

CYBERSECURITY

THE ESSENTIAL BODY OF KNOWLEDGE

Dan Shoemaker, Wm. Arthur Conklin



PREPARING TOMORROW'S
INFORMATION
SECURITY
PROFESSIONALS

Contents

PREFACE	xix
CHAPTER 1	
Information Security Is Important	1
The Story Begins: Zero Hour	1
Assuring Information: Failure Is Never an Option	2
Body of Knowledge	2
Two Common Sense Assumptions for Cybersecurity	3
The Attack Builds: Hours 20 to 36	4
Instilling Order in a Virtual World	5
Coordination of Efforts and Intent	5
Information Diversity and Dispersion	6
Picking up the Pieces: Hours 36 to 72	7
Strategic Governance Processes	8
Creating a Strategic Governance Process	8
Strategic Planning and the Strategic Governance Process	8
The Story Concludes: A New Paradigm	9
A Standard Model for Ensuring Best Practice in Cybersecurity	11
The DHS Essential Body of Knowledge	11
Finding an Appropriate Model	13
The National Strategy to Secure Cyberspace	13
The National Security Professional Development Program	13
The Federal Information Security Management Act (FISMA)	14
Chapter Summary	15
Key Terms	15
Questions from the CIO	16
Hands-On Projects	17
CHAPTER 2	
A Global Roadmap for Security	19
Narrowing the Search: More Questions	19
EBK Competency Areas	21
Fifty-three Critical Work Functions	22
Fourteen Competency Areas	23
Getting Real: Focusing on Implementation	23
Roles in the EBK	24
Organization of Roles in the EBK Framework	26
Executive Roles	27
Functional Roles	27
Corollary Roles	28
Common Functions	29
The Story Continues: It's Never As Easy As It Seems	30
Converting Roles, Competencies, and Functions into an Actionable Plan	32
The Importance of Planning	33
The Story Evolves: Learning How to Make Adjustments	33

Adapting the EBK to the Actual Situation 34
 Chapter Summary 36
 Key Terms. 36
 Questions from the CIO 37
 Hands-On Projects 38

CHAPTER 3

Adapting Best Practice: Tailoring a Solution That Fits 39
 The Story Changes Venues: The Road to Singapore 39
 Walking the Talk. 41
 The Story Progresses: A New Day in Singapore 44
 Developing Solutions from the EBK. 45
 Context 45
 Scope 46
 Availability of Resources. 46
 The Singapore Team: Turning Concepts into Practice 47
 The Chief Information Security Officer 48
 Tailored Operating Procedures for the CISO Role. 49
 Wrapping Up in Singapore: Tailoring the CISO Role 51
 Example: Model EBK-Based Procedures for Two Positions 51
 Another Aspect: Tailoring a Process from Parts of Jobs. 55
 Defining Requirements for a Non-EBK Role. 57
 Chapter Summary 61
 Key Terms. 61
 Questions from the CIO 62
 Hands-On Projects 63

CHAPTER 4

Defining the Company's Executive Roles 65
 Meanwhile, Back in the States... 65
 Assigning Competencies to Roles. 67
 Assessing the Role of the Boss. 67
 Defining the Role of the Chief Information Officer 68
 The CIO and Management of Data Security 69
 The CIO and Management of Enterprise Continuity 69
 The CIO and Incident Management. 70
 The CIO and IT Training and Awareness. 70
 The CIO and Physical and Environmental Security 70
 The CIO and Management of Procurement 71
 The CIO and the Management and Evaluation of Legal, Regulatory, and
 Standards Compliance 72
 The CIO and the Management and Evaluation of Security Risk Programs 73
 The CIO and the Management of the Strategic Management Function 73
 The CIO and the Management of System and Application Security Programs 74
 Assessing the Architect's New Role 75
 Leading the Data Security Function: The Information Security Officer 76
 The Information Security Officer and the Management of Data Security. 77

The ISO and the Management and Design of Digital Forensics Programs 78

The ISO Role and the Management of Enterprise Continuity 79

The ISO and Incident Management 80

The ISO and the Management of IT Training and Awareness 80

The ISO and the Management of the Physical and Environmental Security Function 81

The ISO and the Management of Acquisitions 81

The ISO and the Management and Evaluation of Legal, Regulatory, and Standards Compliance 82

The ISO and the Management and Evaluation of Security Risk Programs 82

The ISO and the Management, Design, and Evaluation of Strategic Management Programs 83

The ISO and the Management of System and Application Security Programs 84

Ensuring the Corporate Commitment to Security: A New Breed of Security Manager 85

Enforcing the Rules: The IT Security Compliance Officer 86

 The SCO and Data Security Compliance 86

 The SCO and Compliance for Digital Forensics 87

 The SCO and the Evaluation of Enterprise Continuity for Compliance 87

 The SCO and the Evaluation of Incident Management for Compliance 88

 The SCO and the Evaluation of IT Systems Operations and Maintenance for Compliance 88

 The SCO and the Evaluation of Network and Telecommunications Security for Compliance 88

Evaluation of Personnel Security for Compliance 88

 The SCO and the Evaluation of IT Training and Awareness for Compliance 89

 The SCO and the Evaluation of Physical and Environmental Security for Compliance 89

 The SCO and the Evaluation of Procurement for Compliance 89

 The SCO and the Design, Implementation, and Evaluation of Legal, Regulatory, and Standards Compliance Processes 90

 The SCO and the Implementation and Evaluation of Security Risk Programs for Compliance 91

 The SCO and the Evaluation of Strategic Management Programs for Compliance 92

 The SCO and the Evaluation of System and Application Security Programs for Compliance 92

Chapter Summary 93

Key Terms 93

Questions from the CIO 94

Hands-On Projects 95

CHAPTER 5

Defining the Company's Functional Security Roles 97

 Building the Information Security Team 97

 The Digital Forensics Professional Role 99

 Daily Tasks 100

 Operational Duties 102

 The Digital Forensics Professional and the Assurance of the Integrity of Forensic Investigations 102

 Incident Management Controls 103

 On the Job with a Digital Forensics Professional 104

 Network and Telecommunications Security 105

 Evaluation of Procurement Processes for Forensic Concerns 105

 Risk Management Procedures 106

 Designing the Security Response: The IT Security Engineer 106

 The IT Security Engineer Role 108

 Data Security Processes 108

 IT Systems Operations and Maintenance Processes 109

 Network and Telecommunications Security Processes 111

 Risk Management Procedures for the Company 112

 System and Application Security 112

 The Perils of Day-to-Day Monitoring 114

On the Job with an IT Security Operations and Maintenance Professional	115
Data Security	115
Digital Forensics	116
Enterprise Continuity	116
Incident Management	116
Incident Response	117
Systems Operations and Maintenance	117
Network and Telecommunications	118
Operational Aspects of Procurement	119
Security Risk Programs	120
System and Application Security	120
Doing the Actual Work of Security: The IT Security Professional	120
On the Job with an IT Security Professional	121
Data Security	122
Enterprise Continuity Programs	122
Incident Management Programs	122
Security Training and Awareness Programs	123
Personnel Security Programs	123
Physical and Environmental Security Programs	124
Regulatory and Standards Compliance Process	125
Risk Management Programs	125
Chapter Summary	126
Key Terms	126
Questions from the CIO	127
Hands-On Projects	128

CHAPTER 6

Defining the Corollary Roles for Security	129
<i>Including Security Functions from Other Areas</i>	129
Ensuring the Physical Protection of Information	131
Physical Security Professional	133
The Physical Security Specialist and the Design and Implementation of Enterprise Continuity Programs	133
The Physical Security Specialist and the Implementation of Physical Security Incident Management Controls	134
The Physical Security Specialist and the Design and Evaluation of Physical Security Aspects of Personnel Security	134
The Physical Security Specialist and the Design and Evaluation of the Physical and Environmental Security Program	135
The Physical Security Specialist and the Design, Implementation, and Evaluation of Risk Management Programs	136
Keeping the Company Liability-Free	137
Privacy Professional	138
The Privacy Specialist and the Design and Evaluation of Data Security for Privacy Considerations	138
The Privacy Specialist and the Design and Evaluation of Incident Management Programs	139
The Privacy Specialist and the Design, Implementation, and Evaluation of IT Security Training and Awareness Programs	140
The Privacy Specialist and the Design and Evaluation of Personnel Security Programs to Ensure Privacy	141
The Privacy Specialist and the Management, Design, Implementation, and Evaluation of Legal, Regulatory, and Standards Compliance	141

The Privacy Specialist and the Management, Design, Implementation and Evaluation of Risk Management Programs for Privacy 142

Ensuring the Security of the Things That the Organization Buys 143

Procurement Professional 144

 The Procurement Specialist and the Management, Design, Implementation, and Evaluation of Secure Procurement Processes 144

 Procurement as a Major Organizational Function 145

Chapter Summary 145

Key Terms 146

Questions from the CIO 146

Hands-On Projects 147

CHAPTER 7

The Data Security Competency 149

 Rewinding the Story Back to the Start: Defining the Required Competencies 149

 Data Security: The Manage Function 151

 Data Security and Policy Assurance 151

 Designing an Effective Approach to Assuring Trusted Access 152

 The Identification Principle and Data Security 152

 The Authentication Principle and Data Security 153

 Ensuring Tighter Security Through Multifactor Authentication 154

 Designing Data Security into the Operation 155

 Turning Policy into Concrete Practice 156

 Factoring Risk into the Development of Policy 156

 Asset Baseline Formulation—Identifying What Has to Be Protected 157

 Understanding Priorities Through Risk Analysis 157

 Aligning Policy to Priority and Implementing Controls 157

 Ensuring Optimum Resource Allocation 158

 Classification 158

 Privilege 158

 Managing the Automated Data Security Process—Account Management 159

 Standard Models for Securing Data 160

 Criterion-Based Access Control 160

 Policy-Based Access Control 161

 Strict Control—the Mandatory Access Control Model 161

 Controlling Access Through Assignment—Discretionary Access Control 162

 Controlling Access by Type—Role-Based Access Control 163

 Data Security: The Implement Function 164

 Establishing Effective, Operational Intrusion Detection 164

 Incident Reporting and Operational Response 165

 Cryptography—Another Part of the Data Security Puzzle 165

 Keys and Algorithms 166

 Cryptography for the Masses—Public Key Infrastructures 166

 Data Security: The Evaluate Function 167

 Data Security and the Maintenance of Continuous Effectiveness 167

 The Data Security Evaluation Plan 168

 Maintaining a Record Through Status Accounting 169

 Status Accounting and the Assessment of Control Performance 169

Chapter Summary 170
Key Terms..... 170
Questions from the CIO 171
Hands-On Projects 172

CHAPTER 8

The Digital Forensics Competency 173
The CIO Gets a Monday Morning Surprise 173
Ensuring the Integrity of the Process 175
 Creating a Trustworthy and Sustainable Forensics Function..... 176
Meanwhile, Back at the Bat Cave, the Forensics People Start the Ball Rolling..... 178
 Creating a Digital Forensics Process..... 180
Putting Forensics on an Operational Footing 184
 Reconstructing Events..... 186
 Managing the Forensics Process Through Evaluation..... 188
Ensuring Correctness Through Routine Evaluations 190
Chapter Summary 190
Key Terms..... 191
Questions from the CIO 191
Hands-On Projects..... 192

CHAPTER 9

The Enterprise Continuity Competency 193
1500 Hrs. on a Wednesday Afternoon..... 193
Continuity Management: Ensuring Effective Recovery from an Adverse Event..... 194
 Friday—0900 195
Successful Preparation Is No Accident 196
 Identifying Contingencies to Address 197
 Preparedness Planning 197
 The Role of Estimation Methods and Tools in Planning 197
 Preparing and Maintaining an Effective Response..... 197
 Risk Assessment and Preparedness Planning 198
Successful Recovery Is No Walk in the Park..... 198
Anticipating Disasters 200
 Documenting a Recovery Plan..... 200
Friday 0950: The CIO Discovers the Advantages of a Solid Plan 201
 Drawing the Right Set of Assumptions..... 202
 Two Essential Factors in the Development of the Continuity Plan 203
Creating a Practical Enterprise Continuity Process..... 204
 Identification and Prioritization of Protected Functions 205
 Designing the Continuity Solution 206
 Ensuring that Everybody Knows What to Do..... 207
Friday 14:00: The Plan Gets Implemented 207
Deploying the Enterprise Continuity Process..... 208
 Ensuring Continuous Availability Through Redundancy 209
 Total Redundancy: Data Recovery Hotsites 209
 Partial Redundancy: Data Recovery Warmsites..... 210
 Simple Operational Redundancy: Data Recovery Coldsites 211

Monday 0900: The Lights Come Back On 211

Ensuring the Continuing Effectiveness of Enterprise Continuity Process 212

 Looking at the Consequences 213

 Understanding the Impact of Threats 214

Chapter Summary 214

Key Terms 215

Questions from the CIO 216

Hands-On Projects 217

CHAPTER 10

The Incident Management Competency 219

 Ensuring That the Company Dodges the Bullet 219

 Considerations in the Incident Management Process 221

 Foreseen and Unforeseen Events 221

 Keeping Watch: Monitoring and Incident Identification 221

 Getting the Incident Report to the Right People 222

 Potential Incidents and Active Incidents 222

 Establishing a Structured Response 223

 Arrayng Resources to Ensure the Right Level of Response 224

 Formulating the IRT 224

 Managing the IRT 225

 The Right Strategy Emerges 225

 Creating a Systematic Response 227

 Developing Baseline Metrics 228

 The CISO Steps up to the Plate 228

 Planning for Incident Management 229

 Making Incident Management Routine 230

 Incident Response and Data 230

 Containment Considerations—the Problem of Dependencies 231

 Automating the Incident Management Process 231

 Ensuring Consistent Execution 232

 Auditing and the Incident Management Process 232

 The Audit Function and Assessment of Performance 233

 Conducting an Audit 233

 Ensuring the Correctness of Audit Evidence 234

 Penetration Testing: A Different Type of Audit 234

 Chapter Summary 236

 Key Terms 237

 Questions from the CIO 237

 Hands-On Projects 238

CHAPTER 11

IT Security Training and Awareness 239

 The Human Factor Is Always a Problem 239

 Ensuring Secure Behavior 240

 The Broad Focus of Awareness 241

 The Narrower Focus of Training 242

 Motivating Consistent Performance 242

- Building a Knowledgeable Workforce 243**
- Designing the Training and Awareness Program 245**
 - Routine Tasks 246
 - Operational Duties 246
 - Management Practice 246
- Training and Awareness: A Constant Evolution 246**
 - Who Receives Training? 247
 - The Role of Discipline 247
 - The Role of Knowledge and Capability 247
 - Data and Feedback. 248
 - Ensuring Disciplined Practice. 248
- Moving the Training Function up the Ladder of Success 249**
 - Determining the Actual Training Needs 250
- Implementing a Capability Maturity Process. 250**
 - Recognition 250
 - Informal Practice 252
 - Security Management 252
 - Deliberate Control 253
- Ensuring Continuous Effectiveness 255**
- Establishing an Effective Review Process 255**
 - Defining and Enforcing Proper Procedure. 256
- Ensuring that the Training Process Is Sustainable 257**
 - Improving the Process Through Assessment 257
 - Review Data as an Organizational Resource. 258
- Chapter Summary 258**
- Key Terms. 258**
- Questions from the CIO 259**
- Hands-On Projects 260**

CHAPTER 12

- Securing the IT Systems Operations and Maintenance Function 261**
 - Getting the Concept into Practice 261
 - Establishing a Coherent Process: Strategic Planning. 263**
 - Implementing the Process: The Operational Security Plan 264
 - Designing the Operational Security Function 265**
 - Designing a Controls Framework 268
 - Human Factors: Ensuring Proper Performance 269
 - Technology: Ensuring Proper Support 270
 - Establishing Reliable Day-to-Day Security 270**
 - Turning Operational Security into a Process 272
 - Implementing the Security of Operations Process. 273
 - Identifying and Reporting Incidents 273
 - Performing an Effective Analysis 274
 - Maintaining Operational Capability. 277**
 - Evaluating Everyday Risk 279
 - Ensuring a Secure Architecture 280
 - Management Data and the Security of Operations Function. 281
- Chapter Summary 281**
- Key Terms. 282**

Questions from the CIO 282
 Hands-On Projects 283

CHAPTER 13

Network and Telecommunications Security 285
 Back in Familiar Territory 285
 Creating a Managed Network 288
 Acceptable Use Policies 288
 Remote Access Policies 288
 Network Security Control Policies 289
 Culture Always Comes First 290
 Defining the Boundaries of Trust 292
 Policy Development for Network Components 292
 Policy Development and the Secure Network Design 293
 Putting the Pieces Together 294
 Implementing the Network Security Function 296
 Network Security Devices: The Firewall 297
 Software-Based IDSs 298
 Staying on Top of Change 300
 Ensuring the Security Is Always Up to Date 301
 Attacking Your Own Network 301
 Read Your Security Audit Reports 302
 Chapter Summary 302
 Key Terms 303
 Questions from the CIO 303
 Hands-On Projects 304

CHAPTER 14

Personnel Security 305
 The People Problem 305
 Planning for Personnel Security 307
 Defining the Boundaries of Control 308
 Identifying Personnel Security Functions Based on Risk 309
 Ensuring Reliable Behavior 309
 Managing Change to the Workforce 309
 Documenting the Personnel Security Function 310
 The Special Situation of Contractors 311
 Making Personnel Security Real 311
 Screening and Hiring Personnel 312
 Job Definition: Building Security In 313
 Background Screening and Hiring 314
 The Special Circumstance of Clearance Levels 314
 Managing the Personnel Security Process 314
 Defining the Principles of Control 315
 Implementing the Personnel Security Process 316
 Practical Considerations for Implementing Security 317
 Implementing Trust Through the Screening Process 318
 Workforce Training and Education 318
 Keeping Identities Up to Date 319
 Personnel Changes 319

Evaluating the Success of the Process 321
 Evaluating Formal Codes of Conduct 322
 Personnel Reviews 322
Chapter Summary 323
Key Terms 324
Questions from the CIO 324
Hands-On Projects 325

CHAPTER 15

Physical Security. 327
 Bridging the Great Divide 327
 The Physical Security Plan 329
 Defining Protected Space 330
 The Physical Security Process 331
 Physical Security Threat Assessments 332
 Designing for Physical Protection 333
 Incorporating Physical Security into the Information Protection Scheme 334
 Threat Identification and Strategy 335
 Maintaining Secure Access 336
 Establishing the Right Internal Countermeasures 336
 Ensuring Against Malicious Actions in the Secure Space 337
 Understanding the Variables in Physical Access Control 338
 Meshing the Controls with the Plan 340
 Implementing the Measures to Control Access 340
 Perimeter Controls: Barriers 341
 Perimeter Controls: Locks 342
 Intrusion Detection in the Physical Space 342
 Evaluating the Physical Security Process 343
 How to Measure Success – Conventionally and Otherwise 344
 Chapter Summary 345
 Key Terms 346
 Questions from the CIO 347
 Hands-On Projects 348

CHAPTER 16

Procurement. 349
 Surviving the Supply Chain 349
 Making the Business and Assurance Case 352
 Factoring Risk into the Process 353
 Developing the Request for Proposals 353
 Selecting the Right Supplier 354
 Developing the Procurement Plan 354
 Designing an Effective Procurement System 356
 Incorporating Security into the Process 357
 Understanding the Constraints 358
 Formulating the Contract 358
 Administering the Contract 359

Implementing Effective Supply Chains 360

Developing the Assurance Framework 362

 Using Standard Assessment to Identify Trusted Suppliers 364

 Evaluating Capability: Defining the Process Dimension 364

 Evaluating Performance: the Capability Dimension 364

Evaluating the Procurement Process 365

Types of Reviews 366

 The Security Review Process 367

 Launching the Security Review Program 367

Chapter Summary 368

Key Terms 369

Questions from the CIO 370

Hands-On Projects 371

CHAPTER 17

Legal and Regulatory Compliance 373

 The CEO Learns the Facts of Life 373

 Compliance and Coordination 375

 Building Management Control 376

 The Need for a Comprehensive Approach 376

 Planning for Control 377

 Control Objectives and Procedures 377

 Sorting Out Complexity in Compliance Management 378

 Developing Meaningful Metrics 378

 The Compliance Officer Goes for a Run 380

 Designing from Policy to Practice 381

 Tailoring Compliance 382

 Defining Concrete Policies 382

 Refining Control Statements 383

 An Example of the Functional Decomposition Process 383

 Documenting Work Practices 383

 The Compliance Officer Gets up Early 384

 Finding Out What You Need to Have 386

 Step One: Control Environment 386

 Step Two: Assessment of Risks 388

 Step Three: Instituting the Proper Controls 388

 Step Four: Assessing the Effectiveness of the Control Set 389

 Step Five: Documenting the Finished Product 389

 The Compliance Officer Gets a New Job 390

 Evaluation Programs and Compliance 391

 Audits and Enforcement 392

 Managing and Improving the Compliance Process 392

 Critical Success Factors 393

 Chapter Summary 394

 Key Terms 395

 Questions from the CIO 395

 Hands-On Projects 396

CHAPTER 18

The Risk Management Competency 397

- The CEO Gets Nervous 397
- Ensuring That Risk Management Supports Business Goals 399
 - The Risk Management Plan 399
 - Implementing a Managed Process 400
 - Risk-Handling Strategies 401
 - Setting Up the Risk Management Planning Process 402
- The CISO Designs a Castle. 404
- The Coordinated Approach to Risk Management 405
 - Risk Management Planning and Risk Assessments 406
 - Conducting a Risk Assessment in Support of Planning 407
 - Designing for Effective Risk Management 407
 - Risk Management Controls. 409
- Implementing Risk Management 410
- Targeting the Security Controls 412
 - Modeling Risks for Prioritization. 413
 - Measuring the Risk Management Process. 414
- The CISO and His Team Go All-In 414
- Risk Management and Operational Evaluation of Change 416
 - Evaluating the Overall Guidance 417
 - Program Management Review 418
- Chapter Summary 419
- Key Terms 420
- Questions from the CIO 420
- Hands-On Projects 421

CHAPTER 19

Strategic Management 423

- Looking at the Long Term 423
- Keeping the Process Coherent 425
 - Ensuring Cooperation Across Functions 426
 - Creating a Strategic Management Model 426
 - Organizing for Proper Alignment. 427
 - Thinking Through What to Protect 427
 - Integrating Cultures as Well as Process 428
- Designing for Governance. 429
- Establishing Control 431
 - Governance Structures 432
 - Developing a Governance Process 432
 - Planning for Governance. 433
 - A Framework for Strategic Management 434
- Ensuring the Strategic Perspective 435
- Control Objectives and Business Goals 436
 - Defining Control Objectives 436
 - Steps to Evaluate Control 436
 - The Details of Implementation. 438
- Making Strategy Quantitative 439
- Making Informed Decisions 440

Ensuring Performance 441
 Evolving the Organization 442
 Assessing Organizational Capability 442
 Chapter Summary 443
 Key Terms 444
 Questions from the CIO 444
 Hands-On Projects 445

CHAPTER 20

System and Application Security 447
 Conflicts Happen 447
 Security in the Lifecycle 450
 Adopting a Top-Down Perspective 451
 Measurement against Benchmarks 452
 Identifying and Judging Risks 452
 Eliminating Hidden Problems 452
 Aligning Processes 453
 Ensuring Better Resource Allocation 453
 The CISO Plans an Attack 454
 Security Policies and Design 456
 Building the Operational Framework 456
 Coordination of the Process and Planning For Security 457
 The CISO Takes a Meeting 460
 Implementing the Process 461
 Human Considerations 462
 Establishing the Overall Operation 462
 Launching the Program 463
 Establishing the Application and System Security Plan 464
 Application and System Security Product Assurance 464
 Application and System Security Process Assurance 465
 Creating an Information-Based Management Process 465
 Monitoring Security Status 466
 Launching a Comprehensive Evaluation Process 467
 Implementing the Process 467
 Assurance of Process 470
 Getting the Participants on the Same Page 471
 Scheduling and Holding Joint Reviews 472
 Project Status Monitoring 473
 Chapter Summary 473
 Key Terms 474
 Questions from the CIO 474
 Hands-On Projects 475

APPENDIX A

Operating Scenario: Humongous Holdings 477

GLOSSARY 485

INDEX 493