

IT Security Management

Lecture Notes in Electrical Engineering

Volume 61

For other titles published in this series, go to
www.springer.com/series/7818

Alberto Partida • Diego Andina

IT Security Management

IT Securiteers - Setting up an IT Security
Function

Alberto Partida
Information Security Expert
GIAC, CEH, CISSP, CISA, CGEIT, MBA
Technical University of Madrid
Universidad Politécnica de Madrid (UPM)
Spain
apartidar@gmail.com
securityandrisk.blogspot.com

Diego Andina
Grupo de Automatización en Señal y
Comunicaciones
Technical University of Madrid
Universidad Politécnica de Madrid (UPM)
Spain
andina@gc.ssr.upm.es

ISBN 978-90-481-8881-9 e-ISBN 978-90-481-8882-6
DOI 10.1007/978-90-481-8882-6
Springer Dordrecht Heidelberg London New York

Library of Congress Control Number: 2010928831

© Springer Science+Business Media B.V. 2010

No part of this work may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, microfilming, recording or otherwise, without written permission from the Publisher, with the exception of any material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work.

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

There are costs and risks to a program of action, but they are far less than the long-range risks and costs of comfortable inaction.

John F. Kennedy, 1961–1963

...the only asset that is undervalued these days in world economy is risk...

Robert Rubin, 2006

Information security is based on outsmarting the other (the dark ;-) side

Alberto Partida, 2008

Acknowledgments

To:

My best half and my beloved editor, Raquel

My mentors in life, my parents, my brother

My mentors in my study life, Diego and Jean-Nöel

My mentors in my working life, Santiago, Carlos, Luis, Fernando, Jan and Dominique

My team colleagues at work

My friends

About the Authors

Alberto Partida is a M.Sc. graduate in telecommunication engineering by Universidad Politécnica de Madrid (UPM), specialised in computer science and IT security. He started in IT security in 1996 as a student preparing his dissertation in the group for Automation in Signals and Communications at UPM, led by Diego Andina. Since 1998, his professional experience covers network, system, application and business process security. Alberto currently provides his expertise to international organisations, coordinating a team of IT and Security experts focused on an IT risk reduction approach within the technology and organisational realm. He also teaches IT and IT security to pre-graduates in a French University. Alberto is a member of the SANS GIAC Advisory Board. He holds CEH, CISA, CISSP, CGEIT, Gold GSEC, Gold GCFW, Gold GCFA, GCIA and GREM GIAC certifications and he has finished his MBA at Henley Business School, ranked in the world's top 15 schools by The Economist MBA ranking. Alberto can be contacted through his blog at securityandrisk.blogspot.com.

Professor Diego Andina was born in Madrid, Spain, received simultaneously two master degrees, on computer science and on communications by the Universidad Politécnica de Madrid (Technical University of Madrid, UPM), Spain, in 1990, and the Ph.D. degree in 1995. He works for UPM where he heads the Group for Automation in Signals and Communications (GASC/UPM). He is author or co-author of more than 200 national and international publications, being director of more than 50 R&D projects financed by National Government, European Commission or private institutions and firms. He is also an associate editorial member of several international journals and transactions and has participated in the organization of more than 50 international events. Diego is co-author of the book "Computational Intelligence for Engineering and Manufacturing" (2007) published by Springer. He is a computational intelligence researcher and an educational innovation expert. In the past, he has worked as a consultant at Andersen Consulting and he was a lieutenant in charge of the Security Office at the Spanish Air Force.

Foreword

In 1862, the gardener James Bateman sent several specimens of the Christmas orchid to Charles Darwin. This orchid was first planted in Britain in 1855 and it did not blossom until 1857. It had been discovered several decades before by the French botanist Louis-Marie Aubert du Petit-Thouars in Madagascar in 1822. The most significant aspect of this flower is the length of its spur. It measures 20–35 cm from the tip to the lip of the flower.

In 1862, Charles Darwin published his book titled “Fertilization of Orchids”, where he predicted that there should be a moth with a proboscis of a similar size. Darwin knew that the Christmas orchid should be pollinated by a moth with a proboscis that could get to the bottom of the flower given that the nectar is stored in the lower 5 cm of its tubular spur. There should be a moth with a proboscis of a similar length, able to reach the nectar from the outside of the flower.

At that time, the reaction in the scientific community was not welcoming. Darwin had to endure some teasing. No one had ever discovered a moth with a two-handspan proboscis.

The moth that pollinates the Christmas orchid was discovered later on in Madagascar in 1903 and it had, indeed, a 25–30 cm long proboscis. It was baptised with the name of “*Xanthopan morganii praedicta*”. The qualifier “*praedicta*” refers to the prediction made by Darwin. We had to wait for the arrival of the 21st century for it to be filmed in action for the first time.

How could Darwin be sure of the existence of that moth? Would it not be possible that another type of insect was responsible for this orchid’s pollination? For Darwin, the reasoning was simple. Tubular flowers of pale or white colours that open at night belong to the floral syndrome called *sphinxophilia*. Such flowers are usually pollinated by *sphinginae* (sphinx moths). These moths have a very long proboscis and obtain nectar while in flight over the flower, similar to what hummingbirds do. That is, sphinxophilias are pollinated by sphinginae. If a sphinxophilia has a 35 cm long spur and the nectar is located in its lower 5 cm, there must be a sphinginae with a 30 cm long proboscis. Simple. Forty-one years passed by until that sphinx moth was discovered and 140 years until it was filmed.

More striking than no one else having this idea before is the fact that scientists contemporary to Darwin did not believe him. Darwin predicted shockingly the

existence of an animal, unknown until then, by simply using the logic of the evolution of species.

Daniel Hunt Janzen states for the first time in 1980 his “theory of co-evolution”. According to it, evolutionary changes that occur in a species are the answer to the selection process that another species makes, whose result transforms into a process of mutual adaptation with the first species. Each one makes the other evolve. This concept can be applied to symbiotic and parasitic relationships, pollination and to the relationship between hunter and prey.

The Christmas orchid and its moth have become one of the most used examples of co-evolution. Let’s go back in time and think of the early days of the relationship between the flower and the moth, when co-evolution began to take shape.

The spur of the flower measured 10 cm and moths’ proboscis reached 5 cm. Moths with a 5.1 cm long proboscis had more chances to survive because they could access food that individuals with a 4.9 cm long proboscis did not reach. Furthermore, moths with a 5.1 cm long proboscis specialised in taking the nectar of orchids with a 10.1 cm long spur and exchanged pollen with specimens having a just over 10 cm long spur, since there were more competitors fighting to land on flowers with a just under 10 cm long spur. This situation promoted the genetic exchange between moths with large proboscis, making each new generation grow in length. You can imagine the rest of the story. Thousands of years later, Darwin managed to predict the existence of the moth by looking only at the flower, and 118 years later Janzen came to explain his theory of co-evolution.

Alberto and Diego have captured in this book some ideas derived from co-evolution applied to the organization of Security in Information Systems.

The application of co-evolution is of interest to us, obviously, not the one that occurs between a flower and a moth, but the one happening among people. We apply the principles of co-evolution to four organisational aspects:

- The first point focuses on the relative speed at which evolution must occur. Leigh Van Valen developed a principle within the co-evolution theory known as the “Red Queen hypothesis”, referring to the Red Queen that appears in Lewis Carroll’s book “Alice in Wonderland”, who states that “you cannot stop running to continue in the same place”. From the co-evolution viewpoint, this principle is often expressed as “for an evolutionary system, continuous improvement is necessary, at least, to maintain adjustment with respect to the systems with which it is co-evolving”. We must transform and evolve at the speed of change of our ecosystem. Not slower or faster.
- The second aspect has to do with what we provide to the process of co-evolution, and what we obtain from it. If we wish for a Christmas orchid to blossom, a fundamental step is to find a moth with a 30 cm long proboscis. If we, as IT security executives, need to patch systems ad-hoc in less than 12 h, the key is not to confront IT operations colleagues with an order. A smarter way may be to achieve a specific budget so that a technical unit can always perform that patching job on demand when required. If we wish for Christmas orchids to blossom, a fundamental step is to find moths with a 30 cm long proboscis.

- The third organisational topic deals with the realistic speed at which we can perform the process of co-evolution. We will start with moths with 5 cm long proboscis. Although the goal is to reach moths with 30 cm long proboscis, the first step will be to strive for a 5.1 cm long proboscis. Transformation in cultural and organisational processes needs to occur gradually and steadily. If we aim to perform a process that currently takes 1 week in just 1 h, a first real success will be to run it in less than 48 h. Only then we will be able to start thinking of reducing the time required for it to less than 6 h. The fundamental tenet is to improve and to start moving towards the target. Most of the times, we will only know the speed we can attain once we have started our journey.
- The fourth and final aspect upon co-evolution refers to the mandate of IT security officers to provide security enhancements to the organisation. This is their contribution to the co-evolution process. However, it is not exclusive to them. If IT security executives fail in fulfilling their mandate, other players will do it for the mere survival of the business.

These foundational recommendations, not only to Information Systems Security, but to any human organization, can be summarised in the following sentences:

- We need to change at the same speed and in sync with our ecosystem. If our environment is re-organised, we should re-organise in the same direction and with the same intensity.
- We should work to reach objectives and not worry about who owns the means to achieve them.
- Determination, patience and perseverance. Every day, we must make our human environment one step closer to achieving the objective.
- We must be the shift lever in our area of expertise, otherwise leadership will naturally disappear.

Santiago Moral

Chief Information Security Officer at BBVA Bank

BBVA Bank ranks in listings such as Fortune 500, S&P 500, and Dow Jones

Contents

1	Vulnerabilities, Threats and Risks in IT	1
	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
2 Security and IT Background	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
3 The Team–Individual Contract	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
4 What to Do: The IT Security Roadmap.....	67
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
5	How to Do It: Organise the Work in “Baby Steps”	91
	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
6 Team Dynamics: Building a “Human System”	113
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
7	Viral Marketing.....	137
	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
8	Management Support: An Indispensable Ingredient	161
	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
9	Social Networking for IT Security Professionals	175
	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

10 Present, Future and Beauty of IT Security	205
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
 Annex 1. Example of an Information Security Test	 231
 Annex 2. Security Incident News Example	 235

Annex 3. IT Security Starter Kit 237

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

References 241

Index..... 245

Audience of This Book

Any fluent English reader can read this book and probably they will find useful tips even if they are far away from practising IT security but close to creating or coordinating a team. Nevertheless, the authors target three clusters of readers:

- IT security professionals, especially those recently entrusted with the daunting task of creating an IT security function, and a team, within an organisation or as an independent entity providing services to different customers.¹
- Chief Officers in organisations considering, making or supporting the decision to create an IT security team.
- IT and IT security pre-graduates or graduates with the intention to take part in the challenging experience of working in IT security.

¹Although we mostly consider in the book the case of a team within an organisation, teams located in firms that provide managed security services to customer organisations can also benefit from this book.

IT Securiteers – Setting up an IT Security Team

The Human and Technical Dimension Working for the Organisation

Current corporate governance regulations and international standards lead many organisations, big and small, to the creation of an information technology (IT) security function in their organisational chart or to the acquisition of services from the IT security industry.

More often than desired, these teams are only useful for companies' executives to tick the corresponding box in a certification process, be it ISO, ITIL, PCI, etc. Many IT security teams do not provide business value to their company. They fail to really protect the organisation from the increasing number of threats targeting its information systems.

This book provides an insight into how to create and grow a team of passionate IT Security professionals. We will call them “securiteers”.¹ They will add value to the business, improving the information security stance of organisations.

Chapters Overview

This book is broken down into the following chapters:

1. Vulnerabilities, Threats and Risks in IT

First, we define and explain what are vulnerabilities, threats and risks using industry standards. Contrary to the initial belief, these concepts are not well and broadly understood and not applied in IT security systematically. Second, we propose an approach to provide IT security that brings value to the business based on the organisation's IT risk appetite.

¹More about the term “securiteers” on Section 2.7.

2. Security and IT Background

The demand of IT security experts is high. This means that not all team members will have an IT security background. Probably some of them will come from other fields, inside or outside IT. Team leaders need to make a strength out of this initial weakness. We highlight how security teams benefit from enrolling developers, script-authors and attentive-to-detail individuals with a drive for achievement. IT security is a relatively new vocation. We also provide input about what and where to study, both in the technical hands-on and the theoretical analytical dimensions.

3. The Team–Individual Contract

Motivation is an inner driving force. Motivating team members is a pre-requisite for the performance of the team. Some elements need to be present but they will not create additional motivation, these are the hygienic factors. On the contrary, motivating factors, also known as motivators, are not always present. When they are, they are different for each team member. Every individual has three dimensions (spiritual, social, professional), which need to be in balance. The team will require everyone's skills and sometimes passion. How to achieve something that cannot be imposed? The key is in the team leader. We propose leaders to let people leave and create a daily scenario that is appealing to work and to grow professionally for current and new team members.

4. What to Do: The IT Security Roadmap

What to do day by day? IT security experts tend to become firemen. This is a reality they need to avoid. "IT securiteers" should base their activities on proven security principles. A threat and a vulnerability analysis will help the team to prioritise their activities. Our proposal is to package security activities as services. A to-do list will call for the creation of specialised mini-teams within the team. Finally, we also refer to some activities an IT security team should not embark on.

5. How to Do It: Organise the Work in "Baby Steps"

How can the team organise the IT security work? We propose the concept of performing "small baby steps" that follow the "underpromise and overdeliver" premise. We perform an analysis of the threats that can affect the team and we recommend planning some "unplanned time" and to avoid individual multitasking. We continue with proposals on how to assign activities, stressing the importance of quality assurance and deadlines. Later on, we suggest how to track and report activities together with how to communicate the team's activities based on a stakeholder analysis.

6. Team Dynamics: Building a "Human System"

Every activity starts with an emotion. We first describe the traits of the IT security profession and we present the main role that the "team board" will play building a "human-based protection system" for the organisation. We then proceed to discuss typical interaction patterns occurring within the team, e.g. how technical and non-technical colleagues interact. We present useful tips to sustain the "human

system” in the team and, finally, we conclude with our view on training and appraisal methods.

7. Viral Marketing

How can customers become the implementation engine of IT security services? In this chapter we justify why and how the team need to sell their products, which are mainly services. We base our proposal on the stakeholder analysis we performed in Chapter 5. We provide some communication principles and we link them with marketing elements as the “extended marketing mix” for IT security. We position the team ready to shift from traditional security awareness campaigns to a more comprehensive viral marketing activity. Even the incident response team could perform punctually some guerrilla marketing. We finalise the chapter with an introduction to the “security stories” the team need to sell and with some observations on human psychology that they need to consider in their security actions to increase success rates.

8. Management Support: An Indispensable Ingredient

Management support needs to be present in the air that any IT security team breathe. However, this air is difficult to find and to keep. In this chapter, we propose that IT security help executives achieving innovations related to risk management. We justify why management support and sponsorship is so crucial for risk management using current risk-related literature. We proceed with an enumeration of existing risk sources and risk types and we include an introduction to operational risk and enterprise risk management. Afterwards, we propose a basic model, “the risk house model” to understand how risks affect organisations and the role of committed management. Finally, we suggest a decalogue for IT security professionals and managers to work in harmony.

9. Social Networking for IT Security Professionals

Networking is a fundamental element for any IT security professional: It opens the door to tendencies, to understand society and to prepare for future professional changes. It requires time and effort but it has the potential to create value for all parties involved. IT security professionals should network both inside and outside the organisation where they provide their services. In this chapter, we present elements of the IT security community such as the most relevant fora and conferences. We also suggest ways to network with academia, physical security colleagues, law enforcement agents and local communities. Finally, we deal with the concept of the personal IT security brand, an asset that the IT security professional needs to actively look after and to grow. They need to provide value to the IT security community and to the market so that they can enjoy a future-proof career.

10. Present, Future and Beauty of IT Security

Digital infrastructures constitute already a relevant strategic and economic asset. States start to launch technical and legal measures to protect them. The digital world is also highly attractive for fraudsters, since the profit to risk ratio (PRR) is

high. We highlight a new and promising market for IT security professionals: The introduction of IT security in small and medium enterprises (SMEs). Subsequently, we mention technical and social trends that will be key for IT security in the coming decade (the emergence of complexity, reputation scores, the death of privacy, the role of IT systems in critical infrastructures, the paradigm change from “an onion” to an “onion ring”, virtualisation, security in “the cloud”, mobile security, micro risk management, the threat of compliance, the potential application to IT security of neuroscience studies and creativity in the technical IT security arena). The journey will not be easy but it will be an exciting lifetime experience.

All chapters incorporate a final section titled “Link to MBA Management Models”. In that section, we provide leads to models that have deserved careful attention in MBA syllabus. They are powerful instruments that can help the reader to manage complexity in IT security.

List of Tables

Table 2.1	Basic division of profiles in the IT security team
Table 2.2	Division of profiles in the IT security team
Table 4.1	Allocation of profiles in the mini-teams within the IT security team
Table 8.1	Management roles before, during and after the implementation of risk management in the organisation

List of Images

- Image 1.1** False impression of security. Closing the gap
Image 1.2 Different organisations have different appetites for IT risk
Image 1.3 Public information displays have already been hacked. What about if someone modifies the display showing the leaving times of the trains in a train station?
- Image 2.1** The IT security leader's goal: orchestrating security
Image 2.2 Leading and coordinating, but not micro-managing
Image 2.3 Time management, a skill not to take for granted
Image 2.4 Building the foundations of security
- Image 3.1** A basic contract will set the team member in motion
Image 3.2 Knowing what motivates the team member opens a window of opportunity
Image 3.3 Leaders need to locate every member in the team's map
Image 3.4 Leaders need to monitor closely their team
Image 3.5 Professional paths are inextricable
- Image 4.1** The onion approach: different layers to defend the "crown jewels"
Image 4.2 Critical actions require different players working together
Image 4.3 IT security should keep complexity away: it is the gate to encounter risks
Image 4.4 What cannot be measured, cannot be managed
Image 4.5 Business users need the right tools
Image 4.6 Change management is a keystone in IT
- Image 5.1** The team need to enjoy the reality they create
Image 5.2 The team base their plan on "baby steps"
Image 5.3 Team members need to close doors before they open new ones
Image 5.4 Everyone in the team should share the load of bureaucracy

- Image 6.1** Building the IT security castle
- Image 6.2** The “gatehouse keeper” checks who joins the team
- Image 6.3** Team leaders need to keep the team in contact with reality
- Image 6.4** IT security teams require result-based control towers
-
- Image 7.1** Security should explain why, not scare
- Image 7.2** Users will understand risks only by experimenting themselves
- Image 7.3** IT security facilities can be a marketing element
- Image 7.4** Security should take note of how human beings tick
-
- Image 8.1** People and technology: two sources of risk
- Image 8.2** IT security guide executives through the risk labyrinth
-
- Image 9.1** Positive emotions facilitate human relationships
- Image 9.2** Face to face interactions build stronger links
- Image 9.3** Networking is like grapes that produce good wine, they need care and attention since day 1
- Image 9.4** The personal IT security brand is a treasure to look after
-
- Image 10.1** IT security professionals need to guide small enterprises in the digital world
- Image 10.2** IT security should not be complex for the user
- Image 10.3** The gate for IT “securiteers” to the 21st century IT security
-
- Image A1** On the top of a waterfall

List of Figures

- Fig. 1.1** Impact probability-graph
- Fig. 1.2** A risk consists of a threat agent taking the chance of a vulnerability
- Fig. 4.1** Priority setting. First step
- Fig. 4.2** Priority setting. Second step
- Fig. 4.3** Priority setting. Third and fourth steps
- Fig. 5.1** Stakeholder analysis and suggested movement direction
- Fig. 6.1** A fact-based result-oriented performance management model
- Fig. 8.1** The “risk house” model
- Fig. 10.1** Every new version of MS Windows has more lines of code than the previous one
- Fig. 10.2** The number of lines also increase in Debian Linux

