

Contents

Foreword	xxv
Chapter 1 IT Security Project Management Building Blocks	1
Introduction	2
Corporate Security Project Plan Components	3
The True Cost of Security	4
Prevention vs. Remediation	6
Potential Economic Impact	8
Business Exposure	11
Cost of Security	12
ROI of Security	14
Project Success Factors	15
Success Factor 1: Executive Support	15
Success Factor 2: User Involvement	17
Success Factor 3: Experienced Project Manager	17
Success Factor 4: Clearly Defined Project Objectives	18
Success Factor 5: Clearly Defined (and Smaller) Scope	19
Success Factor 6: Shorter Schedules, Multiple Milestones	19
Success Factor 7: Clearly Defined	
Project Management Process	20
Success Factor 8: Standard Infrastructure	20
Project Constraints	21
Corporate Strategy and IT Security	23
How Corporate Culture and Policies Impact IT Security	24
Summary	26
Solutions Fast Track	27

Chapter 2 Defining the Security Project	31
Introduction	32
Defining the Security Problem	32
Network Security and the CIA	33
Confidentiality	33
Integrity	34
Availability	34
CIA in Context	34
Define the Problem	36
Defining the Outcome	37
Defining Potential Security Project Solutions	38
Defining the Optimal Security Project Solution	39
Applying Security Project Constraints	40
Scope (Amount of Work)	40
Time (Schedule)	41
Cost	42
Quality	42
Developing the Security Project Proposal	44
Identifying the Security Project Sponsor	45
Summary	47
Solutions Fast Track	47
Chapter 3 Organizing the IT Security Project	51
Introduction	52
Identifying the IT Security Project Team	52
Identifying IT Security Project Stakeholders	53
Defining IT Security Project Requirements	55
Defining IT Security Project Objectives	59
Defining IT Security Project Processes	61
Acceptance Criteria	62
Risk Management	62
Change Management	63
Communication	65
Quality	65
Status Reporting	66
Defect, Error, and Issue Tracking	66
Escalation Procedures	67
Documentation Procedures	67

Approval Procedures68
Deployment69
Operations69
Training70
Summary71
Solutions Fast Track71
Chapter 4 Building Quality Into IT Security Projects . . .	75
Introduction76
Planning IT Security Project Quality76
User Requirements78
Functional Requirements79
Technical Requirements81
Acceptance Criteria81
Quality Metrics82
Change Management Procedures84
Standard Operating Procedures84
Monitoring IT Security Project Quality85
Testing IT Security Project Quality88
Summary90
Solutions Fast Track91
Chapter 5 Forming the IT Security Project Team	95
Introduction96
Identifying IT Security Project Team Requirements96
Roles and Responsibilities97
Competencies100
Technical101
Communication102
Training102
Negotiation103
Translating Technical Language103
Reporting104
Legal, Financial, and Regulatory104
Identifying Staffing Requirements and Constraints105
Acquiring the Needed Staff107
Forming the IT Security Project Team108
Identify Training Needs109

Team Processes and Procedures 109
Team Kick-off Meeting 111
Summary 113
Solutions Fast Track 114

Chapter 6 Planning The IT Security Project 117

Introduction 118
Creating the IT Security Project Work Breakdown Structure 118
Defining Project Tasks and Sub-tasks 121
Checking Project Scope 123
Developing Task Details 125
 Owner 126
 Resources 127
 Completion Criteria 128
 Schedule 129
 Budget 130
 Dependencies 130
 Constraints 131
 Expertise 132
 Tools 132
 Budget 132
 Organizational Change 133
 Governmental or Regulatory Requirements 134
 Lessons Learned 135
Identifying and Working With the Critical Path 135
Testing IT Security Project Results 136
Budget, Schedule, Risks, and Communications 138
 Budget 138
 Schedule 139
 Risks 140
 Communications 140
Summary 142
Solutions Fast Track 143

Chapter 7 Managing the IT Security Project 147

Introduction 148
Initiating the IT Security Project 148
Monitoring and Managing IT Security Project Progress . . 149
 Task Progress 151

Completion Criteria Example – Strong Passwords . . .	152
Project Progress	154
Issues Reporting and Resolution	155
Documentation	156
Monitoring IT Security Project Risk	157
Managing IT Security Project Change	158
Key Stakeholder Change	158
Key Staff Change	160
Key Environmental Change	160
Testing IT Security Project Results	161
Summary	164
Solutions Fast Track	165
Chapter 8 Closing Out the IT Security Project.	169
Introduction	170
Evaluating Project Completion	170
Closing Issues Log, Change Requests, and Error Reports . .	172
Preparing for Implementation, Deployment, and Operational Transfer	173
Preparing for Implementation	174
Preparing for Deployment	175
Preparing for Operational Transfer	176
Reviewing Lessons Learned	178
Documentation and Compliance Reports	181
Summary	185
Solutions Fast Track	186
Chapter 9 Corporate IT Security Project Plan	189
Introduction	190
Defining Your Security Strategy	190
Legal Standards Relevant to Corporate IT Security	192
Selected Federal Laws	194
Gramm–Leach–Bliley Act	194
Health Insurance Portability and Accountability Act	195
Sarbanes–Oxley Act	197
Federal Information Security and Management Act	197
FERPA and the TEACH Act	198
Electronic Communications Privacy Act and Computer Fraud and Abuse Act	199

State Laws200
Unauthorized Access200
Enforcement Actions201
Three Fatal Fallacies202
The “Single Law” Fallacy202
The Private Entity Fallacy203
The “Penetration Test Only” Fallacy203
Do It Right or Bet the Company:	
Tools to Mitigate Legal Liability204
We Did our Best; What’s the Problem?204
What Can Be Done?206
Understand Your Legal Environment207
Comprehensive and Ongoing Security Assessments, Evaluations, and Implementation207
Use Contracts to Define Rights and Protect Information208
Use Qualified Third-party Professionals209
Making Sure Your Standards-of-Care	
Assessments Keep Up with Evolving Law209
Plan for the Worst210
Insurance211
Corporate IT Security Project Plan Overview212
Corporate Security Auditing215
Choosing A Target216
Why Security Fails218
Improper Configuration218
Failure to Update219
Faulty Requirements219
Human Factors220
Policy Issues221
Incorrect Assumptions222
Corporate IT Security Project Parameters224
Project Objectives224
Project Parameters225
Scope225
Schedule227

Budget	228
Quality	229
Requirements	230
Key Skills Needed	231
Operating System Skills	233
Network Skills	233
Application Skills	234
Security Tools Skills	234
Programming Skills—Compiled Languages	235
Programming Skills - Scripting Languages	235
Key Personnel Needed	236
Project Processes and Procedures	237
Project Work Breakdown Structure	239
WBS Example 1	239
Work Breakdown Structure Example 2	240
Project Risks	245
Project Constraints	247
Project Assumptions	248
Project Schedule and Budget	248
Managing the Project	252
Closing Out the Project	252
Summary	254
Solutions Fast Track	255
Chapter 10 General IT Security Plan	261
Introduction	262
IT Security Assessment and Auditing	262
Perimeter or Boundaries	265
Internal Network	266
Servers and Hosts	266
Applications and Databases	266
Data	267
Contact Information	267
Business Information	268
Extranet and Remote Access	268
Valid User Accounts	268
System Configuration	269
Types of Security Assessments	269

Vulnerability Scanning	270
Pen Testing	272
Risk Assessment	274
Risk Assessment: Asset Protection	275
Risk Assessment: Threat Prevention	279
Risk Assessment: Legal Liabilities	286
Risk Assessment: Costs	288
Impact Analysis	293
Public Access Networks	295
Legal Implications	296
Authentication	298
Access Control	302
Physical Access to Equipment	302
Local Access to Network	303
Remote Access to Network	303
Auditing	304
Policy Review	304
Physical	305
Technical	305
Administrative	308
Process and Procedure Review	308
Operational Review	309
Legal and Reporting Requirements	309
Attacks	310
Non-intrusive Attacks	310
Intrusive Attacks	312
Assessment and Audit Report	315
Elements of a Findings Report	316
Defining the Steps Taken	316
Defining the Vulnerability or Weakness	317
Defining the Criticality of Findings	317
Defining Mitigation Plans	318
Defining Owners, Timelines, and Deliverables	318
Format of a Findings Report	319
Project Plan	320
Project Problem Statement	320
Problem Mission Statement	321

Project Objectives	321
Potential Solutions	322
Selected Solution	324
General IT Security Project Parameters	325
Requirements	325
Types of Requirements	326
Project Specific Requirements	326
Scope	327
Schedule	329
Budget	330
Quality	330
Key Skills Needed	331
Technical Skills	331
Non-Technical Skills	332
Key Personnel Needed	332
Form the Project Team	333
Project Processes and Procedures	333
General IT Security Project Plan	334
Project WBS	335
Project Risks	336
Project Constraints	336
Project Assumptions	337
Project Schedule and Budget	337
Summary	339
Solutions Fast Track	339
Chapter 11 IT Infrastructure Security Plan	345
Introduction	346
Infrastructure Security Assessment	346
Internal Environment	348
Information Criticality	348
Impact Analysis	349
System Definitions	350
Information Flow	350
Scope	351
People and Process	351
User Profiles	352
Policies and Procedures	353
Organizational Needs	353

Regulatory/Compliance	354
Technology	355
Establishing Baselines	356
Addressing Risks to the Corporate Network	356
External Environment	359
Threats	360
Recognizing External Threats	362
Top 20 Threats	367
Network Security Checklist	369
Devices and Media	370
Topologies	371
Intrusion Detection Systems/ Intrusion Prevention Systems (IDS/IPS)	374
System Hardening	380
Other Infrastructure Issues	381
Other Network Components:	
Routers, Switches, RAS, NMS, IDS	382
Network	383
External Communications (also see “Remote Access”)	384
TCP/IP (Some TCP/IP Information Also Found in the “Routers” Section)	385
Administration	388
Network Management	392
Routers and Routing	398
Firewall	401
Intrusion Detection/Intrusion Prevention	404
Remote Access	405
Project Parameters	408
Requirements	409
Functional Requirements	410
Technical Requirements	410
Legal/Compliance Requirements	412
Policy Requirements	412
Scope	413
Schedule	413
Budget	414
Quality	415
Key Skills Needed	415

Key Personnel Needed	417
Project Processes and Procedures	418
Project Team	419
Project Organization	420
Project Work Breakdown Structure	420
Project Risks and Mitigation Strategies	427
Project Constraints and Assumptions	429
Project Schedule and Budget	431
IT Infrastructure Security Project Outline	432
Summary	434
Solutions Fast Track	435
Chapter 12 Wireless Security Project Plan	441
Introduction	442
Wireless Security Auditing	443
Types of Wireless Network Components and Devices	445
Wireless Technologies	448
Types of Threats	449
War Dialing, Demon Dialing, Carrier Signal Scanning	450
Wardriving, NetStumbling, or Stumbling	452
Bluetooth Attacks	459
Risk Assessment	463
Asset Protection	464
Threat Prevention	469
Legal Liabilities	479
Costs	480
Impact Analysis	483
Wireless Security Project Parameters	485
Requirements	486
Functional Requirements	487
Technical Requirements	488
Legal/Compliance Requirements	490
Policy Requirements	491
Scope	492
Schedule	493
Budget	494
Quality	495
Key Skills Needed	497
Key Personnel Needed	499

Project Processes and Procedures	499
Project Team	500
Project Organization	501
Project Work Breakdown Structure	502
Project Risks	506
Project Constraints and Assumptions	507
Project Schedule and Budget	508
Wireless Security Project Outline	509
Summary	510
Solutions Fast Track	512
Chapter 13 IT Operational Security Plan	517
Introduction	518
Operational Security Assessment	519
Incident response	521
Company-Wide Incident Response Teams	523
Response Team Services	525
Response Team Assessment	529
Security Management Services	529
Risk Analysis	530
Trend Analysis	530
Disaster Planning	530
Education and Awareness	531
Policies	537
Founding Principles of a Good Security Policy	538
Understanding Current Policy Standards	539
Creating Corporate Security Policies	542
Policy Distribution and Education	552
Maintaining Corporate Security Policies	553
Disaster Recovery	554
Facilities	556
Operations	556
Information and Communications	557
Business Insurance	558
Regulatory Issues	559
Health Insurance Portability and Accountability Act	561
Gramm-Leach-Bliley Act	562
Sarbanes-Oxley Act	563

Project Parameters565

 Problem566

 Mission/Outcome567

 Solution567

 Scope568

 Cost569

 Time569

 Quality570

 Functional Requirements571

 Technical Requirements572

 Legal/Compliance Requirements574

 Success Factors574

 Required Skills574

 Personnel Needed575

 Project Processes and Procedures576

Project Team577

Project Organization578

Project Work Breakdown Structure579

Project Risks and Mitigation Strategies584

 Incident response584

 Policy management585

 Disaster planning585

 Regulatory/compliance585

Project Constraints and Assumptions586

Project Schedule and Budget586

IT Operational Security Project Outline587

Summary590

Solutions Fast Track591

 Operational Security Assessment591

 Project Parameters593

 Project Team593

 Project Organization593

 Project Work Breakdown Structure594

 Project Risks and Mitigation Strategies594

 Project Constraints and Assumptions594

 Project Schedule and Budget595

Index.....597