249
8.31.2	Who is This Course for this Software Exploitation?	249
8.31.3	Reading Purposes	250
8.31.4	Key Training Purposes	250
8.32	Using Updates and Patches for Software	250
8.32.1	Introduction of Applying Software Updates and Patches	250
8.33	References	252
Appendix A: Figures		257
Appendix B: Graphs		263
Appendix C: Glossary		264
Index		279