Table of Contents

About the Author vii

Preface xiii

Chapter 1.0 Industrial Network Security 1
- 1.1 What Are Industrial Networks? 1
- 1.2 What Is Industrial Network Security? 2
- 1.3 The Big Picture: Critical Infrastructure Protection 4
- 1.4 The Challenge: "Open and Secure" 6
- 1.5 Who's Working on What? 7
- 1.6 Federal Regulatory Authority 9
- References 9

Chapter 2.0 A Security Backgrounder 11
- 2.1 Physical, Cyber, and Personnel Security 11
- 2.2 Risk Assessment and IT Cybersecurity 14
- 2.3 Risk Assessment for the Plant 19
- 2.4 Who's Responsible for Industrial Network Security? 21
- 2.5 Tips for Making the Business Case to Upper Management 25
- 2.6 Making the Business Case with Data 26
- References 27

Chapter 3.0 COTS and Connectivity 29
- 3.1 Use of COTS and Open Systems 29
- 3.2 Connectivity 30
- 3.3 What You Get that You Didn't Bargain For 30
- References 31

Chapter 4.0 Cybersecurity in a Nutshell 33
- 4.1 Security Is a Process 33
- 4.2 Basic Principles and Definitions 33
- 4.3 Basic Principles: Identification, Authentication, and Authorization 36
- 4.4 More Cyber Attack Case Histories 37
- 4.5 Risk Assessment and Risk Management Revisited 39

4.6 Cyber Threats 40
4.7 Vulnerabilities 40
4.8 A Common COTS Vulnerability: The Buffer Overflow 42
4.9 Attacker Tools and Techniques 44
4.10 Anatomy of the Slammer Worm 45
4.11 Who's Guarding Whom? 46
References 48

Chapter 5.0 Countermeasures 49
5.1 Balancing the Risk Equation with Countermeasures 49
5.2 The Effect of Countermeasure Use 49
5.3 Creating an Industrial Network Cyber Defense 54

Chapter 6.0 Cyberdefense Part I – Design and Planning 57
6.1 Defense in Layers 57
6.2 Access Control 62
6.3 Principle of Least Privilege 65
6.4 Network Separation 66
References 67

Chapter 7.0 Cyberdefense Part II – Technology 69
7.1 Guidance from ISA-99 TR1 69
7.2 Firewalls and Boundary Protection 70
7.3 Intrusion Detection 73
7.4 Virus Control 75
7.5 Encryption Technologies 78
7.6 Virtual Private Networks (VPNs) 85
7.7 Authentication and Authorization Technologies 87
References 91

Chapter 8.0 Cyberdefense Part III – People, Policies, and Security Assurance 93
8.1 Management Actions and Responsibility 93
8.2 Writing Effective Security Documentation 94
8.3 Awareness and Training 99
8.4 Industrial Network Security Assurance Program: Security Checklists 100
8.5 Security Assurance: Audits 102
8.6 Adding in Physical Security 103
8.7 Adding in Personnel Security 104
References 105

Chapter 9.0 New Topics in Industrial Network Security 107

9.1 Red Teaming: Test Yourself Before Adversaries Test You 107

9.2 Different Types to Answer Different Questions 108

9.3 Red Teaming Industrial Networks – Caution, It's Not the Same! 109

9.4 System Security Demands Both Physical Security and Cybersecurity 110

9.5 The Transportation Connection: Passenger Rail and Cybersecurity 111

References 113

Chapter 10.0 Defending Industrial Networks–Case Histories 115

10.1 A Large Chemical Company 115

10.2 Another Company's Story–Procter & Gamble 120

Appendix A – Acronyms 123

Index 127