

CONTENTS

List of Figures	xiii
Preface	xv
1. Introduction	1
Strategy Overview	1
Strategy and Information Technology	2
Strategy and Information Security	2
An Information Security Strategic Planning Methodology	4
The Business Environment	4
Information Value	5
Risk	5
The Strategic Planning Process	6
The Technology Plan	6
The Management Plan	6
Theory and Practice	7
2. Developing an Information Security Strategy	9
Overview	9
An Information Security Strategy Development Methodology	10
Strategy Prerequisites	11
Research Sources	12
Preliminary Development	18
Formal Project Introduction	18
Fact Finding	18
General Background Information	19
Documentation Review	19
Interviews	20
Surveys	22
Research Sources	23
Analysis Methods	23
Strengths, Weaknesses, Opportunities, and Threats	24
Business Systems Planning	25
Life-Cycle Methods	27
Critical Success Factors	28
	v

vi CONTENTS

Economic Analysis	29
Risk Analysis	31
Benchmarks and Best Practices	32
Compliance Requirements	33
Analysis Focus Areas	34
Industry Environment	35
Organizational Mission and Goals	35
Executive Governance	36
Management Systems and Controls	36
Information Technology Management	37
Information Technology Architecture	39
Security Management	40
Draft Plan Presentation	42
Final Plan Presentation	43
Options for Plan Development	44
A Plan Outline	45
Selling the Strategy	47
Plan Maintenance	49
The Security Assessment and the Security Strategy	49
Strategy Implementation:	51
What is a Tactical Plan?	52
Converting Strategic goals to Tactical Plans	52
Turning Tactical Planning Outcomes into Ongoing Operations	53
Key Points	53
Plan Outline	56
3. The Technology Strategy	59
Thinking About Technology	59
Planning Technology Implementation	61
Technology Forecasting	62
Some Basic Advice	66
Technology Life-Cycle Models	68
Technology Solution Evaluation	69
Role of Analysts	70
Technology Strategy Components:	72
The Security Strategy Technical Architecture	73
Leveraging Existing Vendors	76
Legacy Technology	77
The Management Dimension	78
Overall Technical Design	79
The Logical Technology Architecture	82
Specific Technical Components	84
Servers	84
Network Zones	85

External Network Connections	86
Desktop Systems	86
Applications and DBMS	88
Portable Computing Devices	90
Telephone Systems	91
Control Devices	92
Intelligent Peripherals	93
Facility Security Systems	94
Security Management Systems	96
Key Points	100
4. The Management Strategy	109
Control Systems	111
Control Systems and the Information Security Strategy	113
Governance	116
Ensuring IT Governance	117
IT Governance Models	118
Current Issues in Governance	120
Control Objectives for Information and Related Technology (CobiT)	121
IT Balanced Scorecard	121
Governance in Information Security	122
End-User Role	123
An IT Management Model for Information Security	124
Policies, Procedures, and Standards	131
Assigning Information Security Responsibilities	134
To Whom Should Information Security Report?	135
Executive Roles	136
Organizational Interfaces	138
Information Security Staff Structure	141
Staffing and Funding Levels	142
Managing Vendors	146
Organizational Culture and Legitimacy	149
Training and Awareness	152
Key Points	153
5. Case Studies	155
Case Study 1—Singles Opportunity Services	155
Background	155
Developing the Strategic Plan	157
Information Value Analysis	158
Risk Analysis	159
Technology Strategy	161
Management Strategy	162
Implementation	164

viii CONTENTS

Case Study 2—Rancho Nachos Mosquito Abatement District	166
Background	166
Developing the Strategic Plan	168
Information Value Analysis	169
Risk Analysis	170
Technology Strategy	171
Management Strategy	172
Implementation	173
Key Points	174
6. Business and IT Strategy:	175
Introduction	175
Strategy and Systems of Management	176
Business Strategy Models	178
Boston Consulting Group Business Matrix	178
Michael Porter—Competitive Advantage.	181
Business Process Reengineering	183
The Strategy of No Strategy	185
IT Strategy	190
Nolan/Gibson Stages of Growth	191
Information Engineering	194
Rockart's Critical Success Factors	198
IBM Business System Planning (BSP)	199
So is IT really "strategic"?	201
IT Strategy and Information Security Strategy	202
Key Points	203
7. Information Economics	205
Concepts of Information Protection	205
Information Ownership	208
From Ownership to Asset	211
Information Economics and Information Security	214
Basic Economic Principles	215
Why is Information Economics Difficult?	219
Information Value—Reducing Uncertainty	220
Information Value—Improved Business Processes	223
Information Security Investment Economics	224
The Economic Cost of Security Failures	225
Future Directions in Information Economics	227
Information Management Accounting—Return on Investment	228
Economic Models and Management Decision Making	229
Information Protection or Information Stewardship?	231
Key Points	232

8. Risk Analysis	235
Compliance Versus Risk Approaches	235
The “Classic” Risk Analysis Model	240
Newer Risk Models	243
Process-Oriented Risk Models	243
Tree-Based Risk Models	245
Organizational Risk Cultures	247
Risk Averse, Risk Neutral, and Risk Taking Organizations	248
Strategic Versus Tactical Risk Analysis	254
When Compliance-based Models are Appropriate	255
Risk Mitigation	256
Key Points	257
Notes and References	259
Index	265

