

# Contents

<b>1 Vulnerabilities, Threats and Risks in IT .....</b>	<b>1</b>
Foundational Concepts.....	1
1.1 Three Definitions: Vulnerability, Threat and Risk.....	1
1.2 Examples of Threats, Vulnerabilities and Risks .....	2
1.3 Impact and Probability Graph.....	4
1.4 Risk and Active and Passive Voices in Grammar .....	4
1.5 Internal and External Elements in a Risk.....	5
Information Risk Management Theory.....	6
1.6 Information Properties .....	6
1.7 Risk Management Activities.....	6
1.7.1 Risk Assessment .....	7
1.7.2 Risk Mitigation .....	7
1.7.3 Risk Acceptance.....	7
1.7.4 Risk Communication .....	8
1.8 Risk Management: Example Number 1.....	8
1.8.1 Risk Assessment .....	8
1.8.2 Risk Mitigation .....	8
1.8.3 Risk Acceptance.....	9
1.8.4 Risk Communication .....	9
1.9 Risk Management: Example Number 2.....	9
1.9.1 Risk Assessment .....	9
1.9.2 Risk Mitigation .....	10
1.9.3 Risk Acceptance.....	10
1.9.4 Risk Communication .....	10
Appetite for IT Risk: Let the Business Lead .....	11
1.10 IT Security Getting Close to Reality.....	11
1.11 IT Provides Solutions to the Business .....	12
1.12 IT Provides Secure Solutions to the Business.....	12
1.13 How to Derive Appetite for IT Risk From Management Decisions .....	13
1.14 Risk Perception by Human Beings .....	14

Where to Focus: Business Value of IT Security .....	15
1.15 How to Keep IT Security Work Real by Avoiding Doomsday Tellers and Collecting News .....	15
1.16 Profit to Risk Ratio .....	17
1.17 Smart Selection of Risks to Mitigate Following the Pareto Principle in IT Security .....	18
1.18 How to Spend Resources Wisely and Transparently: Reputation and Emotions .....	19
1.19 No Business Value Without Business Knowledge .....	20
1.20 Smart Behaviour for IT Security Practitioners .....	20
Link to MBA Management Models .....	21
<b>2 Security and IT Background</b> .....	23
Professional Outlook and Profiles for IT Security .....	23
2.1 IT Security Workforce .....	24
2.2 Basic IT Security Profiles .....	24
2.3 Extended IT Security Profiles .....	25
2.3.1 Technical IT Security Profiles .....	25
2.3.2 IT Security Governance Related Profiles .....	26
2.3.3 Provision of IT Security Expert Advice .....	27
2.3.4 IT Security Marketing .....	27
2.4 The Coordinator, the Facilitator and the Trainee .....	27
Skills and Backgrounds for Team Members .....	30
2.5 Technical Skills .....	30
2.6 Soft Skills .....	32
2.7 Possible Backgrounds Present in the Team .....	35
Security Studies .....	36
2.8 Engineering or Management .....	36
2.9 Alternative Paths to Obtain IT Security Expertise .....	37
2.10 What to Study .....	38
Link to MBA Management Models .....	41
<b>3 The Team–Individual Contract</b> .....	43
How to Create Win-Win Deals on the Team–Individual Contract .....	43
3.1 Contract Between the Team and the Team Member .....	44
3.2 Basic Terms and Conditions of the Agreement: Creating a Team’s Culture .....	44
3.3 What Is Motivation? Herzberg and Maslow .....	46
3.4 Internal Balance in Human Beings .....	48
3.4.1 The Work Dimension .....	49
3.4.2 The Social Dimension .....	49
3.4.3 The Personal/Spiritual Dimension .....	49
3.5 Identification of Internal Balance Coordinates .....	50
3.5.1 The Work Dimension .....	50
3.5.2 The Social Dimension .....	52
3.5.3 The Spiritual Dimension .....	52

Behavioural Guidelines for Team Leaders.....	53
3.6 Communication, Communication and Communication .....	54
3.7 Time Availability for the Team .....	55
3.8 Adoption of Preventive Measures for the Team.....	55
3.9 Proposal of Mentoring Services.....	56
3.10 Care but No Intervention.....	56
3.11 Design of Easy Processes and Assignment to Wise People .....	57
3.12 Public Praise Sessions and Private Criticism .....	58
3.13 Support of Team Members.....	58
Resourcing the Team.....	59
3.14 New Team Members Joining the Team.....	59
3.15 Profile Preparation for a New Team Member .....	60
3.16 Advertising the Vacancy .....	60
3.17 Assessing Applications: Three Basic Principles.....	60
3.18 Preparing the Selection Process .....	61
3.19 Elements of the Selection Process .....	62
3.19.1 Day 1 Test: Phone Interview .....	62
3.19.2 Day 2 Test: Tests and Face to Face Interview .....	64
3.20 How to Say Goodbye to the Team .....	65
Link to MBA Management Models .....	66
<b>4 What to Do: The IT Security Roadmap.....</b>	<b>67</b>
Founding Activities on Principles.....	68
4.1 IT Security Teams Should Not Occupy Their Days Mostly with “Fire Alerts” .....	68
4.2 Basic Security Principles: The Foundation of the IT Security Activities.....	68
4.2.1 Defence in Depth .....	69
4.2.2 Protection of the Crown Jewels.....	69
4.3 Additional Security Principles .....	70
4.3.1 Least Business Privilege Required.....	71
4.3.2 Segregation of Duties .....	71
4.3.3 Four-Eye Principle .....	72
4.4 Software Development Security Principles .....	72
Stock-Taking Exercise and Prioritisation.....	73
4.5 Vulnerability Analysis: Inventory Exercise .....	73
4.5.1 Planning .....	74
4.5.2 Information Gathering/Discovery .....	74
4.5.3 Vulnerability Identification/Attack .....	75
4.5.4 Reporting.....	75
4.6 Threat Analysis: Military Strategy Revisited.....	75
4.7 How to Set Priorities .....	76
Provision of Security Services .....	79
4.8 Security Services.....	79
4.9 How to Build the To-Do List .....	80

4.9.1	Networks .....	80
4.9.2	Data .....	81
4.9.3	Systems .....	81
4.9.4	Applications .....	82
4.9.5	Identities .....	82
4.10	IT Security Specialities: Teams Within the Team .....	83
4.10.1	The Red Team: Security Testing and Incident Response .....	83
4.10.2	The Blue Team: Identity and Access Management .....	84
4.10.3	The Green Team: Security Device Administration and Monitoring .....	85
4.10.4	The Yellow Team: Security Governance, Compliance and User Awareness .....	86
4.10.5	The White Team: Changing Security .....	86
4.11	Activities That an IT Security Team Should Avoid .....	87
	Link to MBA Management Models .....	89
<b>5</b>	<b>How to Do It: Organise the Work in “Baby Steps” .....</b>	<b>91</b>
	Shaping the Daily Reality .....	92
5.1	Threats to the Performance of the Team .....	92
5.1.1	Service Requests .....	92
5.1.2	Organisational Confusion (Politics) .....	93
5.1.3	Time Thieves .....	93
5.2	Plan in “SMALL Baby Steps” .....	94
5.2.1	Every Trip Starts with a First Step .....	94
5.3	Baby Step Assignment Within the Team .....	96
5.4	Responsibility Transfer .....	97
5.5	How to Plan the Team’s Time .....	98
5.6	Compulsory Ingredients for the Planning .....	99
5.7	Multiple Tasks at One Time .....	100
5.8	Finalising Baby Steps .....	100
5.8.1	Provision of “IT Security Win Rides” .....	100
5.8.2	Increase in Levels of Self-management and Independence .....	100
5.8.3	Increasing Comfort Levels .....	101
	Managing Expectations .....	101
5.9	Stakeholder Analysis .....	101
5.9.1	Top Senior Management .....	102
5.9.2	Line Management .....	102
5.9.3	Business Areas .....	102
5.9.4	Final Users .....	103
5.9.5	Other IT Teams in the Organisation .....	103
5.9.6	IT Security Teams Members .....	104
5.9.7	IT Security Team Members’ Social Circles .....	104
5.10	How to Communicate with Stakeholders .....	105

Managing Activities.....	106
5.11 How to Report Activity Progress.....	106
5.12 How to Track Activities Internally.....	107
5.12.1 The Morning Gathering .....	107
5.12.2 Online Weekly Reporting.....	107
5.13 External Deadlines .....	108
5.14 How to Invite Team Members to Perform New “Baby Steps” .....	108
5.15 How to Deal with Red Tape .....	109
5.16 Basic Communication Tools for the Team and the Organisation .....	110
Link to MBA Management Models .....	111
<b>6 Team Dynamics: Building a “Human System” .....</b>	<b>113</b>
The IT Security Paradox .....	114
6.1 Traits of the IT Security Profession .....	114
6.1.1 Passion .....	114
6.1.2 Heterogeneous Background .....	114
6.1.3 Brief History .....	115
6.1.4 Continuous Change.....	115
6.1.5 Hacking Comes From Curiosity .....	115
6.2 How to Build the IT Security Castle.....	116
6.2.1 Archers Ready to Battle from the Battlements .....	116
6.2.2 The Keepers of the Gatehouse .....	118
6.2.3 The Drawbridge .....	120
Interaction Patterns Within the Team.....	122
6.3 Technical Versus Non-technical Mini-teams Within the Team.....	122
6.4 The Guru Working with the Non-gurus .....	123
6.5 Tasks for the User Access Administration Team Members .....	124
6.5.1 Juniors Run the Identity Shop.....	124
6.5.2 Release Skilled Members from Identity Management Tasks.....	125
Life Always Finds Its Way: Working in the Organisation .....	125
6.6 How Team Members Deal with Problems: Using the Socratic Way.....	125
6.7 How to Manage Working Time.....	126
6.8 How to Fine Tune the “Human System”.....	128
6.8.1 Task Rotation .....	128
6.8.2 Trial and Error.....	128
6.8.3 Competition in the Team.....	129
6.8.4 Types of Contracts in the Team.....	129
Team Member Development and Appraisal .....	130
6.9 Training Measures.....	130
6.9.1 On-the-Job Training .....	130
6.9.2 Certified Trainings .....	131

6.9.3	Security Conferences .....	131
6.9.4	Product-Related Trainings .....	132
6.10	Appraising Team Members.....	132
6.10.1	Performance Planning .....	132
6.10.2	Supporting Performance .....	132
6.10.3	Reviewing Performance .....	133
	Link to MBA Management Models .....	134
	Link to Nature Management Models .....	135
<b>7</b>	<b>Viral Marketing.....</b>	<b>137</b>
	Communication to Sell IT Security Services.....	138
7.1	Why Should IT Security Teams Communicate?.....	138
7.2	To Whom Should the Team Communicate? Their Audience: Their Stakeholders .....	138
7.2.1	Top Senior Management .....	139
7.2.2	Line Management .....	139
7.2.3	Business Areas and Final Users .....	139
7.2.4	IT Teams in the Organisation .....	139
7.3	Communication Principles to Follow .....	141
7.4	What Should the IT Security Team Communicate?.....	141
	From Raising Awareness to Marketing IT Security.....	142
7.5	Characteristics of Services: From Awareness to Marketing.....	143
7.6	The Extended “Marketing Mix” for IT Security.....	143
7.6.1	Product/Service .....	144
7.6.2	Price .....	144
7.6.3	Place .....	145
7.6.4	Promotion.....	145
7.6.5	Physical Evidence .....	146
7.6.6	The Emergency Room Effect.....	147
7.6.7	Processes .....	147
7.6.8	People.....	148
7.6.9	Power to the Users .....	148
7.7	How to Position the IT Security Team.....	148
7.7.1	The Market.....	148
7.8	Viral IT Security Marketing.....	150
7.9	An IT Security Viral Marketing Example: Identifying Socially Connected Colleagues.....	151
7.10	The Role of the Incident Response Team in Guerrilla Marketing .....	152
	Security Stories to Sell and Human Psychology Aspects.....	153
7.11	The Security Stories.....	153
7.11.1	Stories for End Users .....	153
7.11.2	How to Approach the Elaboration of Security Policies .....	154

7.11.3	Stories for Managers .....	155
7.11.4	Stories for Other IT Teams.....	155
7.12	Behavioural Economics to Consider When Marketing IT Security .....	155
7.12.1	Decisions, Cheating and Ethics.....	155
7.12.2	Subjective Expectations About Money and Prices .....	157
	Link to MBA Management Models .....	158
<b>8</b>	<b>Management Support: An Indispensable Ingredient .....</b>	<b>161</b>
	Executives in Organisations Need to Manage Risks of Different Nature.....	162
8.1	Managers: Decisive Stakeholders of the IT Security Team .....	162
8.2	Risk Management Could Become a Management Innovation.....	163
8.3	Risk Sources and Risk Types Affecting the Organisation .....	164
	Two Risk Containers: Operational and Enterprise Risk Management .....	166
8.4	Operational Risk .....	166
8.5	Enterprise Risk Management: A New Dimension of Risk as an Opportunity .....	167
	A Model to Understand Risks and a Decalogue to Work with Managers.....	168
8.6	The “Risk House” Model: How Executives Can Treat Risks .....	168
8.6.1	The Risk Management Block.....	169
8.6.2	The Information Block.....	169
8.7	The Ten Commandments to Transform Executives into Our Best Allies .....	170
	Link to MBA Management Models .....	173
<b>9</b>	<b>Social Networking for IT Security Professionals .....</b>	<b>175</b>
	Human Beings Are Social Beings.....	176
9.1	Reasons for Networking in IT Security .....	176
9.1.1	Quicker Way to Learn New Tendencies.....	176
9.1.2	Easier Way to Understand Society .....	176
9.1.3	Open Door for Future Professional Changes .....	176
9.2	Social Networking Foundations for IT Security: The “Spiral of New Value” .....	177
9.2.1	When Professionals Share Information, They Create Value.....	177
9.2.2	Networking Requires Time .....	177
9.2.3	The Significance of People and Not Organisational Charts.....	177
9.2.4	A Smile Can Take IT Security Far Far Away.....	178
	Networking Inside the Organisation .....	180

9.3	Targets for the Networking Efforts of the IT Security Team .....	180
9.3.1	IT Security Customers .....	180
9.3.2	Other IT Teams .....	181
9.3.3	Security Colleagues in the IT Security Team.....	181
9.4	Locations to Practice Networking.....	182
9.4.1	Common Use Facilities .....	182
9.4.2	Meetings with Business Areas .....	182
9.4.3	Any Interaction with Customers Is a Potential Opportunity .....	183
9.5	How to Proceed with Networking.....	183
	Networking Outside the Organisation.....	184
9.6	The IT Security Community .....	185
9.6.1	The IT Security Community in the Same Industry .....	185
9.6.2	How to Share Security-Related Information When Networking .....	185
9.6.3	The IT Security Community Working in Different Industries .....	186
9.7	Examples of IT Security Fora .....	186
9.7.1	IT Security Governance-Related Networking Possibilities .....	187
9.7.2	Technical IT Security Related Networking Possibilities .....	188
9.7.3	Worldwide Known IT Security Conferences .....	189
9.8	How to Network with Academia: Schools and Universities.....	192
9.9	How to Network with Law Enforcement Agencies .....	193
9.10	How to Network in the Local Community.....	193
	Networking for the Personal IT Security Brand .....	195
9.11	Networking to Increase the Value of the IT Security Professional .....	195
9.11.1	Small and Medium Enterprises (SMEs) Demand IT Security Services .....	195
9.11.2	Big Corporations Focus on Their Core Business and Outsource Support Functions.....	196
9.12	How to Build IT Security Reputation .....	197
9.12.1	Provision of Value to the IT Security Community.....	197
9.12.2	Provision of Value to the IT Management Community.....	199
9.13	Recommendations to Build an IT Security Personal Brand .....	199
9.13.1	Security by Default Does Not Mean Social Isolation.....	199
9.13.2	Modesty and Honesty.....	199
9.13.3	Preparation for the Unknown .....	200
9.13.4	The Company of Better People .....	200
9.13.5	A Permanent Ambassador Role .....	201
	Link to MBA Management Models .....	203



<b>10 Present, Future and Beauty of IT Security .....</b>	<b>205</b>
The Present of IT Security .....	206
10.1 The Relevance of IT Security Now .....	206
10.1.1 First Worldwide Reactions .....	207
10.2 IT Security in Small and Medium Enterprises .....	209
10.3 The Attackers' Industry .....	211
10.3.1 IT Technical Experts .....	212
10.3.2 Fraud Brains .....	212
10.3.3 Internet Mules .....	212
10.4 IT Security Information Analysis .....	213
The Future of IT Security .....	213
10.5 The Emergence of Complexity .....	214
10.5.1 Code Complexity .....	214
10.5.2 Complexity in the User Interface .....	215
10.6 A Possible Filtering Mechanism: Reputation Scores .....	216
10.7 The Death of Personal Privacy .....	217
10.7.1 Internet-Based Intelligence Collection .....	217
10.8 Critical Infrastructure Protection .....	218
10.9 Change of the Security Paradigm: From an Onion to an Onion Ring .....	219
10.9.1 Multi-organisational Value Chains .....	219
10.9.2 Labour Market Events .....	219
10.10 IT Security for Virtual IT and for "The Cloud" .....	220
10.10.1 Virtualisation .....	220
10.10.2 Virtual IT Infrastructure Services: Cloud Computing .....	220
10.11 Mobile IT Security .....	221
10.12 Additional Leads on the Future of IT Security .....	222
10.12.1 Expert Forensic and Legal Support .....	222
10.12.2 The Importance of Laziness and Logs .....	223
10.12.3 Risk Management and Decision Making .....	223
10.12.4 IT Security and the Threat of Compliance .....	224
The Beauty of IT Security. An Attractive Field to Work In .....	224
10.13 Creativity in the Social Realm of IT Security .....	224
10.13.1 IT Security Creativity for Human Groups .....	224
10.13.2 Creativity for IT Security Professionals .....	227
10.14 Creativity in the Technical Arena of IT Security .....	227
10.14.1 Cyberwar Weapons .....	227
10.14.2 Digital Security Ants .....	228
Link to MBA Management Models .....	230
 <b>Annex 1. Example of an Information Security Test .....</b>	 <b>231</b>
 <b>Annex 2. Security Incident News Example .....</b>	 <b>235</b>

**Annex 3. IT Security Starter Kit ..... 237**

**Index of MBA Models Referenced at the End of Every Chapter ..... 239**

**References ..... 241**

**Index..... 245**

IT Security Management

IT Securiteers - Setting up an IT Security Function

Partida, A.; Andina, D.

2010, XXXV, 247 p., Hardcover

ISBN: 978-90-481-8881-9