THE INFORMATION SYSTEMS SECURITY OFFICER'S GUIDE

Establishing and Managing a Cyber Security Program

THIRD EDITION

DR. GERALD L.KOVACICH

Amsterdam • Boston • Heidelberg • London
New York • Oxford • Paris • San Diego
San Francisco • Singapore • Sydney • Tokyo
Butterworth-Heinemann is an imprint of Elsevier

ELSEVIER

CONTENTS

About the Author *xiii*

Preface *xvii*

Acknowledgments *xxi*

Introduction *xxiii*

Section I: The Working Environment of the Cyber Security Officer

1. Understanding the Past and Present Cyber-Information World Environment **3**

Ah, the Good 01'Days! 4

Global Information Infrastructure 10

National Information Infrastructure 11

How Did We Get from Adam to the Internet? 11

Changing Criminal Justice Systems 21

The Human Factor 24

Summary 26

2. Understanding the Past and Present Global Business and Management Environment **27**

The Changing Business and Government Environments 28

Understanding the Business Environment 31

Management Responsibilities and Communicating with Management 33

Creating a Competitive Advantage through a Cyber Security Program 39

Service, Support, and a Business Orientation 41

Business Managers and Cyber Security 42

What Company Managers Should Ask ofTheir Cyber Security Professionals 44

What Cyber Security Professionals Should Do 45

Questions to Consider 46

Summary 46

3. An Overview of Related World Views of Cyber Security **49**

Evolution of Laws, Standards, Policies, and Procedures 50

Global via the UN 51

The EU 53

Asia 53

South America 54

Africa 55
Canada 55
United States 55
Summary 61

4. A Glimpse at the History of Technology 63
What Is Technology? 64
From Cave Man to Cyber Security Professional and Information Warrior 64
Revolutions and Evolutions in High Technology 65
From the Twentieth Century to Today: Technology and the Advent of High Technology 66
The Internet 75
The High-Technology-Driven Phenomenon 78
Faster and More Massive High-Technology-Driven Communications 79
The Beneficial Effect of Hacker Tools and Other Malicious Software on Network Security with Dual Roles as Cyber Security Tools 80
Other High-Technology Tools in Cyber Security 82
Welcome to the Twenty-First-Century Technology 84
Summary 86

5. Understanding Today's Threats in the Cyber Vapor—"War Stories" from the Front Lines 89
Reported Digital Battlefield Attacks and Related Stories 90
Summary 100

Section II: The Duties and Responsibilities of a Cyber Security Officer

6. The Cyber Security Officer's Position, Duties, and Responsibilities 103
Introduction 104
The Cyber Security Officer in a Global Corporation 106
Cyber Security Officer Duties and Responsibilities 109
Goals and Objectives 109
Leadership Position 110
Vision, Mission, and Quality Statements 112
Cyber Security Principles 114
Project and Risk Management Processes 114
Cyber Security Officer and Organizational Responsibilities 115
Summary 118

7. The Cyber Security Program's Strategic, Tactical, and Annual Plans 119

Introduction 120

Corporate's Cyber Security Strategic Plan 121

Corporate's Cyber Security Tactical Plan 124

Cyber Security Annual Plan 125

Questions to Consider 128

Summary 128

8. Establishing a Cyber Security Program and Organization 131

Introduction 132

Corporate Cyber Security Program 132

Cyber Security Officer Thought Process in Establishing the Cyber Security Organization 152

Questions to Consider 172

Summary 172

9. Determining and Establishing Cyber Security Functions 175

Introduction 176

Processes 177

Valuing Information 179

International Widget Corporation (IWC) Cyber Security Program Functions Process Development 184

Cyber Security Officer's Cyber Security Program Functions 185

Access Control and Access Control Systems 187

Evaluation of All Hardware, Firmware, and Software 189

Risk Management Program 191

Security Tests and Evaluations Program 193

Noncompliance Inquiries 194

Contingency and Emergency Planning and Disaster Recovery Program 194

Questions to Consider 198

Summary 199

10. Establishing a Metrics Management System 201

Introduction 202

Metrics 1: Cyber Security Program Level of Effort Drivers—Number of Users 207

Examples of Other Metrics Charts 211

Project Management 218

Questions to Consider 221

Summary 222

11. Annual Reevaluation and Future Plans 223

Introduction 223

One-Year Review 224

Cyber Security Program Strategic, Tactical, and Annual Plans 228

Linking Cyber Security Program Accomplishments to Corporate Goals 228

Metrics Analysis 230

Planning for Next Year 231

Questions to Consider 233

Summary 234

12. High-Technology Crimes Investigative Support 235

Introduction 235

Duties and Responsibilities of a Cyber Security Officer in Deterring High-Technology Crimes 236

Assisting with Computer Forensics Support 238

Dealing with Law Enforcement 240

Questions to Consider 242

Summary 243

Section III: The Global, Professional, and Personal Challenges of a Cyber Security Officer

13. Introduction to Global Information Warfare 247

The Possibilities 248

Introduction to Warfare 250

Four Generations of Warfare 250

Introduction to Global Information Warfare 251

Information Warfare Will Hit You in Your Pocketbook 254

Business Is War 256

IW Broadly Encompasses Many Levels and Functions 257

What IW Is… and Is Not 257

Being Prepared-Bad Things Will Happen 260

The Possible Breakdowns in an Information Environment 261

Going beyond Three Blind Men Describing an Elephant: Information Warfare Terms of Reference 261

Information Warfare Is a Powerful Approach for Attaining and Maintaining a Competitive Advantage 268

How to Use IW to Achieve Goals and Objectives 269

Coherent Knowledge-Based Operations 270

Network-Centric Business 271
Knowledge Management 271
Summary 272
Note 272

14. The Cyber Security Officer and Privacy, Ethical, and Liability Issues 273

Introduction to Privacy Issues 273
Introduction to Ethics Issues 274
Codes of Ethics 277
Corporate Ethics, Standards of Conduct, Business Practices, and Corporate Values 278
Liability Issues 279
Questions to Consider 280
Summary 280

15. A Career as a Cyber Security Officer 283

Introduction 284
The Cyber Security Officer's Career Development Program 285
Education 286
Questions 300
Summary 300

16. A Look at the Possible Future 301

Surviving into the Future 303
New Old Approach to Security—Defensive Approach 304
The Changing Environment 305
The Need for Enlightened and Dedicated Leadership 305
Global Trends 306
Offensive-Defensive Cyber Attacks 310
The Future of the Internet 311
Questions 311
Summary 311

Index *313*