



Michael Erbschloe

# Physical Security for IT

# *Contents*

<b>Preface</b>	<b>xiii</b>
<b>Acknowledgements</b>	<b>xv</b>
<b>Introduction</b>	<b>xvii</b>
<b>1. Physical Security Overview</b>	<b>I</b>
1.1 Why Physical Security Is Important	2
1.2 The Relationship Between Physical and Cyber Security	3
1.3 Guard Against Disgruntled Employees and Angry Former Employees	4
1.4 How Activists and Corporate Foes Can Hurt You	5
1.5 Vandals Who Damage for Fun	6
1.6 Saboteurs Who Work for Profit	7
1.7 Thieves and Spies Are Everywhere	9
1.8 Domestic Terrorists Are Still a Threat	10
1.9 International Terrorist Are a Growing Threat	12
1.10 Physical Security for Natural Disasters	14
1.11 Physical Security for Random Incidents	15
1.12 Action Steps to Improve Physical IT Security	16
<b>2. Establishing a Physical IT Security Function</b>	<b>19</b>
2.1 Organizational Placement of the IT Physical Security Function	20
2.2 Interdepartmental Relationships for Physical Security	22
2.3 Evaluating Financial Resources	23
2.4 The Role of Corporate Security	24
2.5 The Role of IT Security	25

2.6	The Role of Network Security	26
2.7	Relationships with Law Enforcement	27
2.8	Relationships with Private Security Providers	29
2.9	Establishing and Utilizing an Alert System	30
2.10	Action Steps to Improve Physical IT Security	32

### **3. Developing an IT Physical Security Plan 35**

3.1	Overview of the Planning Process	36
3.2	Developing the IT Physical Security Plan	38
3.3	Utilizing Existing Risk Exposure Analysis	39
3.4	Integrating Physical IT Security and Cyber Security Planning	40
3.5	Integrating Physical IT Security and Disaster Recovery Planning	41
3.6	Integrating Physical IT Security and Business Continuity Planning	42
3.7	Working with Your Insurance Company	43
3.8	Evaluating Regulatory Requirements	44
3.9	Action Steps to Improve Physical IT Security	48

### **4. Major Elements of a Physical IT Security Plan 51**

4.1	Overview and Mission Statement	54
4.2	Organizational Responsibilities	54
4.3	Duty Officers	55
4.4	Contact Lists	56
4.5	Security Procedures for Data Centers	56
4.6	Security Procedures for Wiring and Cabling	58
4.7	Security Procedures for Remote Computers	59
4.8	Security Procedures for Desktops	60
4.9	Security Procedures for Department-Based Servers	61
4.10	Security Procedures for Telecom and Datacom Equipment	62
4.11	Security Procedures for Manufacturing Control Equipment	63
4.12	Security Procedures for Surveillance and Alarm Systems	64
4.13	Action Steps to Improve Physical IT Security	65

<b>5. Developing and Documenting Methods and Procedures</b>	<b>67</b>
5.1 The Process of Developing Methods and Procedures	68
5.2 Devising a Format for Documenting Procedures	69
5.3 Physical Security Procedures for Data Centers	70
5.4 Physical Security Procedures for Wiring and Cabling	71
5.5 Physical Security Procedures for Remote Computers	72
5.6 Physical Security Procedures for Desktops	72
5.7 Physical Security Procedures for Department-Based Servers	73
5.8 Physical Security Procedures for Telecom and Datacom Equipment	74
5.9 Physical Security Procedures for Manufacturing Control Equipment	75
5.10 Physical Security Procedures for Surveillance and Alarm Systems	76
5.11 Action Steps to Improve Physical IT Security	77
<b>6. Auditing and Testing Procedures</b>	<b>79</b>
6.1 How to Audit and Test Procedures	79
6.2 Auditing and Testing for Data Centers	82
6.3 Auditing and Testing Wiring and Cabling Security	85
6.4 Auditing and Testing Remote Computer Procedures	86
6.5 Auditing and Testing Desktop Procedures	87
6.6 Auditing and Testing Procedures for Department-Based Servers	88
6.7 Auditing and Testing Telecom and Datacom Equipment Security	89
6.8 Auditing and Testing Manufacturing Control Equipment Security	90
6.9 Auditing and Testing in Surveillance and Alarm System Security	91
6.10 Action Steps to Improve Physical IT Security	92
<b>7. The Role of the Incident Response Team</b>	<b>95</b>
7.1 The First Report	97
7.2 The Confirmation Process	99
7.3 Mobilizing the Response Team	99
7.4 Notifying Management	100

7.5	Using the Alert System	101
7.6	The Preservation of Evidence	102
7.7	When to Call Law Enforcement	103
7.8	Returning to Normal Operations	104
7.9	Analyzing Lessons Learned	105
7.10	The Role of the Incident Response Team During Disasters	107
7.11	Action Steps to Improve Physical IT Security	113

## **8. Model Training Program for Organization Staff 117**

8.1	Training for IT and Security Professionals	118
8.2	The Basics of Training	119
8.3	Building Awareness About Physical Security for IT Assets	120
8.3.1	Testing and Evaluating the Module	123
8.4	How to Identify Potential Threats and Vulnerabilities	124
8.4.1	Slides for Disgruntled and Angry Former Employees	125
8.4.2	Slides for Social and Political Activists	126
8.4.3	Slides for Random Vandals	126
8.4.4	Slides for Professional Saboteurs	127
8.4.5	Slides for Thieves and Spies	128
8.4.6	Slides for Domestic and International Terrorists	129
8.4.7	Slides for Natural Disasters	130
8.4.8	Slides for Data Center Security	131
8.4.9	Slides for Wiring and Cabling	131
8.4.10	Slides for Remote and Mobile Computing	132
8.4.11	Slides for Desktop Computers	132
8.4.12	Slides for Department-Based Servers	133
8.4.13	Slides for Telecom and Datacom Equipment	133
8.4.14	Testing and Evaluating the Module	134
8.5	Reporting Suspicious Behavior or Security Violations	135
8.5.1	Testing and Evaluating the Module	136
8.6	What to Expect from Different Departments	136
8.6.1	Testing and Evaluating the Module	137
8.7	How the Internal Alert System Works	138
8.7.1	Testing and Evaluating the Module	139
8.8	Performing the Administrative Aspects of a Training Program	139
8.9	Action Steps to Improve Physical IT Security	140

<b>9. The Future of Physical Security for IT Assets</b>	<b>143</b>
9.1 The Impact of National Security Plans	144
9.2 The Role of ISACS	154
9.2.1 The Chemical Sector ISAC	157
9.2.2 The Electricity Sector ISAC	158
9.2.3 The Energy ISAC	159
9.2.4 The Financial Sector ISAC	160
9.2.5 The Healthcare ISAC	161
9.2.6 The Highway ISAC	161
9.2.7 The Information Technology ISAC	162
9.2.8 The Telecommunications ISAC	163
9.2.9 The Public Transit ISAC	166
9.2.10 The Water ISAC	167
9.3 Action Steps to Improve Physical IT Security	168
 <b>Appendix A: Physical Computer Security Resources</b>	 <b>169</b>
 <b>Appendix B: Physical Security Glossary and Acronyms</b>	 <b>177</b>
 <b>Appendix C: Action Step Checklists</b>	 <b>191</b>
 <b>Appendix D: Physical Security Planning Checklists</b>	 <b>199</b>
 <b>Index</b>	 <b>217</b>