LECTURE NOTES IN ELECTRICAL ENGINEERING | 61

Alberto Partida Diego Andina

IT Security Management

IT Securiteers – Setting up an IT Security Function

Springer

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

Springer

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

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

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.

[1] Although 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.

[1] More 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

List of Images

List of Figures

Chapter 1
Vulnerabilities, Threats and Risks in IT

Chapter 1: What will the reader learn?

This chapter answers the following questions:

- What is a risk, a threat and a vulnerability?
- How can IT security professionals describe a risk?
- What is an information risk management methodology?
- How can an IT security team use it? Two telling examples.
- How can an IT security team provide advice in an organisation?
- What is the organisation's IT risk appetite?
- Which risk management strategy should an IT security team follow?
- Smart moves on IT security.

In this initial part of the first chapter we define and explain, with the help of two very different examples, the three most important risk foundational concepts together with an introduction on present information risk management methodologies and their common steps.

Foundational Concepts

1.1 Three Definitions: Vulnerability, Threat and Risk

The International Standards Organisation, ISO,[1] defines risk as "***the combination of the probability of an event to happen and its consequence***", with no positive or negative connotation. However, most of the times the concept of risk contains

[1] ISO (2002), pp. 1–16.

A. Partida and D. Andina, *IT Security Management: IT Securiteers - Setting up an IT Security Function*, Lecture Notes in Electrical Engineering 61,
DOI 10.1007/978-90-481-8882-6_1, © Springer Science+Business Media B.V. 2010

a negative meaning in the sense of an undesired effect. We define risk using two familiar and adjacent concepts: Vulnerability and threat.

A ***vulnerability*** is "a flaw or weakness in a system, in a procedure, in a design, in an entity, in an implementation, or in an internal control that could be exercised (accidentally triggered or intentionally exploited) by a threat and result in a security breach or violation of the system's security."[2]

A ***threat*** is "a potential cause of an incident that may result in harm to a system or organisation."[3] Threats normally require an active subject to materialise the damage, the ***threat agent***.

A ***risk***, in its usually negative connotation, appears when a given threat materialises, makes use of a vulnerability and produces an undesired effect.

This may be a surprise for the reader, but it is common to find difficulties to distinguish between these three concepts: Vulnerabilities, threats and risks. The difference probably blurs due to colloquial language, where it is frequent to exchange them, e.g. "Alice is a risk for the company" or "Alice is a threat to the company" or "system X constitutes a risk (or a threat) for the company. These concepts are related but they are not exchangeable. We focus first on key aspects of their definition to be able to differentiate them through a couple of examples.

1.2 Examples of Threats, Vulnerabilities and Risks

A ***vulnerability*** is an ***internal property of the system*** we are focusing on, the same way it is its colour, size or level of hardness.

Example number 1: In the children's tale of the three little pigs, the first little pig builds a house out of straw. The wolf blows it down and eats the little pig. The house made of straw had the vulnerability of being made of such a light material that it could be blown away, leaving the little pig unprotected.

Example number 2: We propose to imagine a meeting room, located within a company's facilities, where a laptop is connected to their corporate network. The laptop presents the user log-in screen. It is attached to the meeting table with a security steel cable (locked with a four-figure combination lock). One vulnerability in this laptop could be that someone could boot it from the CD drive using a live CD.[4] This way, they could have IP connectivity, and therefore, initial access to the corporate local network.

---

[2]Adapted from NIST (2002a), pp. 1–F1.

[3]ISO (2004), pp. 1–28.

[4]A live CD is a CD-ROM with a self-contained operating system, usually a flavour of Linux, which provides an almost fully-fledged operating system platform from where to work on regardless of the operating system installed on the computer's hard disk (e.g. Backtrack, Ophcrack, Helix, Ubuntu). See a list of live Linux CDs at http://www.livecdlist.com. Last accessed 8-11-2009.

In both examples, the described vulnerability alone, a house made only of straw and an unattended laptop connected to a corporate network, do not create an incident by itself. There is always the need for an external subject to take advantage of the vulnerability to provoke a specific incident. This is the threat agent or, simply, the threat.

A ***threat implies an action*** originated by a party, external to the system that is the subject of analysis, i.e. an active subject or agent exercising an action on it. In the example number 1, the threat is someone, the wolf, getting close to the house and blowing to tear down the little pig's house. The wolf is a ***threat agent***. In our example number 2, a threat is then someone sneaking into the meeting room and booting the laptop from a live CD that they could carry to obtain access to the corporate network.

Once the internal nature of a vulnerability and the external subject nature of a threat are explained, the concept of risk is straightforward. ***Risk*** is composed of two elements: The conjunction of a given threat exercising a vulnerability. The image of ***a threat making use of a vulnerability*** and producing a normally undesired event is essential to understand the notion of risk. The probability of this event happening and its impact describe the risk (typically graded as simply as high, medium or low).

In the first example, the conjunction of a house made out of straw (vulnerability) and a wolf willing to blow the house away (threat) constitutes a risk for the little pig. The risk is that the little pig loses its house and the wolf eats the little pig. The answers to the following three questions facilitate the description of risks and their subsequent communication to key stakeholders:

- What can happen? (Description of the potential incident)
- How can it happen?
- When and why can it happen?

Following up with the second example, someone booting up the laptop from a live CD and accessing the corporate network constitutes a risk. But, somehow, this is a generic risk and this was coming from our original, pretty undetermined, threat. This is the way we can get confused with the concept of risk. To avoid this confusion, we need to continue specifying the scenario, e.g. someone accessing the network and causing a denial of service to one of the company servers. This starts to be a more specific and understandable risk.

With these simple examples, we show one of the difficulties present in risk assessment: Frequently, IT security professionals deliver generic statements in their risk analysis. In our first example, the risks mentioned are descriptive enough.[5] However, in our second example, the risk was "someone accessing the network". What does this mean? Implicitly, this could mean a lot to an IT savvy person but a decision-maker in the company will probably not grasp all the consequences of this network access. ***The more specific the description of the risk, the easier the risk assessment will be understood***.

[5] The piglet could lose its house and its life.

We suggest, therefore, that IT security professionals should complement risk descriptions with real details about the risk scenario. The application of this statement to the second example would be: Someone accesses the network using IT tools that are easily available and produces a denial of service to the internal email server, leaving users in the organisations with no email service for several hours or days.

1.3 Impact and Probability Graph

A powerful way to communicate risks to system and data owners is to locate them in a two-dimensional graph, according to their impact and probability. Normally, the y-axis represents the impact, the forceful consequence[6] of the risk taking place. The x-axis represents the probability of the risk to happen, the likelihood that the risk materialises. The display of different risks on this graph facilitates decision-makers the prioritisation of security measures.

A common strategy proposes to mitigate first risks with a high impact and a high probability to occur. Those risks with only either a high impact or a high probability are the second priority. From those two types, normally risks with high impact take precedence to risks only with high probability of occurrence. Finally, risks with low impact and low probability occupy the last place in IT security order of priority.

Impact and probability graph's detractors argue that although the impact can objectively be assessed and quantified, the risk probability value is a subjective estimate. This is the reason why we propose to keep track of security incidents happening in the world to similar organisations.[7] This knowledge will provide realism to any probability estimation.

The probability dimension is strongly related to the attractiveness that ***threat agents*** find to make use of a vulnerability. This attractiveness is directly proportional to the threat agents' profit to risk ratio: The potential profit the attacker could have compared with the risk they run (Fig. 1.1).[8]

1.4 Risk and Active and Passive Voices in Grammar

We already mentioned that everyday language usually brings some confusion to the concepts of threat, vulnerability and risk. The possibility to use either the active voice (the wolf eats the little pig) or the passive voice (the little pig is eaten by the wolf) to describe the same scenario is great as a language tool but it puzzles readers when risks and threats are the topics of discussion.

[6] Definition of impact from the web site www.wordreference.com. Last accessed 20-09-2009.

[7] See Section 1.15.

[8] See Section 1.16.

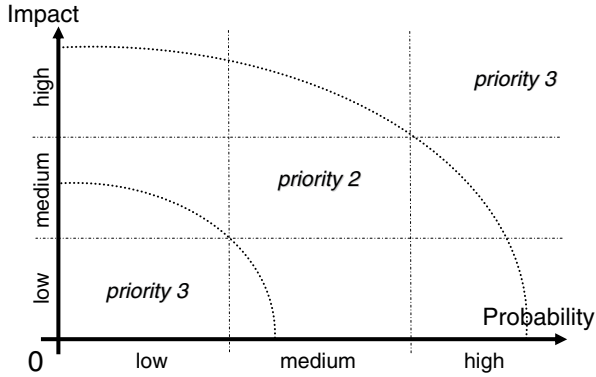

Fig. 1.1 Impact–probability graph

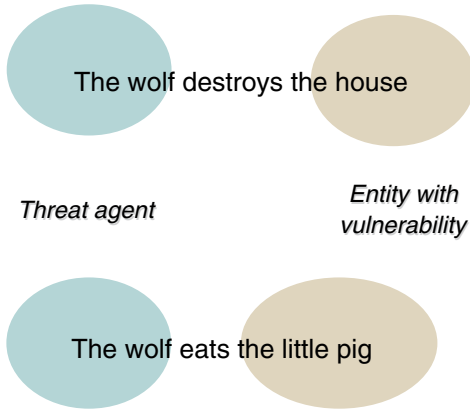

Fig. 1.2 A risk consists of a threat agent taking the chance of a vulnerability

Since the ***threat agent*** plays an active and decisive role, we recommend using only the active voice so that we can always identify the threat when looking at the subject of our sentences, e.g. the wolf blows the little pig's house away and eats the little pig (Fig. 1.2).

1.5 Internal and External Elements in a Risk

As a summary, it is essential to remember:

- The internal nature of a vulnerability in any system.
- The external nature and active role of a threat.
- The existence of a risk by the conjunction of these two elements causing an undesired event.

The more specific the description of the event, the easier it will be to understand the risk. The consequence that the risk produces if it happens and the probability that it occurs constitute two common dimensions to describe risks.

Information Risk Management Theory

We introduce the concept of risk management methodologies and apply it to our two examples to finalise the first part of Chapter 1.

1.6 Information Properties

Risks posed to information emerge from threats targeting one or more information properties. The three main information properties to consider constitute the CIA[9] acronym:

- Confidentiality: Only authorised individuals or entities can access information.
- Integrity: Information is accurate and complete.
- Availability: Information is accessible and usable by an authorised entity.

There are more information properties adjacent to CIA, such as:

- Auditability (possibility to check actions performed)
- Non-repudiation (authorship guarantee)
- Non-mediation (no knowledge of the existence of the piece of information)

However, the three main properties, CIA, cover the majority of possible threat vectors.

1.7 Risk Management Activities

ISO[10] and NIST,[11] two worldwide known entities producing standards and industry best practice guidelines, break down the foundations of risk management methodologies into four different activities: Risk assessment, risk mitigation, risk acceptance (term used by ISO) and risk communication.

[9] Adapted from ISO (2005), pp. 1–115.

[10] ISO (2002), pp. 1–16.

[11] NIST (2002a), pp. 1–F1.

1.7.1 Risk Assessment

An undesired event, a risk, is categorised in two dimensions: The probability of the event happening and the impact to the system (and therefore, to the business). Risk assessment consists of risk identification and evaluation (probability and impact) plus the recommendation of risk-reducing measures. The quality of the risk assessments performed by IT security teams depends on whether they are understood by the recipients and whether they trigger the implementation of appropriate mitigating measures.

The risk assessment methodology proposed by ISO[12] comprises three major activities, being risk identification, risk analysis and risk evaluation. NIST[13] proposes a more comprehensive risk assessment methodology encompassing nine primary steps, currently considered industry best-practices:

1. System characterisation
2. Threat identification
3. Vulnerability identification
4. Control analysis
5. Likelihood determination
6. Impact analysis
7. Risk determination
8. Control recommendations
9. Results documentation

The decision to focus on a threat analysis or on a vulnerability analysis or on both of them is not an easy one. It will depend on available resources, in terms of security and business expertise, time line requirements and company policies.

1.7.2 Risk Mitigation

It consists of prioritising, implementing and maintaining the appropriate risk reduction measures recommended in the risk assessment process to minimise risks to an acceptable level.[14]

1.7.3 Risk Acceptance

Remaining risks need to be re-evaluated and mitigated with new measures or accepted by information owners and senior management.

---

[12] ISO (2002), pp. 1–16.

[13] NIST (2002a), pp. 1–F1.

[14] Adapted from NIST (2002a), pp. 1–F1.

1.7.4 Risk Communication

Accepted risks need to be transparently communicated to key stakeholders to avoid a false feeling of security.

We revert to our examples and apply these steps. At the same time, we also take the chance to introduce the concept of "*appetite for risk*".[15]

1.8 Risk Management: Example Number 1

1.8.1 Risk Assessment

For the little pig, the piglet, and the risk of him (we use him and not it) losing his house and being eaten, there is a high probability of that occurring if the wolf lives around and sees him. The impact on the little pig of losing his house is considerable, but, it is certainly less than the wolf eating him.

As we can see in this example, a useful way to describe the impact (and subsequently, the risk) is by using clear comparisons (for the piglet, the impact of losing the house is smaller than the impact of being eaten).

1.8.2 Risk Mitigation

Examples of measures that the piglet can take to mitigate this risk are:

1. Building an electrified fence all around its house.
2. Hiring a physical security (hunting) service to keep the wolf away from the house.
3. Building an inconspicuous house so that the wolf does not pay attention to it.

We can always find a myriad of measures that an IT security team can implement to mitigate a risk. The key is to reach the right balance between the resources devoted to it and the value of the asset they are protecting. This is where current risk management theories really need a close contact with reality (e.g. in the form of risk quantification and asset valuation[16]). Later on this chapter, we will visit the

[15] See also Section 1.13.

[16] Traditional risk management methodologies can lead to a "permanently unfinished analysis" due to the rapid change of value in assets. Condensed from an interview in Spanish security magazine SIC to Santiago Moral, available at http://www.revistasic.com/revista62/entrevista00_62.htm. Last accessed 31-10-2009.

idea of the value of the risk-mitigating measures and the value of the protected asset and how the former is not always less than the latter.[17]

1.8.3 Risk Acceptance

Our friend, Mr. Piglet, will surely have a limited budget to implement some of the risk mitigating measures. Probably he cannot afford hiring a hunting service to protect him from the wolf at any time. However, he can build a decent fence with the limited budget he has. Somehow, he is then obliged to accept the remaining risk (the wolf could jump off the fence and break havoc). The dimensions and quality of the fence depend on a very elegant concept named "***appetite for risk***". In plain words, how much risk is Mr. Piglet willing to accept for his house and for his life considering also the resources he can use to protect himself. Section 1.13 delves deeper into this key concept.

1.8.4 Risk Communication

Once the mitigating measures have been decided, they need to be implemented and the remaining risk needs to be communicated and accepted by the stakeholders, especially those running the risks. In this example, Mr Piglet plays two different roles: The one deciding which risk measures to implement and the one exposed to the risk. The risk communication exercise is trivial in this case.

In big organisations, however, players making risk-mitigating decisions can be far away from business owners. This is due to complex hierarchical structures and ineffective decision making processes. In those cases, organisation boards require a clear communication of the risks that their organisation runs at any time. The owners of the organisation (normally, the owners of the information) run the real risk. We have a closer look at this in the second example.

1.9 Risk Management: Example Number 2

1.9.1 Risk Assessment

A laptop connected to the corporate network in an empty meeting room: If physical access control measures exist to enter the organisation's facilities, there is a small probability of someone entering the room unescorted and accessing the network. The impact of this access, however, if key servers, holding essential information for the business, are connected to the same corporate network, is high (e.g. a denial of service attack on one of them).

[17] See Section 1.16.

1.9.2 Risk Mitigation

The risk-mitigating measures in this case may come from very different angles, for example:

1. Physical security staff can issue an organisational guideline stating that no unescorted visitor could enter any meeting room alone.
2. They can also install a CCTV system in all meeting rooms to deter from stealing or misusing those laptops during the time available between meetings.
3. IT staff can disable the option to boot from any other device than the hard disk in any laptop present in any meeting room.
4. They can also remove all laptops from meeting rooms.

1.9.3 Risk Acceptance

If we imagine that this meeting room is in a service company whose main asset is information (e.g. a customer database made out after decades of running the business with millions of credit card numbers stored in a central database), then it seems reasonable to think that the owner of the company would have a limited "*appetite for risk*" and they will accept the remaining risk of someone accessing the corporate network only after having implemented the first three measures proposed in the risk mitigation section.

1.9.4 Risk Communication

In a big organisation, it would already be a success if the IT security team is in charge of performing the risk assessment of our example. They should communicate risks undergone by the organisation on this scenario literally to the owner of the organisation. This entails the use of the appropriate business language (and not IT jargon) and efficient mechanisms such as quarterly reports, risk dashboards and other tools that we propose in this book.[18]

Equally, the owner of the organisation should communicate clear "appetite for risk" criteria to risk-related functions such as the IT security team. The way to communicate the risk acceptance threshold is usually through money-related figures (budget, affordable losses, brand value) and/or through assertive and transparent risk-related decisions.[19]

[18] See Chapters 5 and 7.

[19] See Section 1.13.

Appetite for IT Risk: Let the Business Lead

The second part of the first chapter brings the pendulum from theory to practice: How the IT security team can keep close contact with reality and with the organisation where the team works. We can apply these specific learning points to the IT security team as from day 1. The starting point is getting to know the organisation's IT ***appetite for risk***.

1.10 IT Security Getting Close to Reality

Currently, organisations are adopting comprehensive risk management methodologies to comply with industry standards and stakeholders' requirements. IT standards, such as ISO 20000 or its implementation, the best practices collected in ITIL, include an information security management chapter.

Every IT security expert should know and master the risk management foundations presented earlier on in this chapter. However, risk management methodologies give organisations an impression of being secure that, unfortunately, is not based on reality. To start with, IT security groups need to identify the gap between this formal impression and the real state of IT security in the organisation. Then, they need to actively close this gap. This book shows how to achieve this (Image 1.1).

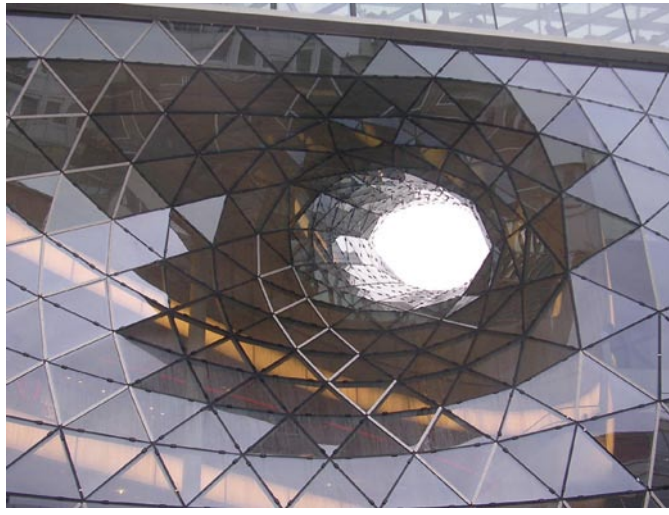

Image 1.1 False impression of security. Closing the gap

1.11 IT Provides Solutions to the Business

The reason of being of every IT department is to provide IT-based solutions to the business. IT groups follow a project-based methodology to bring these IT solutions to the business. Business and IT managers entrust a resourceful group of experts, the project team, with a new IT-related activity to provide a solution in a given time frame with a certain amount of resources.

The theoretical approach consists of linking the risk management methodology in place in the organisation with the project management methodology used in-house. This recommendation sounds logical and appropriate. However, it is not sufficient: Reality tells that nowadays the provision of IT solutions needs to be agile and to accommodate customers' business needs in a fast and changing manner.

Realistically, the triadic mantra for an IT project is to provide the IT delivery on time, on budget and with a required quality. IT security can only slightly change the direction of a project and improve a little bit this project triad. The earlier IT security works with the project team, the greater its influence will be.

1.12 IT Provides Secure Solutions to the Business

Business is in business to do business[20] *(Mike Poor 2007)*

These words by Mike Poor say it all. We would add to these words: "…and not security". In most organisations, IT and IT security are only support areas, not core business areas. Management boards tend to consider IT and IT security as any other support function: An important function, certainly, maybe essential, but not the core of the business.

Making business is taking risks: IT security needs to provide business makers with a clear risk description so that they can make informed risk-related decisions. More often than desired, security acts as the obstacle for the business to run risks, some of them even unknown to the decision-makers. The ultimate role of IT security is to inform the owner of the business of IT risks run by the organisation.

> Therefore, IT security professionals should forget the sentence "you cannot do it, it is very insecure" and change it for "we will do it in a more secure way".

The 100% secure IT system is the one that is off and buried in a block of concrete. However, that system is of no use to the business. The IT security team provide advice on how to deliver the functionality demanded by the business, and not on how to prevent the business from getting their idea materialised. The business will implement their idea anyway. Therefore, it is better for the organisation (and for the team) that they do it with the IT security team, rather than in a totally uncontrolled manner.

---

[20] Mike Poor, IT security professional and SANS trainer (2007). See http://www.sans.org/training/instructors.php#Poor. Last accessed 22-09-2009.

The task of IT security is to let the project team deliver a solution according to the organisation's appetite for risk[21] by providing expert advice on the risks the organisation faces due to the IT solution. The project team can only deliver a secure IT solution if they are aware of IT security requirements. Ideally, if the organisational setup allows it, the IT security team in the organisation should be able to advise project team members directly.

1.13 How to Derive Appetite for IT Risk From Management Decisions

It is rare that a management board provide input to an IT security team on the precise risk the organisation is willing to run, or better said, the risk they are willing to take. Even though this question deserves an answer, soon IT security leaders see that it is never directly answered. Why? We explore the following scenario: How could we answer how much money would suffice us to live happily ever after? Wouldn't we be tempted to speak up, letting our imagination run, and answer with an extravagantly high sum?

The appetite for risk question produces an output similar to the "money to live happily ever after" question: Most of us would answer with an inaccurate and extravagant response. It is frequent to listen to answers covering the full range, from:

- The organisation cannot accept any risk, to
- The organisation will accept any required risk for the business to go on.

Both extremes are equally useless to determine the IT security measures the organisation needs. We suggest that IT security professionals follow this practical approach:

1. Getting to know the core business processes of the organisation. The description in few sentences based on the mission statement or on the main marketing slogan is insufficient. Being completely able to follow a business-related meeting or a conversation with peers in the customer business areas should be enough to fulfil this first requirement.
2. Establishing permanent contacts with the business areas. The IT security team should know on what they are working and participate in their main business developments and plans. This way, the team can understand how much risk the business run on other fields (credit risk, market risk, reputational risk).
3. Understanding the strategy of the customer business areas and following that strategy while delivering IT security products (risk assessments, mitigating measures, security advice).

[21] See Section 1.13.

Image 1.2 Different organisations have different appetites for IT risk

These three points constitute an effective way for the IT security team to provide value to the organisation using their IT risk management and IT security skills. However, they are difficult to put into practice by any IT security team based only on IT knowledge. This is still the case in most organisations. Very seldom, IT security team members enjoy seasoned business acumen. Although rare, economic, social and psychological experience is also very valuable for an IT security team (Image 1.2).[22]

1.14 Risk Perception by Human Beings

In the last decades, evolutionary psychology and neuroscience provide evidence on how human beings perceive risks.[23] We use different "mental calculators" that, depending on what they are based on, make them bad or good risk assessors. From the risk management point of view, we recommend taking this fact seriously when dealing with high-level qualitative risk probability considerations: Often human beings are far away from providing realistic risk estimations.

For example, there is an increase in the perception of risk materialisation if we continuously encounter information in mass media about worst case scenarios happening. We lose focus on how improbable is the happening of that event. Steve Pinker[24] confirms that the violent death rate in humans since 2000 is literally

[22] See Chapter 2.

[23] See reference in the presentation "risk perception and the problems we make for ourselves", available at http://www.ramas.com/wttreprints/sranortheastReprint1.pdf. Last accessed 22-08-2009.

[24] Professor at Harvard Department of Psychology. See http://pinker.wjh.harvard.edu/index.html. Last accessed 22-09-2009.

decreasing, while, if we follow mass media, we all have the feeling that the number of violent acts is increasing.

Where to Focus: Business Value of IT Security

After explaining the foundations of risk management and the way to understand the organisation's appetite for IT risk, we propose a set of measures to IT security professionals so that they can provide business value. The IT security team need to explain their colleagues their tasks and why they are important for the business. Traditionally, IT professionals, and especially IT security experts, pay insufficient attention to this dimension of their work. In the following sections we propose measures to increase the understanding of the need of IT security throughout the organisation.[25] Chapters 4 and 5 delve deeper on what to do and how to do it.

1.15 How to Keep IT Security Work Real by Avoiding Doomsday Tellers and Collecting News

Only what it is detected is real. Organisations do not welcome risk visionaries. It is not wise to permanently raise the alarm in the organisation. The IT security team need to refrain from using the "cry wolf" approach in the form of informing[26] about every potential risk that could happen. Whenever they need to report about a real risk, we proposed to accompany the factual description of the risk with two proposals for a solution, a short-term patch and a long-term set of security measures.

IT security needs to base their risk-related advice only on real events. A way to achieve this is to maintain a constant flow of security news into the organisation: Security incidents happening to similar organisations, new vulnerabilities and new threats appearing on a daily basis on reputable media.[27] Annual trends, data breaches and top risks reports from industry players such as telecommunications providers, government agencies and security-related organisations are excellent sources of information (Image 1.3).[28]

---

[25] OECD (2003).

[26] More than informing, sometimes IT security teams threaten organisations with their "apocalyptic" statements.

[27] See an example of security incident news in Annex 2.

[28] For example:

– The 2009 data breach investigation report from Verizon. Available at http://www.verizonbusiness.com/products/security/risk/databreach/. Last accessed 13-10-2009.
– The XIV Internet Security Threat report from Symantec. Available at http://www.symantec.com/business/theme.jsp?themeid=threatreport. Last accessed 13-10-2009.
– The 2008 CSI Computer Crime and Security Survey. Available at http://gocsi.com/forms/csi_survey.jhtml. Last accessed 13-10-2009.

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?

We suggest sharing this IT security news with the organisation stakeholders in an attractive format to entice them to read it regularly, adding even some funny IT security incident, e.g. hacks in digital public announcement displays or traffic road signs.[29]

We propose to inform also about how identified risks are mitigated in reality by competitors or similar organisations. There is a simple way to package information that, under the right circumstances, can make it irresistible[30]: Offering specific examples of documented incidents without over emphasizing them. Even better, playing them down and just adding a cunning "*it could very rarely also happen here*".

The knowledge that the team get from these security events feeds their risk assessment process. They can create a list of threats, vulnerabilities and mitigating measures out of those security incidents. This list could start modestly, but it will soon be the team's threat, vulnerability and measures database. This database will offer the security team a consistent way of assessing risks. The team need to maintain this risk-related database updated and re-visit it frequently. This way, their risk assessments will be founded on real life events. This is fundamental to justify their security advice.

---

[29] As an example, we can read this piece of news reporting on a hacked traffic digital sign, available at http://www.dallasnews.com/sharedcontent/dws/news/localnews/transportation/stories/013009dnmetzombies.1595f453.html. Last accessed 20-07-2009.

[30] Gladwell (2000) p. 73. More on this topic in Chapter 7.

It is recommendable to complement that collection of IT security news with the follow-up measures that affected organisations implemented to recover from the incident and to prevent new occurrences. This type of information is usually more difficult to gather. We propose to make use of industry publications, contacts in the industry and public resources such as Internet (especially trustworthy sites).

Security incidents happening to the organisation are also a very valid source of information. Real-time monitoring should be part of the daily IT security activities. It will enable the team to document the real threats that they detect. Only those real threats will justify budget for security measures. The ultimate goal of the team is to protect the organisation from those detected threats.

We suggest creating an IT security incident response team within the IT security team, based on clearly cut, swift and effective procedures. They will be the cornerstone to investigate and reply to security incidents while being a silent but impressive marketing tool within the organisation on why they need an IT security team for their business.[31] Whenever an IT security incident will happen, they will be ready to cope with it with a pre-tested plan.[32]

The security incident scenario is in constant change. However, there is a permanent element in all of them: Intention. There is an agent (the threat) performing an action (taking the chance of a vulnerability) with a specific purpose. Unintentional events can also cause IT security incidents (e.g. more than 500,000 laptops are lost every year on U.S. airports[33]). However, with the lack of an intended purpose, they can be mitigated more easily.

1.16 Profit to Risk Ratio

The price-earnings ratio of a listed company is a valuation ratio of the company's current share price compared to its per share earnings.[34] This is a useful way to compare shares in stock exchanges. The greater the ratio, the more expensive the company share is.

A useful way to compare risks will be the ratio between the profit that a potential attacker could have when exploiting a vulnerability and the risk the attacker runs when using the vulnerability. The greater the ratio, the more frequently this risk will materialise. There will be potential attackers intending to take the risk: They could obtain a relatively high profit running a relatively low risk. If there is a specific type of attack that works, threat agents will use it.

---

[31] See Chapter 7.

[32] See a comment on this respect from Richard Bejtlich, Director of Incident Response at General Electric, available at http://taosecurity.blogspot.com/2008/09/is-experience-only-teacher-in-security.html. Last accessed 13-10-2009.

[33] See http://www.pcworld.com/businesscenter/article/147739/laptops_lost_like_hot_cakes_at_us_airports.html. Las accessed 22-09-2009.

[34] Definition provided by http://www.investopedia.com. Last accessed 22-08-2009.

The IT security incident database[35] should confirm this fact. It should contain multiple examples of high profit to risk ratio incidents. The team will base their profit to risk ratio figures on real data they are collecting in the security incident news database.[36] Security activities and measures should focus on mitigating those scenarios with a high profit to risk ratio (PRR). Attackers will target them: They have a lot to earn and not much to lose. Once the team have identified those security activities, we suggest keeping a limited number of them running in parallel.[37] Too much variety running simultaneously brings complexity and lack of focus. Few selected IT security endeavours with smart[38] objectives and committed deadlines will bring success to the team and, more importantly, to the organisation.[39]

1.17 Smart Selection of Risks to Mitigate Following the Pareto Principle in IT Security

The Pareto principle, also known as the 80-20 rule, shows how, in many and diverse situations, 80% of the effects come from 20% of the causes.[40] IT security does not escape from this principle: 80% of the consequences that the materialisation of a risk brings stem from the use of 20% of the existing vulnerabilities. The drawback, though, lies on how to identify that 20% of vulnerabilities that will be exploited. There is no silver bullet for this.

Impact–probability graphs and the profit-to-risk ratio help to apply Pareto. We identify two sets of risks, considering that IT security budgets are never enough for everything that an IT security team would like to implement:

- Risks severely affecting the organisation, i.e. those ones with the greatest impact.
- Risks with the highest profit-to-risk ratio, i.e. those ones that are extremely attractive to attackers, basically due to two simple reasons:
  - Attackers put hardly anything at stake when performing the action.
  - If successful, the benefit they obtain is juicy.

We add the probability dimension to both sets. The database collecting IT security incidents happening in the world is useful to obtain at least an estimation of how probable it is that those risks will occur in the organisation. The team need to distinguish between probable risks and possible risks.

---

[35] See Section 1.15.

[36] See Section 1.15.

[37] As we mention in Chapter 5.

[38] See http://en.wikipedia.org/wiki/SMART_criteria. Last accessed 20-09-2009.

[39] See Chapters 4 and 5.

[40] Pareto principle definition from www.wikipedia.org. Last accessed 20-09-2009.

We propose to prioritise the work, and the expenditures, following the 80-20 rule. Teams will define and implement, first, IT security mitigating measures for those risks with a high impact, high probability[41] and high profit to risk ratio, and for those scoring high in at least two of these three dimensions. This approach will provide the best "bang for the buck[42]" in terms of IT security for the organisation.[43]

The reader can however think that a remote, improbable and not known risk could anyway materialise and take all risk mitigating plans to real failure. This is indeed possible, although not probable, and the reason why the setting up of a well-trained security incident response function within the IT security team scores also high in the activity prioritisation list.[44]

1.18 How to Spend Resources Wisely and Transparently: Reputation and Emotions

The general principle proposes to avoid spending more resources in assessing risks than those that would be spent if the problems really occurred[45] and provide financial transparency to risk/return metrics.[46] Otherwise, IT security detractors in the organisation, following different goals, have an easy and powerful way to show the ineffectiveness of IT security measures.

There are occasions when the team need to mitigate risks spending more resources than those lost if the risks materialise. These exceptional situations exist and they are tightly bound with emotions and reputation.

Regarding emotions, as an example, it is frequent to find high-value armoured doors protecting homes with low economic value inside. The emotion that the owners would feel if their home is broken in leads them to spending more in protecting their home that the actual value of their belongings. Although this is a rudimentary example, similar situations exist in business.

About reputation, the value of some public organisations reside on their reputation, a security incident provoking relatively low loses going public could put them out of business due to the loss in their image and reputation.

In addition to this, organisations need to avoid being the last one in their industry taking any security measure.[47] In any industry, being the last company implementing

[41] See Fig. 1.1 and Chapters 4 and 5.

[42] Aabo et al. (2004), pp. 1–34.

[43] See Chapter 4.

[44] So that they can quickly apply corrective measures if an incident happen.

[45] Dillon and Paté-Cornell (2005), pp. 15, 17, 18 and 24.

[46] Rinnooy (2004), pp. 26–31.

[47] Idea coming from a conversation with Santiago Moral, IT security professional (2007).

a specific security measure can have negative consequences, both from the reputational and the operational side:

– In terms of reputation, competitors could easily use that fact to attract disappointed customers out of that company.
– Operationally, attackers will target that company for as long as they do not implement the corresponding mitigating security measure.

If we were able to provide an economic value to an emotion and to a certain reputation, these two exceptions will also fall under the general principle mentioned in this section.

1.19 No Business Value Without Business Knowledge

The IT security team need to grasp the importance of their role for the organisation. Slowly but surely, they need to comprehend that their mandate is to support the business with their IT security advice and actions. They need to understand the business of the organisation and the role they play in it.[48]

In the first example,[49] Mr. Piglet could defend himself from the wolf in an effective way if he would study the habits and acts of the wolf.

In the second example, the risks the organisation faces by someone knocking out the customers' database server through a denial of service attack, launched from an unattended laptop, could translate into a severe lack of revenue. The IT security team can make this translation only if they are into what is being cooked in the organisation: If the team know that the marketing department constantly use the database during business hours. Every time a customer contacts the hotline through the phone or the web, their information is pulled out of the database into a nice graphical interface used by the associate answering their request.

1.20 Smart Behaviour for IT Security Practitioners

How can the organisation learn about the value that IT security provides? We propose these three basic actions:

1. Reporting achievements in a clear and concise way to IT colleagues and management and to business colleagues.
2. Proposing pro-active measures when detecting an IT security risk. With pro-active we mean that eliminating the vulnerable business process is not an option, but modifying, improving or replacing it is an option.
3. Focusing the available energy on smart targets and avoiding turf wars within the organisation. They demand the energy required in more important fields, such as to do the IT security job.

[48] Adapted from Glen (2003), p. 16. Useful reference to lead IT geeks.

[49] See Section 1.8.

In this chapter, we have dealt with the theoretical and practical foundations of IT security: Risks, risk management, appetite for risk and provision of business value.

Chapter 1: Learning points

- A risk is a threat (an active agent) making use of a vulnerability.
- Impact–probability graphs describe risks.
- IT risk management need to be complemented by real data.
- IT needs to provide solutions to the business. IT security as well.
- Business owners need to understand the risks they run.
- IT security teams need to know the business and its IT risk appetite.
- IT security is a support area.
- IT security should focus on real threats that create real risks.
- They need to be careful with high profit to risk ratio (PRR) risks.
- IT security needs to provide business value.

Link to MBA Management Models

We have selected two models that could help us in the analysis of the external and internal environment surrounding your IT security team:

PESTLIED model
External environmental factors (among others, political, economical, social, technological, legal factors) than affect our organisation and our team.

The 7 'S' framework *(by Mintzberg and Quinn, 1991)*
Interconnected internal factors that influence the organisation's effectiveness, especially its ability to change (staff, strategy, skills, style, systems, structure, shared values).

More generically, a ***SWOT analysis*** (strength, weakness, opportunities and threats *by Johnson and Scholes, 1989*) can also aid in understanding the internal and external context of the team.

See references: Harding and Long (1998) and links:
http://www.valuebasedmanagement.net/methods_PEST_analysis.html
http://www.valuebasedmanagement.net/methods_7S.html
http://www.valuebasedmanagement.net/methods_swot_analysis.html

See Annex 1 for an example of a test to assess understanding of the basic contents of this chapter.

Chapter 2
Security and IT Background

Chapter 2: What will the reader learn?

This chapter answers the following questions:

- What does the IT security workforce look like?
- Which basic profiles does an IT security team need?
- Which specific profiles does an IT security team need?
- Which technical skills does the team need?
- Which soft skills does the team need?
- Where can the team leader find these required profiles?
- Where and how can anyone start in security?
- What to study?

Professional Outlook and Profiles for IT Security

The IT security team needs to be built of experts, professional individuals willing and motivated to provide value to their customer organisation. This is easier said than done. This chapter provides a path to compose a team with the potential to excel in their mandate.[1] The profiles and skills mentioned constitute a necessary condition to create a capable team. Unfortunately, it is not a sufficient condition. Other elements such as motivation, organisation and team dynamics play an important role as we will comment on the subsequent chapters.

[1] To provide IT security expertise, see Section 1.19.

A. Partida and D. Andina, *IT Security Management: IT Securiteers - Setting up an IT Security Function*, Lecture Notes in Electrical Engineering 61,
DOI 10.1007/978-90-481-8882-6_2, © Springer Science+Business Media B.V. 2010

2.1 IT Security Workforce

The IT security profession, although with ancient foundations on physical security and military topics, is very young. In terms of degree of evolution, IT security is still a baby. The number of IT security professionals in the world is estimated to be 1.66 million.[2] This figure is supposed to increase up to 2.7 million professionals in 2012. Three figures to help understanding this increase in the number of professionals: In 2009, reports mention that there are between 100 and 150 million web applications on the Internet and hardly less than 10% of them have undergone any kind of security test before going live.[3]

IT security is relatively anti-cyclical. Traditionally, strong industries, such as banking, automotive, telecommunications and pharmaceutical, demand IT security experts. Even during periods of economic downturn, when the entire IT market suffers from layoffs, security is one of the fields that best resist hard times.

Salaries for IT security professionals are high. They are mostly placed in the upper range of IT salaries. In 2008, out of a survey made by SANS with over 2,100 respondents,[4] 38% of them earned US$100,000 or more per year. Regarding educational levels, the same survey mentioned that 75% of security professionals hold a bachelor's degree or higher.

In the majority of companies, IT security is still growing in importance and budget. This is why companies strive to create a capable and dependable IT security team even when there is still a small number of reputable universities providing IT security curricula.

2.2 Basic IT Security Profiles

The concept of IT security entails a wide variety of activities and specialities. Nowadays, we can state that no human being can master all of them simultaneously. This is why, as in other complex disciplines, once an organisation has reached a certain size, the IT security function requires a team and not only one individual.

The initial division of labour is rather basic: There are technical and governance related activities. Technical tasks require a command line or a graphical interface and policy-related tasks require a word processor. The former tasks need hands-on IT security skills and the latter ones drafting, synthesis and communication skills, together with a basic understanding of security principles[5] and technical implementations.

---

[2] Frost & Sullivan (2009), p. 6.

[3] Minute 46–48 in episode 149 of pauldotcom podcast, available at http://pauldotcom.com/2009/04/pauldotcom-security-weekly---e-5.html. Last accessed 20-09-2009.

[4] SANS (2009a), p. 0.

[5] See Sections 4.2– 4.4 for additional information on security principles.

Table 2.1 Basic division of profiles in the IT security team

Basic IT security profiles	
Technical	Governance related
Network	Security policies
Operating systems	
Applications	

Technical IT security skills constitute a set comprehensive enough to deserve careful analysis. IT elements can be broken down into networks, systems and applications. The same division is valid for IT security:

- Network security: Ability to technically apply IT security principles in networks. This mix requires IT network administration and IT security expertise.
- Operating system security: Ability to secure and test operating systems. The two main current flavours are Windows and Linux/Unix.
- Application security: Ability to secure applications. This is a very broad term. A database can be considered an application. A web server is also an application. In this case, depending on the applications used by the organisation, the team will require knowledge on how to secure them.

Security governance includes a comprehensive set of security policies. They need an author: Someone able to understand the business use of an IT component and to draft an understandable policy which considers business and security requirements. The key to succeed is to allow for the business use of the IT element while preserving the security of the organisation's information.

These two profiles, technical and governance, although different, need to exchange information and understand each other's work. Security policies are normally independent from the underlying technology. However, their implementation entails the creation of hardening procedures. This requires technical IT security skills. Thus, both profiles, although different in activities, need to follow a common strategy (Table 2.1).

2.3 Extended IT Security Profiles

Having the basic division of profiles in mind, we additionally propose a practical division of profiles or roles based on everyday activities. Depending on the size of the organisation, the same position could potentially perform more than one role. We begin with the technical IT security profiles and subsequently we will mention the governance related roles.

2.3.1 Technical IT Security Profiles

The first profile we focus on is the ***security tester***. They perform technical security tests including penetration and vulnerability tests. This is a very technical profile,

requiring expertise on IT networks, operating systems and applications. The technical skills of a security tester are the ones required also to handle an IT security incident.

Therefore, the security tester can also play the role of an ***incident handler***, the second technical IT security role we include. There is one decisive difference between the incident handler and the security tester, but it is not technical: The first one requires the ability to work under pressure. The second one has the privilege to plan their tests.

The third profile to highlight is the ***security administrator***. There are security devices that need to be administered: These are, among others, firewalls, authentication devices, intrusion detection (and prevention) systems and vulnerability scanners. The administration of these devices should fall under the responsibility of the security administrator.

This profile is still popularly known as the one in charge of user identity management in an organisation. User identity management is a very broad and complex field that covers all IT user provisioning and user administration activities. Traditionally, security administrators have created identities and allocated access rights in the information systems within the organisation.

We suggest to split the security administration profile into two: ***Security device administrator*** and ***user identity and access administrator***. They require different technical skills and their activities can reach different degrees of automation: In user and access management, a smart identity management implementation could automate many of the IT user creation steps. In security device administration, even with the existence of a centralised management console, automation is not a plausible priority, mainly because this activity does not consist of repetitive self-contained steps.

The last technical profile we propose to add to the team is a ***security monitoring operator***. Slowly but surely, security activities in the team will include an increasing number of monitoring tasks. This profile will start off security activities triggered by the occurrence of a specific combination of log entries. Their tasks range from gathering, monitoring and reacting on logs to creating automated alerts based on their criticality. The operator will initiate security procedures that should already be established and tested, including those designed to answer critical events.

2.3.2 IT Security Governance Related Profiles

Adjacent to the technical core of the team, the organisation will require IT security governance related profiles. They set the policy framework, a set of IT security "playing rules" that will guide the entire organisation, and the IT security team, in their daily business.

The first profile that we describe is the IT security ***policy writer***. The secure use and configuration of IT systems usually requires the elaboration of a contract stating how the system may be used. This is the starting point of a security policy. The writer of those policies needs to be able to understand basic security principles and

transpose them into specific security policies. A mixed technical and business-related background is optimal for this profile.

Security policy writing is a complex task. The inhabitants of the organisation need to understand the policy and its purpose and to be able to apply it while performing their business activities. Conciseness, consistency and applicability need to be features of every security policy in the organisation.

The security policy writer needs to find the sweet spot in the organisation so that business can proceed and, at the same time, security is not neglected. Security policies are part of IT security governance, together with the innovative creation of IT security links to other aspects of IT governance and corporate governance. This tough goal requires additional support from a new profile we add to the team, the security communicator.

The ***security communicator*** is the second profile we cite. An extrovert figure, preferably with a mix of technical and governance related skills, that will play a key role in two scenarios:

2.3.3 Provision of IT Security Expert Advice

They will become key IT security resources in "changing activities" like IT projects. Therefore, professionals performing this role should cover the three main technical security fields: Network, operating system and application security.[6]

2.3.4 IT Security Marketing

In addition to provision of IT security knowledge, security communicators need to show the need for current organisations to follow IT security principles. They will:

- Lead security awareness campaigns.
- Facilitate the introduction of new security policies in the organisation by explaining them to the business areas when required.

This role is similar to the software product evangelist role present in many companies since the 1990s: Expert technical knowledge plus excellent communication skills with technical and non-technical audiences. Simple but telling and eye-opening demonstrations will be among the activity portfolio of the security communicator.

2.4 The Coordinator, the Facilitator and the Trainee

All profiles mentioned will lead a handful of ongoing activities at any time in the IT security team. These activities require a degree of synchronisation and a common tempo. The coordination of the team calls for an orchestra conductor role: A multi-disciplinary

[6] See Section 2.2.

profile that we will call ***security coordinator***. They will have experience in technical security, security governance and business analysis. The coordinator will keep the harmony within the security team, set the strategy to follow and drive the interaction with the rest of the organisation. Hopefully they are not the only source of inspiration within the team, but they definitely need to be one of the inspiring forces.

We have not used the word manager on purpose (apart from the specific tasks of user identity and access and security device management). Management tasks within the security team are not exclusive to the coordinator role. Most profiles in the team will manage time, budget, resources, including additional workforce to accomplish a specific project. The main duty of the security coordinator is to tune all management activities happening within the team (Image 2.1 and 2.2).

Traditionally, the existence of a manager implies the existence of a hierarchical command line. Hierarchy should be kept as flat as possible within the security team. Expertise and specialised knowledge are more important that hierarchy. Every team member is the manager in their field of expertise.

The coordinator will lead and be responsible for the overall decision making process. This is the only possible way to effectively fulfil the mandate[7] of the team.

There are two important figures within the security team that we have not mentioned yet: The team facilitator and the trainee.

The ***security team facilitator*** veils for the smooth functioning of the team in all terms different from IT security. Typical activities falling under their responsibility are budget monitoring, contract procurement, maintenance of published security information in the organisation and task progress monitoring.

Image 2.1 The IT security leader's goal: orchestrating security

[7] To provide IT security expertise, see Section 1.19.

Image 2.2 Leading and coordinating, but not micro-managing

The facilitator works tightly with the coordinator. Together, they ensure that all team members can work and that planned activities move on accordingly. Their challenge, working together as one reporting and monitoring unit, is to foresee team requirements and to answer them or, at least, to identify them so that activities can progress.

With regard to individual needs, we propose to use a three-dimensional system: Every team member has a professional, a social and a personal/spiritual side that requires a certain degree of balance. We will elaborate on this in Chapter 3.

The last profile that any future-proof IT security team should have constitutes a link to the current academic world: The ***security trainee***.[8] Trainees provide fresh air to the team. They will normally be students in their last stage of their IT security or IT degree, preparing their dissertation or finalising their last subjects.

This initiative is a win-win deal. They have the possibility to attain real-life experience at first hand working with IT professionals and the team has the opportunity to learn new IT trends and tools, e.g. from the use of social networks as a replacement of email to the last useful switches for the *nmap*[9] command-line.

Trainees require support and mentorship. Our suggestion to achieve a win-win deal with trainees is the following: They benefit professionally from their stay with the security team and the customer organisation gets value from them. We recommend appointing a committed senior team member as the trainee's mentor. Each senior team member should mentor one or, at the most, two trainees. This way, teams can allocate sufficient time from their senior members to look after and develop trainees. Especially when the

[8] Annex 3 presents the IT security starter kit: Useful references for potential IT security trainees.

[9] Nmap is a security scanner originally written by Gordon Lyon (also known by his pseudonym Fyodor). Nmap is a "Network Mapper", used to discover computers and services on a computer network. Information obtained from http://en.wikipedia.org/wiki/Nmap. Last accessed 20-09-2009.

Table 2.2 Division of profiles in the IT security team

IT security profiles	
Technical	Governance related
Security tester	Security policy writer
Incident handler	Security communicator
Security administrator:	
– Security device administrator	
– User identity and access administrator	
Security monitoring operator	
Security coordinator	
Security team facilitator	
Security trainee	

team is just created, we recommend limiting the number of trainee positions. As a rule of thumb, not more than a trainee position per five team members is advisable.

This concludes the initial enumeration of profiles for an IT security team. We summarise them in Table 2.2.

Skills and Backgrounds for Team Members

We present the magical success recipe for the IT security team: A set of skills, technical and soft traits, optimal to build an IT security team. We also provide in these sections possible backgrounds from which these profiles could come from. Information provided here is very valuable to prepare selection processes that will fill positions in the team.

2.5 Technical Skills

We present the list of technical skills for each profile. They can be included in the description of an open vacancy for the team. It may be difficult to find real resumes that fulfil completely the technical skills mentioned here. We suggest using this list as a guideline to assess what the team already have and what they need to develop, acquire or learn.

Security tester: Hands-on mastery of security testing tools such as vulnerability scanners, network scanners and penetration testing tools is essential for these team members. Scripting,[10] programming and database experience need to appear on the list of skills too. Candidates will probably have a good knowledge in general IT and security principles. Should the latter be lacking, they could surely obtain them while they work and provide value to the team.

Incident handler: General IT and security principles knowledge with a sufficient level of detail about network, application and operating system security. They need

[10] "Lazy" professionals with scripting skills will automate as much as possible to free up their working time. They are optimal candidates for technical IT security teams.

to be able to follow and understand security testers and security administrators. Hands-on knowledge in security tools, network and system forensics, scripting, development (programming languages) must also be part of their toolbox. Finally, they require writing skills to elaborate incident reports.

Security device administrator: Firewall management skills, basic Unix and MS Windows operating systems knowledge and network concepts are in their list of technical skills. They also need to show readiness to handle new user interfaces (be it a token-based authentication server, a VPN terminator, etc.) and ability to follow an operational procedure.

User identity and access administrator: They need to offer operating system knowledge in the most common flavours (MS Windows and Unix/Linux), a basic understanding of user repositories technologies (LDAP and Active Directory) and certain knowledge of the basic security principles (such as segregation of duties, four-eye principle and least required business privilege). They should be able to write and to follow an operational procedure.

Security monitoring operator: The portfolio of skills should include a basic knowledge in common operating systems and networking protocols, ability to write and follow an operational procedure and understanding of the general concept of event monitoring and alert response.

Security policy writer: They need to have a basic understanding of the business processes taking place in the organisation. They will use their process analysis, synthesis and drafting skills to prepare security policies. They will also use their negotiation skills to agree on basic security principles (that they need to understand and use) with business areas. Policy writers require also experience with technical IT system configuration and audit processes. Current compliance initiatives in organisations require them to know and understand IT governance frameworks such as COBIT[11] and ISO standards.

Security communicator: They need to be skilled on technical IT security concepts present in networks, operating systems and applications, together with general security principles and basic business analysis skills, so that they can apply them in their engagements and advertise them using their marketing, public relations and selling skills.

Security coordinator: They need to build their business and strategy-setting expertise on top of their past experience on technical security and security governance positions. Business-related certifications, such as an MBA, confirming their business analysis skills, would be a plus.

Security team facilitator: They need to be able to understand basic IT and IT security principles together with essential business processes. The team will definitely benefit from their ability to synthesise and comprehend the bigger picture in the organisation.

[11] The Control Objectives for Information and related Technology (COBIT) is a set of best practices (framework) for information technology (IT) management created by the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI) in 1996 network. Information obtained from http://en.wikipedia.org/wiki/Cobit. Last accessed 20-09-2009.

Security trainee: They are students finalising (or just graduated) an IT or an IT security degree. They need to feel comfortable both with the command line and with a word processor.

2.6 Soft Skills

After presenting the technical skills the team should enjoy, we proceed to deal with the other essential half of the magical success recipe, the collection of soft skills that need to be present in the team. We propose to talk about skills that the team should have as a collective entity. Not all members will have all of them but the team need to show them as a group. This means that the majority of team members need to possess them or show clear signs that they could adopt them following group dynamics.

Attention and attraction to detail: Carefulness is at the heart of the basic security principles. A big number of security vulnerabilities, especially application development bugs, come from the lack of attention, mostly rooted in lack of time, when developing applications. Security team members need to observe and react upon the details of any situation they work on. This skill contributes to build an image of quality delivered by the team.

Drive to achieve: The security team needs to complete tasks. Not only to start them but also to finalise them within the timeframe agreed. There is a patent threat not to finish tasks, either because new and more urgent tasks appear in the horizon or because undertaken tasks need the concourse of stakeholders, external to the team, that are not available or work with a different priority list.

Failure acceptance: Unfortunately, some activities performed in the team will fail. This is a universal fact that happens in all human activities. However, these failures should be taken in the team as a lost match, that is all. The championship continues. Team members should be resilient to failure. They need to look forward and accept failure as an essential element of their professional life. New tasks, new possibilities will appear sooner than they think.

This is hard to accomplish, especially for IT literate people: It was by spending hours and days that they reached a respectable level of expertise on a specific operating system, application or device. They have, consequently, difficulties to find the right time to leave out that code that it does not compile, the application that does not behave as expected, and similar cases. This does not mean that they just have to try once and let it go. Finding the right balance is a sign of seniority and expertise. IT security professionals working in a team under a defined activity plan can afford neither to be perfectionists nor to be led by frustration. They can only exercise perfectionism during their free time, and the little they will have, they would need to find personal balance working, or enjoying, not in front of a screen.

Tolerance: A passionate IT security professional will find security breaches from day 1, or even from day 0, before reaching their office, via the Internet. Minutes after

entering the organisation's facilities, they will observe visitor announcement and escort procedures and they would already start assessing them. This behaviour is in their nature, similar to a medical vocation. They live security. They enjoy having a security mind and, even better, these professionals are usually well paid for this. However, they are not alone in the organisation and, as Mike Poor[12] says, "business is in business to do business, not security". IT security team members need to understand this premise and behave accordingly as professionals. Arrogance is not an option. They need to show a certain degree of tolerance.

Given their broad IT expertise, security professionals will interact regularly inside and outside the organisation with individuals with different fields of expertise and surely lower levels of security education. They need to interact peacefully and constructively with them.

Communication: This is always a big challenge among IT people. An example of this, a valuable IT security guru can attend, as a student, a 6-day specialised security training and talk less than two words per day with their neighbour seated next to them. IT security professionals need to be able to communicate with other technical and non-technical people.

Self-organisation: The team will have a busy activity plan. Regardless of the size of the organisation, human resources devoted to security will probably be overbooked. Members of the team need to be able to organise their time, resources and prioritise them according to the team's and organisation's strategy, without falling into undesired states of anxiety. They need to feel comfortable working independently without a daily supervision that can lead to excessive doses of micromanagement (Image 2.3).

Continuous learning: IT professionals require a permanent updating process in terms of new products, solutions and technologies appearing in the market and providing value to the industry. IT security professionals necessitate a continuous knowledge recycling, even more than in other disciplines. Reading, studying, sharpening their hands-on skills, following top-notch security sites need to be an inherent part of every "securiteer" (a passionate security professional).

A way to show a continuous learning process is through security certifications. It may be not the perfect way, since, out there, in the job market, there are experienced exam-takers that can pass almost any exam with sufficient preparation but without sufficient technical knowledge. Preparing a test does not always mean hands-on working experience with the topic of the exam but, at least, several reputable certifications guarantee some technical foundations present in the certificate-holder, especially if the certificate requires a regular renewal.

Stress-resilience: It is frequent to find players in the organisation with clear and expedite goals that, somehow, clash with basic security principles. Typical cases are project

[12] Mike Poor is a SANS trainer, founder of the company Inguardians. He pronounced these words in a SANS training in Ireland, 2007.

Image 2.3 Time management, a skill not to take for granted

managers carrying on their projects with very demanding business requirements and very little security content. Although it is a broadly accepted principle that IT security should be frontloaded up to the very initial conceiving phases of any project, in practice, it is still not always the case. In those unfortunate occasions, team members, required by project managers in late stages of their projects, need to be capable to cope with extraordinary pressure exerted by project stakeholders. This is not because they dislike security, but, simply put, because they have different goals.

Security professionals need to live up to their mandate, providing expert advise on IT security topics, without endangering the flow of business, even though sometimes this can mean reporting serious vulnerabilities and witnessing how, nevertheless, the system goes live. This is often a cause of stress. The key point is to keep business owners updated so that they can take an informed decision.

Healthy passion: Human actions are triggered by emotions.[13] A passion is a strong emotion.[14] The team need members that are driven by their love to security and their desire to see things well done. If they are driven by both loves, excellent. If not, at least one of those, to security or to quality, must appear.

Versatility and innovation: As we mentioned, IT security professionals need to have a wide variety of skills and, ideally, they need to introduce new elements into their deliverables, always with the aim to increase the value added to the business.

The list of soft skills can be endless. As mentioned with the technical skills, this list is useful to identify existing gaps in the team.

[13] Damasio (1994), pp. 127–165, Chapter 7, titled 'Emotions and feelings'.

[14] See http://www.wordreference.com/definition/passion. Last accessed 20-09-2009.

2.7 Possible Backgrounds Present in the Team

Once we have proposed the optimal composition of the team in terms of technical skills and personal traits, we point out possible origins from where team leaders can recruit these profiles.

The first possible background everybody can think of is the vocational one. IT security teams find candidates with a strong IT background who are passionate about security. They live and love security. They breathe security and they cannot hide it. This is actually an advantage for the recruiter because it will not be difficult to find and inspire passionate candidates. Their goal is to work in IT security and to develop professionally further and further in this exciting field. If possible, the recruiter should first try to populate the team with this type of vocational individuals.

We like to call them "securiteers" (using a similar approach than in marketing with the informal and contemporary euphemism "marketeer"[15] and also reminding us of the ancient "musketeers[16]"). Our experience shows that at least a good third of the team should be passionate "securiteers".

The second possible background is the traditional IT field. Professionals with strong IT hands-on capabilities, but unfortunately not so passionate for security, are also required for the team. Their knowledge on coding (using programming languages), scripting, command line interfaces, system administration and databases definitely enrich the collective profile of the team.

The art and the soft skills of the security coordinator come now into play. These IT experts need to understand and apply basic security principles that they may not be yet familiar with on their everyday activities. The security coordinator has to create the adequate environment so that these senior IT experts are inoculated with a "clear security mind" while they do not lose their genuine IT expertise and initiative. Otherwise they will soon feel alienated and they will flee from the team. We provide some tips to achieve this environment in the following chapter.

The third origin of candidates is the business, the industry where the team work. Business specialists, with a deep and extended understanding of business process analysis or simply with broad and wide understanding of what it is being done in the organisation, are potential candidates to complement the technical profiles in the team, specially if they are willing to change and swim in the IT technical pool.

Business profiles are very valuable. They act as a first sounding board within the team when a security proposal (be it a new security policy or procedure) leaves the team to reach part or the entire organisation. They are optimal candidates for the communicator and the policy writer profiles if they also have some IT background.

---

[15] See http://en.wikipedia.org/wiki/Marketeer, probably with some remote links to the superhero Rocketeer, see http://en.wikipedia.org/wiki/Rocketeer. Last accessed 20-09-2009.

[16] Members of a military unit created in France in 1622 with high sprit de corps and can-do attitude. They were made popular by Alexander Dumas's novel published in 1844. Adapted from http://en.wikipedia.org/wiki/Musketeer. Last accessed 20-09-2009.

Image 2.4 Building the foundations of security

We suggest checking in the organisation whether an HR programme to swap positions exists. It could help to attract business people into the team. In terms of numbers, our proposal is similar to the one we mentioned for trainees. One position per each group of five team members can easily proceed from the business world.

Security Studies

The following sections delve into the academic studies and alternative paths that can lead to mastering IT security (Image 2.4).

2.8 Engineering or Management

How can anyone study IT security? Currently there are already several bachelor degrees specialised on IT security.[17] This is becoming a real study option.[18] Traditionally, students first accomplished an IT bachelor's or master's degree and

[17] As an example, the ISC[2] organisation provides a resource list at https://resourceguide.isc2.org/educational.asp. Last accessed 20-09-2009.

[18] See for example a recently created Ethical Hacking Bachelor's degree in Northumbria University, UK Information available at http://www.northumbria.ac.uk/?view=CourseDetail&code=UUSETH1. Last accessed 9-10-2009.

afterwards they specialised in IT security via post-graduate education, either in the form of a doctorate or a master, or via on-the-job experience, especially if their end of degree dissertation dealt with an IT security topic.

Broadly, there are two main schools in IT security that coincide with the basic division of security profiles,[19] technical security and governance or process-related security. The first school requires a deep technical understanding of IT and the second school refers much more to governance processes and information security practices. The ideal provider is the one merging both schools and curricula or at least offering subjects from both worlds. Nevertheless, this is a first choice that the potential student has to take, to focus on the command line, hands-on IT security[20] or to stress the educational path to sharpen information security procedural and governance aspects.[21] The first school is also known as IT security engineering and the second option is known as information security management.

2.9 Alternative Paths to Obtain IT Security Expertise

Similar to what happens in most professions, there are alternative educational paths to get IT security expertise. The obvious one is on-the-job training. IT security is not an exclusive field to university students. Candidates willing to learn IT and showing big doses of soft skills[22] and sound analysis and synthesis skills can become excellent security professionals if they are mentored during several years by experienced "securiteers".

There is an alternative educational path that it is worth referring to. Professionals coming from the physical security world (military or law enforcement forces) constitute a very valuable asset for IT security provided that they understand and have expertise on IT or, as a minimum, that they are willing to get comprehensive IT training, comparable to a respectable IT bachelor degree.

The basic principles used in IT security have their foundations on older security-related disciplines[23] such as law enforcement, military strategy and fraud prevention. For example, principles such as defence-in-depth come from ancient military strategy.[24] IT is just a new field of application. The team will benefit from members with physical-security experience that are willing to join the IT field. This is also why it is not rare to find both teams, IT security and physical security, near each other in an organisation's chart.

---

[19] Mentioned in Section 2.2.

[20] For example, visit http://www.sans.edu/programs/msise/. Last accessed 20-09-2009.

[21] An example, visit http://www.isaca.org/Content/NavigationMenu/Students_and_Educators/Model_Curriculum/Model_Curriculum_Info_Sec_Mgmt_15Dec08.pdf. Last accessed 20-09-2009.

[22] Soft skills as mentioned in Section 2.6.

[23] As mentioned in Section 2.1.

[24] See http://en.wikipedia.org/wiki/Defence_in_depth. Last accessed 20-09-2009.

We can also find links between IT security principles and biology, and this is not only because of the use of concepts such as virus and worms in IT. The three-phased defence concept of prevention, detection and control used in biology is also repeatedly applied in security. Although it is rather unusual to find professionals coming from natural sciences willing to join IT security, this note is just to discourage any initial prejudice against any alternative professional field like biology, economics, statistics, sociology, psychology, physics and many more joining the team. Team leaders can recruit them provided that there is a patent declaration of intent that IT knowledge is or will be under their belt in the short or middle term.

2.10 What to Study

The syllabus varies depending on whether the focus is on IT security engineering or on information security management.

In the case of the IT security engineering path, we propose the following syllabus for an IT security bachelor's degree.[25]

Year 1

- *IT and business foundations*
- *Risk management foundations*
- *Security foundations*

Following what we have proposed in these first chapters, students will need to have a solid foundation on IT and business concepts, risk management methodologies together with the ability to understand what a vulnerability, a threat and a risk are. This first year will also present and work on the collection of basic security principles such as defence-in-depth, least required privilege, segregation of duties, audit and monitoring, four-eye principle and similar foundations.[26]

Year 2

- *Operating systems*
- *Networking*
- *Applications: Databases, web servers*
- *Scripting languages*

The second year goes deeper than the IT foundations. This means that operating systems, networking and application models will be the heavy weights of the curricula. Students will grasp these subjects applying a very practical learning approach with case studies, workshops and continuous assessment through lab assignments.

[25] A real example of the syllabus of an Ethical Hacking Bachelor's degree can be found at http://nuweb.northumbria.ac.uk/live/webserv/modules.php?code=UUSETH1. Last accessed 9-10-2009.

[26] More about security principles in Sections 4.2 and 4.3

Scripting languages and their link with the use of web-based applications and databases appear already in this second year. Students need to obtain a practical mastery in scripting. They will be automating security actions through scripting during their professional life.

Year 3

- *Security testing*
- *Intrusion detection*
- *Hacking methods*
- *Defence-in-depth techniques*

The third year is deals with security products and deliverables that organisations are currently demanding from IT security professionals. Focused, practical and value-adding topics that are increasingly requested by big organisations and that, rather sooner than later, will also be demanded by small and medium enterprises.[27]

For the information security management path, year 1 could be shared with the IT security engineering path. The proposal for years 2 and 3 would be:

Year 2

- *Information security standards and frameworks*
- *Project management*
- *Marketing and Security awareness communication*
- *Policy and procedure elaboration*

Information security management is tightly coupled with corporate compliance. Students need to familiarise with existing ISO standards and industry frameworks such as ITIL and COBIT. In addition to this, they need to understand and apply project management techniques since there is an important coordination element in information security management.

As we mentioned before, describing the security communicator profile, there are important awareness campaigns to perform within organisations. Information managers need to drive them as real marketing and communication activities, therefore, they require marketing and communication foundations.

This second year also includes learning points on how to write effective (policy) documents and procedures that can be applied, followed and, above all, accepted.

Year 3

- *Information security management*
- *Measuring and monitoring*
- *IT and corporate governance*

The third year for security policy-related students will provide a global conceptual umbrella on how to really manage information security and link it with IT strategies

[27] See Section 10.2

and corporate governance. A key element for this management task will be the construction of key performance indicators to monitor security events with the aim to measure progress and risks.

In addition to these subjects, we propose to enrich the syllabus every year with non-IT related disciplines where technical and policy students will be together. These are for example:

Year 1

- *Theatre workshops*
- *Writing workshops (analysis and synthesis)*

Security students need to be capable of making themselves understood both verbally and in written and addressing different types of audience (technical and business literate). They will need to get multiple references and inputs and, in a short time, understand the underlying process, share and discuss security views and produce recommendations themselves. This is why they need to practise their synthesis and analysis skills.

Year 2

- *Time management. Resource prioritisation*
- *Music foundations*

It is frequent to see security professionals drowning into endless to-do lists that are never completed. It is also very frequent for security teams to start multiple tasks and to leave them incomplete. We propose to provide students with a strong foundation on how to manage priorities, resources and, above all, time.

Why do we include music in this second year? Music[28] is a form of art using sounds that requires understanding harmony principles. It is also a creative activity completely different to all other proposed subjects. Students will benefit of this break and understand the importance of achieving harmony in their security activities.

Alternatively, we can also find similarities between reading a music score and trying to make sense of an encrypted text when doing cryptanalysis or understanding a piece of code.

Year 3

- *Public relations*
- *Psychology*

Non-IT proposals for the third year are much more focused on professional requirements. Security students need to understand and practise how to present ideas and gather acceptance or even leadership. Finally, understanding some notions of human psychology and how emotions and actions are related will benefit students in their professional lives.

[28] See http://en.wikipedia.org/wiki/Music. Last accessed 20-09-2009. We know prominent IT "securiteers" playing in a band as a hobby.

Students would continue after these 3 years with a year working part-time in a security team while they prepare their end-of-degree dissertation. This would consist of two independent elements:

– A practical paper on a security implementation performed in the hosting company.
– And an entrepreneurial proposal to launch a new security service or product.

To finalise this chapter, this radically different syllabus does not exist yet in any educational institution. We encourage decision-makers and governments to allocate resources to this idea that we will happily contribute to set it into motion.

The authors are convinced that innovation in security education will provide better value to organisations with a "business-aware IT securiteer": An individual capable of providing security expertise while understanding the surrounding context.

Chapter 2: Learning points

- IT security professionals are growing in number and importance.
- Two main types of profiles in the team: Technical and policy-related.
- There are more technical profiles than policy-related ones.
- Their technical skills are very specialised and profound.
- Their soft skills are as important as their technical skills.
- There are three main possible backgrounds candidates can come from.
- Security studies: Engineering or information security management.
- There are alternative paths to study security.
- Proposal of an alternative syllabus for an IT security degree.

Link to MBA Management Models

We have selected two HR-related models that could help us when forming and growing an IT security team:

Belbin's team roles model *(by Belbin, 1984)*
This model proposes that there are eight roles that interact to constitute an effective team.

Group development *(by Tuckman and Jensen, 1977)*
Groups undergo a lifecycle: Forming, storming, norming, performing, adjourning.

See references: Harding and Long (1998) and links:
http://en.wikipedia.org/wiki/Belbin_Team_Inventory
http://en.wikipedia.org/wiki/Group_development (Tuckman's stages 1977)

Chapter 3
The Team–Individual Contract

Chapter 3: What will the reader learn?

This chapter answers the following questions:

- What is the team–individual contract?
- Which basic principles contain this contract?
- How can team members create and grow their motivation?
- What is the internal balance theory we propose?
- How can a team be in harmony?
- How does motivation affect team performance?
- Why do leaders need to assess motivation and internal balance?
- What do team leaders need to care about the team as coordinators?
- How new colleagues join the team and former ones leave?

How to Create Win-Win Deals on the Team–Individual Contract

The IT security team consists of a number of professionals. These professionals are human beings. Each of them is an individual with their needs, expectations and feelings. The team will only perform well if certain conditions for each of its members are met. Team members need to find motivation to set security activities into motion and to lead them to a successful end. Frustration is a permanent threat to the team. The team leader needs to adopt mitigating measures against this threat. This chapter proposes a way to channel team members' motivation while looking after the reasons why a professional would join and work in the team.

A. Partida and D. Andina, *IT Security Management: IT Securiteers - Setting up an IT Security Function*, Lecture Notes in Electrical Engineering 61,
DOI 10.1007/978-90-481-8882-6_3, © Springer Science+Business Media B.V. 2010

3.1 Contract Between the Team and the Team Member

We consider in this chapter that the team leader role, the person in charge of the creation and maintenance of the team, plays also the security coordination role described in Section 2.4. Therefore, we assume that the coordinator has a clear interest to succeed in the creation and sustainability of the team. If both roles fall under different individuals, everything we propose in this chapter applies also to that scenario, with the additional requirement that both players need to be aligned with the team's objectives and need to succeed.

Even though the title of the chapter refers to the contract between the team and the individual, in reality the contract is based on a tacit agreement between two individuals:

– The professional joining the team, the newcomer.
– And the leader and coordinator of the team.[1]

The non-written terms and conditions that these two players agree upon will give shape to the nature of the membership that the newcomer will have in the team.

Harmony is one of the necessary conditions for the team to perform as expected. However, it can only exist if there is certain balance in the minds, spirits and bodies of its members. This is the reason why the establishment of the team–individual contract is so paramount.[2] Depending on those agreed terms and conditions, the individual will be able, or not, to find their balance and the motivation to achieve results within the team.

The contract we refer to is far more complex than a collection of written pages that two legal entities can sign and be bound to. The typically non-written part of the agreement between the newcomer and the team leader is as important as the written employment contract signed between the organisation and the employee. The next section suggests some key elements that this agreement should cover. Since this agreement is not written, it is necessary to communicate it right and avoid accessory noise. The greater the effort that the leader and the team member devote to shape this agreement, the higher the chance to keep and grow motivation on them (Image 3.1).

3.2 Basic Terms and Conditions of the Agreement: Creating a Team's Culture

Human actions are triggered by emotions.[3] The team leader needs to start off the right emotions in the professional joining the team. These emotions will constitute the initial hotbed for their motivation. They will enable the creation of an entire

[1] The culture of the organisation plays definitely a role in this context. See Chapter 8.

[2] Mallol (2008), p. 72.

[3] Damasio (1994), pp. 127–165, Chapter 7, titled 'Emotions and feelings'. As mentioned in Section 2.6.

Image 3.1 A basic contract will set the team member in motion

team within a professional working environment. We propose a set of basic principles that will nurture the team–individual contract and hence they will create a team's culture.

The first principle of the agreement is ***respect***. The individual needs to respect all other individuals present in the team and, broadly, in their working environment, not only their peers and colleagues in the organisation but also any individual they need to interact with during their professional career. We take this consideration to the extreme and we propose that they need to show respect towards any human being they communicate with. Respect is the base for every healthy communication. Although it seems an intrinsic human virtue, it is not always put systematically into practice.

Any show of lack of respect, such as a harmless shout at a colleague, or just an act of disdain, gives exactly the opposite message that security people need to broadcast: Calmness and sovereignty. A lack of technical savviness can be treated and improved. A lack of respect is much more difficult to treat, especially within a team that needs to work together from day 1 on.

The second principle of the agreement is ***transparency***. All team members need to be able to clearly grasp team and organisational aspects. They all need to realise that team leaders favour those members who work better or make a greater effort.[4] Any sign of opaqueness on people and team-related topics will endanger members' commitment with the team's mission. It is especially important to bring transparency to any decision made affecting team objectives, strategy and performance.

[4] Mallol (2008), p. 129.

Even if they do not agree, team members need to understand decisions and changes made in the team.

The third leg on which the agreement will rest on is ***responsibility***. Every team member is responsible for their activities. Whenever a team member starts off a task or answers a customer request, they are responsible for its successful ending. For example, devoting time and effort to hand over tasks to another team member before a planned leave or before a scheduled training is a simple demonstration of this basic principle. This seems to be an obvious subject. However, the team coordinator will need to invest plenty of energy to make this principle a reflex action in every team member's behaviour.

Challenging reality is the fourth principle. New members can bring fresh and new ideas to the team only if they are encouraged to air their thoughts,[5] concerns and make alternative proposals before they accommodate to the team's way of working. This is one of the few natural ways that teams have to evolve and team leaders need to look after it.

Provided that these challenges are respectful, structured and fact-based, the team coordinator should, at a minimum, devote some time alone or with other senior team members to scrutinise the validity and the possibility of implementation of every new proposal. If the team eventually adopts a proposal, then we suggest the "challenger" member be the one leading its implementation supported by the team's decision-makers. Should the proposal be rejected, then the team leader needs to objectively justify the reason of the non-acceptance[6] to the "challenger".

3.3 What Is Motivation? Herzberg and Maslow

Every human action has a specific direction and is framed within a specific behaviour. Motivation is the internal condition that sets that direction and activates that behaviour.[7] In the team, the leader needs to create the appropriate environment for every team member to find their inner motivation.[8]

---

[5] Mallol (2008), p. 129.

[6] As an addition to the terms and conditions explained here, Rudolph W. Giuliani in his book titled "Leadership" (Giuliani 2002) mentions the following relevant principles:

- First things first
- Prepare relentlessly
- Everyone's accountable. All the time
- Surround yourself with great people
- Reflect, then decide
- Underpromise and overdeliver

[7] See http://en.wikipedia.org/wiki/Motivation. Last accessed 20-09-2009.

[8] Motivation is based on the individual's autonomy, mastery and purpose. See Dan Pink's TED conference, available at http://www.ted.com/talks/dan_pink_on_motivation.html. Last accessed 9-10-2009.

A first step towards the creation of that environment, the "hotbed" for the motivation, is the establishment of the four basic principles.[9] A second step is to accept that this "hotbed" is different for each team member. The art of the team leader will be to amalgamate the necessary ingredients so that the majority of team members are motivated. It is only then when we can talk of motivated team members and harmony in the team.

Critical mass[10] is the minimum number of team members that need to be motivated for the team to make progress. The task of the team leader is to keep that critical mass stable and to increase it progressively.

The creation of this critical mass is a daily job for the team leader. They need to prepare the motivation's "hotbed". Herzberg[11] proposes hygienic factors and motivators.

Hygienic factors do not motivate individuals but their absence completely demotivates people. Hygienic factors are, among others, salary, administration, management, status and working conditions. Motivators motivate when they are present. Among others, some of them are achievement, recognition, responsibility, advancement, growth and nature of work. Hygienic factors and motivators are not equal for all individuals.

These factors are important to consider in every human team at work. They also apply in an IT security team. Although it is an overly rational exercise, in case of lack of motivation in a team member, a good first diagnosis action is to identify first which type of factors are present and which motivators are absent for their case. Hygienic factors need to be present before any motivator can trigger an effective (and motivated) behaviour.

Maslow refers to a hierarchy of needs.[12] He states that even though people have different needs, they all have similar fundamental need patterns. They are ordered in what he called a hierarchy of needs and human beings all move along this hierarchy in similar ways, depending on the circumstances that surround them. Starting from the most basic musts (lower in the hierarchy), to the most elaborate desires (higher in the hierarchy), we all have physiological, safety, social, self-esteem and self-actualisation needs. Basic needs are easy to satisfy and elaborate needs are not.

It is useful to diagnose where in this hierarchy each team member is located. With this analysis, leaders can make a plan to address clear needs so that the team member can worry only about their self-esteem and self-actualisation needs. These are the needs we expect team members can satisfy while providing value to the IT security team.

These two human resources motivation-related models help to find out the ***action source*** for each team member, including the leader and coordinator.

---

[9] Proposed in Section 3.2.

[10] We adapt the term "critical mass" using in nuclear chain reactions to the IT security team world. See http://en.wikipedia.org/wiki/Critical_mass. Last accessed 20-09-2009.

[11] Herzberg (1968), pp. 53–62.

[12] Maslow (1954, 1987), pp. 90–150 from edition in 1954.

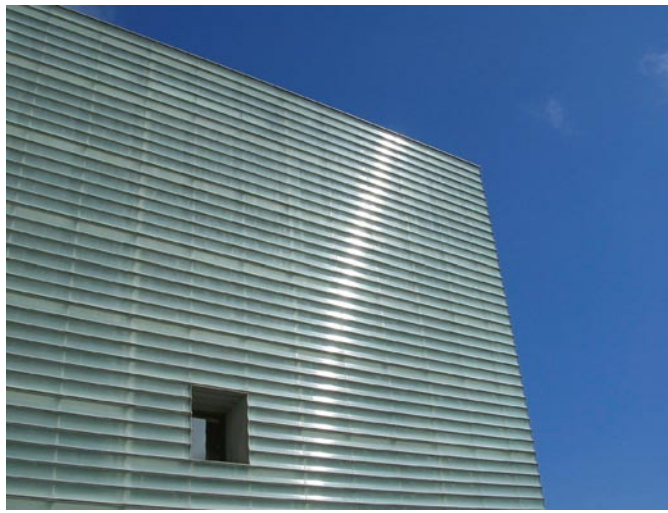

Image 3.2 Knowing what motivates the team member opens a window of opportunity

The ***action source*** is an x-ray picture of their motivation's health: For each individual in the team, the current status of their hygienic factors and motivators, together with their current location in the hierarchy of satisfied needs (Image 3.2).

As a first step, the team leader needs to find the ***action source*** status for every team member by talking and interacting with them. Second, the leader together with the team member will revisit the ***action source*** status at least every quarter. This suggested frequency applies to team members that are performing optimally. Lower performance levels require more frequent ***action source*** status check-ups.

3.4 Internal Balance in Human Beings

We tend to compartmentalise all the activities we do in our lives. We talk of Alice at work, Alice at home with her family and friends and Alice as a person. We all have a number of roles we play every day. All these roles are related to a degree that we usually do not suspect. We propose to talk of any act performed by an individual as the result of an emotion coming from three dimensions interacting among each other continuously: The work dimension, the social dimension and the personal or spiritual dimension.

With time, in everyone of us, these three dimensions need to be in balance. In the IT security team, this must also be the case. Only individuals with a balanced mix of their three dimensions can be motivated and aim at performing optimally within a team on a permanent basis.

3.4.1 The Work Dimension

It refers to the human being within their working relationship context. In the current society, the most frequent case for a large amount of people is that they need to work to pay up their bills, keep a certain living standard and, if possible, satisfy a professional vocation.

3.4.2 The Social Dimension

Human beings interact with each other. They need to share their victories, to celebrate them. People need support from their loved ones when they fail or have problems. Although there are different degrees of interaction, introvert and extrovert people, they all are social creatures that normally communicate with both family members and with partners, colleagues, friends, neighbours and any other human being living within their scope of daily interaction.

3.4.3 The Personal/Spiritual Dimension

Our brain hates the lack of stimuli.[13] Up to a point that, when we are sleeping, we dream so that parts of our brain keep on receiving stimuli and working with them. The way we feel, the way we are and the way we act are the result of a unique mix coming from our genes, our current and past environment and our expectations. This is what eventually constitutes our entity as human beings. Our personal/spiritual dimension.

Similarly to Section 3.3, we propose this three-dimensional model as a useful tool to analyse how the team member scores on each of these dimensions with the objective to offer a better win-win deal on their team–individual contract.

In the middle and long term, imbalances among these three dimensions produce suboptimal results in team members' lives and deliverables. We need, first, to assess where the leader and the team member are and, second, to re-visit the assessment on a regular basis.

We propose to use the models presented in Sections 3.3 (motivational factors and needs to satisfy) and 3.4 (internal balance dimensions) in regular interviews between the leader and each team member. In a forthcoming section in this chapter, we mention some unavoidable tasks that a leader needs to accomplish to locate their team's action source.

Nevertheless, every interview is a bi-directional communication process. This means that the leader needs to get ready to share with their team members their

[13] Lupien (2007). Video of her conference.

assessment using both motivation and internal balance-related tools. The interviewee will only consider the assessment process fair if both interlocutors, leader and team member, share their respective analysis.[14]

3.5 Identification of Internal Balance Coordinates

After introducing the three dimensions present in every individual's internal balance, we provide in this section a series of probing questions that assist team leaders to find out the position of each team member in this space. This assessment of the internal balance displayed by the IT security colleagues will help the leader to find clues that could eventually become collaboration threads and valid communication channels with each of them.

3.5.1 The Work Dimension

The IT security team leader needs to have an answer for three questions from each of the team members. It is not advisable to pose these questions as if they were part of a hiring interview. There is the risk of receiving a nicely prepared, almost standard, answer that would bring nothing to the assessment. Leaders should have possibilities to obtain an honest answer if they have shown trustworthiness and openness when creating the contract with the team member.[15]

Question a: *What do you feel most proud of among your latest work achievements?*

An honest answer to this question provides the team leader with valuable information to locate the team member within the work dimension. Human beings tend to devote their efforts and attention to activities they like. With this answer, they tell what they like at work. The leader should try to assign or create activities that are in line with the answers they give. As a minimum, they should have a chance to apply the knowledge and/or skills acquired and to live again a successful experience.

Question b: *Which latest failure at work you would not like to be repeated again?*

The team leader needs to analyse the replies and work hard to avoid that they experience a similar scenario while they are part of the team. Those scenarios can have negatives consequences both for the team member and for the entire team. Leaders should provide team members with tools that could improve their resilience,

[14] The "Johari window", a cognitive psychological created by Joseph Luft and Harry Ingham in 1955 in the United States to help understanding interpersonal communications (see http://en.wikipedia.org/wiki/Johari_window. Last accessed 20-09-2009.). Using their terms, we propose leader and team members to locate themselves in the "arena" perspective (compared to the blind spot, façade and unknown). West and Turner (2008), p. 274.

[15] See Sections 3.1 and 3.2.

should they face a similar failure event. As an example, their resilience could get better if they train their communication skills, their presentation skills, their empathy or their ability to see the global picture: Does the organisation fulfil its mission and are the team's goals aligned with the organisation's goals?

Question c: *It is Sunday evening and you think about the work that is expecting you next morning in the office.… How do you feel about it?*

The answer to this question tells the leader whether they are happy with the work they are currently doing. If the leader identifies unhappiness in the interviewee, and they are a professional worth keeping in the team, the leader's priority will be to arrange a new contract with them[16] that would improve their situation and their happiness in the team, e.g. new tasks, different desk, new training objectives or simply a brand new way of communication between them and the leader.

In addition to this, the answer also tells to which of these two groups of professionals they belong to:

- Those that are passionate for their work at the office.
- Those that exchange their time and professional effort just for money, status or even better, to be able to work at what they are really passionate for after leaving the office.

Every human being is ready to devote a huge effort and a great dose of attention into any activity they are passionate for. Passions are the opposite to obligations.

About the fact of being passionate or not for the IT security job, most teams have both types of professionals. It is healthy to have both working approaches in the same team.

Leaders should provide to people passionate for IT security the possibility to excel and go deeper in their passion. They should encourage them to publish papers, to make presentations at security conferences, etc. For example, if they like coding and they have good scripting skills, they will welcome encouragement to go and devote extra time to find zero-day vulnerabilities in popular pieces of software. They could afterwards report them following responsible vulnerability disclosure principles and their professional reputation would increase inside and outside the organisation.

Those professionals that work in the team but they are not really passionate for IT security need to feel that their high-value deliverables are adequately rewarded. For them, work is a means to be able to live their real passion outside work but they also need to see they are highly appreciated in the team.

The belief that IT security teams need to consist purely of IT security passionate members is unrealistic. There will be critical tasks, including activities based on stringent procedures such as incident response, in which non-passionate professionals, given their emotional detachment, can perform even better than passionate professionals.

By the way, leaders should try to find out the passion, other than IT security, that these team members have, be it nature, sports, theatre, arts.... It can facilitate the relationship with them and eventually unveil that, maybe, they have a similar passion.

[16] See Section 3.1.

3.5.2 The Social Dimension

This assessment intends to identify the degree of social interaction the team member feels comfortable with. Again we propose three questions to perform an initial "triage":

Question a: *Remember an important academic or business-related occasion you lived lately (e.g. your graduation day, a promotion at work, etc.). How did you celebrate it?*

The number of people they mention in the answer, their relationship with the individual, the way they celebrated and the occasions they remember provide input to assess whether the individual is definitely a people person or rather an introvert subject with a small but very loyal group of friends or any other type of person between these two extremes.

The magic recipe regarding this topic consists of trying not to move the person out of their comfort zone. Considering the entire team, team leaders need to build a cluster of reasonably different but not conflicting social behaviours.

Question b: *In your past but recent working experience (or study experience if they currently live their first working experience), how often did you meet with your colleagues outside the office?*

The frequency they mention in their answer helps team leaders positioning the individual within the team's behaviour spectrum. Leaders should bear all team members' answers in mind when planning social activities with the team outside the business context.

Question c: *This question only applies to those team members who have been working with the team for longer than a year. Did you celebrate this year your birthday with your team peers?*

Smart leaders make an attempt to answer this question just by checking with other senior team members to avoid posing the query directly in the interview, which could be seen as a clumsy and indiscrete act. The telling fact on this topic is change. If they used to do it before but they did not plan it in the last year, it could mean that now they have a reason, maybe a demotivating experience lived in the office, not to do it. It is the leader's task to investigate this.

3.5.3 The Spiritual Dimension

What keeps our brain busy? To assess this dimension we propose a cognitive technique used in psychology lately to handle generalised anxiety disorder[17]: *The descending arrow*. It consists of a series of chained questions and answers, all of them around the sources of worry for the individual. A practical example would be to start a conversation with the question "*what worries you at this moment*?".

[17] Öst and Breitholtz (2000), pp. 777–790.

Image 3.3 Leaders need to locate every member in the team's map

Using the precise answer to this question, the interviewer asks again "*from this answer, what worries you precisely if that situation takes place*?". This technique continues up to a point when the one or two most basic worries of the individual are patent.

With all the leads obtained by following this internal balance assessment, the IT security leader can locate team members and themselves in the three internal balance dimensions. As advised in Section 3.3, the assessment is a continuous process with regular check-up sessions[18] throughout the working year (Image 3.3).

Team leaders should not underestimate the amount of time, attention, care and energy that this continuous assessment deserves and requires. They always need to summarise the interviews using written notes for the record and share them with the team member.

Behavioural Guidelines for Team Leaders

The leader of the team has a set of objectives, a mission, to accomplish with the help of all team members. The leader alone is not able to accomplish the mission. Leaders need to lead by example and, slowly but surely, need to bring team members onboard and, although some voices argue that tasks can be imposed, we are certain that nowadays no activity can be bluntly imposed to any professional.

Imposition works once and only for a very short time and team leaders need to care for a durable team. This is the reason why it is of great importance for the leader to follow the behavioural guidelines we propose in the coming sections.

[18] Check up sessions can also happen without holding a formal meeting.

Together with the principles we suggested in Section 3.2, they constitute the recipe towards creating a dependable IT security team working for a long-term mission.

3.6 Communication, Communication and Communication

This is requirement number one for the leader. They need to understand how communication among human beings takes place. They communicate with their voice, body language and words.[19] Leaders' communication acts need to be predominantly face to face and verbal. If their organisational guidelines advise to communicate in written, using memos or email, they need to follow those guidelines, for the record, but also to do it verbally.

All of us receive much more valuable information in a face to face communication. Precisely, what makes sometimes emails be misunderstood, giving ground for conflict, is the lack of body language and voice features.

When leaders communicate, they need to show that they care as they would like that their colleagues would care for them.[20] Leaders also need to let the team know that they are personally committed with the team's mission and with everyone in the team. Their permanent communication task is sharing their conviction that the team will succeed with all team members.

Leaders should remember that they first need to give, and maybe, later on, they receive something valuable in exchange.[21] Their body language needs to show conviction and their voice needs to transpire assertiveness in their communications. Human beings at the receiving end of the communication channel will instantly notice it if this is not the case. And, what it is worse, team members will spot it and will act consequently, be it working with less interest (as the leader showed in their communication), be it preparing their leave if this is a permanent situation.

Introvert individuals can be good team leaders, but they would need to fine tune their communication skills from day 1 in office. We propose the following practical tips to communicate:

- Preparing the script beforehand, even if it is only a mental sketch of what the message will be.
- Rehearsing the pitch in front of a mirror (or using a video camera). Reality can be cruel.
- Keeping messages short and to the point.
- Avoiding boredom among the audience.
- Providing anchors with examples or visual aids to reinforce the message.
- Above all, avoiding monologues. They are the main source of jokes among team members.

[19] According to Atkinson (2005), Chapter 11, figures are: Tone of voice: 55%, body language: 38% and words: 7%.

[20] Mallol (2008), p. 202.

[21] Mallol (2008), p. 202.

3.7 Time Availability for the Team

Team leaders and coordinators interact many times a day with team members. It is on them to foster and to reward the behaviour that favours face to face interaction against email exchange. The latest research studies performed on group dynamics show how human beings feel comfortable being part of groups consisting of 5 to 8 people.[22] If the team has a higher number of members, it is time to create mini teams within the team, probably with different but synchronised leaders.

It is possible to postpone contacts with team members for 1 or 2 days if there is an urgent topic requiring the leader's attention: An IT security incident or imminent problems with the budget. This lack of rapport with the team should not be longer than a week, or even the length of some holidays. When the leader is back in body and mind, they need to take up again the personal contact with their team members. This requires the leader's attention and time, and it has priority over reading emails.

Leaders should acknowledge that a leadership role requires a predominant human contact element every working day. This is probably different from their previous position if they come from a technical job in which their objectives depended mostly on their technical knowledge and not on other people's performance.

3.8 Adoption of Preventive Measures for the Team

Apart from usual business related follow-up meetings with team members, leaders need to plan frequent motivation and internal balance assessment sessions.[23] They need to devote sufficient time to these assessments. On average, the first sessions could take longer than 60 min, and, once everyone is familiar with the process, between 40 and 50 min.

Every team member should have the opportunity to talk to the leader privately every 8–12 weeks. This frequency will be inversely proportional to the degree of seniority and synchronisation already existing between each of the team members and the leader.

Mastering these sessions is a complex skill that the leader needs to acquire. Team members and leaders should benefit from each follow-up session. Members need to feel that sessions are tailor-made for their particular traits and leaders need to receive valuable input to know their team better. The threat to mitigate is the possible belief that these meetings are part of an unfair way the leader has to obtain privileged information to micromanage every single aspect of the team.

---

[22] Van Vugt et al. (2008), pp. 182–196.

[23] Introduced in Sections 3.3– 3.5

Finally, leaders should be aware that sharing an evening or a weekend, every now and then, with the team, outside a business context, can provide them with valuable input on how they feel and what is worrying them. Actually, assessment sessions after a social event are much easier to steer. These social gatherings contribute to create rapport between the team and the leader. The leader will be seen as much more approachable and human.

3.9 Proposal of Mentoring Services

The leader's experience both as a team coordinator and as an IT professional can be very useful for the professional development of most team members. Proactive leaders need to inoculate the desire for a continuous professional and personal growth among team members.

However, not all members will appreciate that their coordinator would propose areas for improvement, or simply, to develop from scratch because they just do not have those skills. Therefore, to avoid conflicting views, leaders should simply offer their mentoring services, without imposing them, to those members that are truly interested in receiving this, and sometimes not-nice-to-hear, input.

Typical examples of voluntary and advisory career developing services are:

- Acquiring foreign languages reading, speaking and writing skills.
- Tips to improve slides used in presentations.
- Advise on how to present in public.
- Ways to prepare and present a resume and a job interview.
- Specialised IT security fields in which the team member could excel if they make an extra effort such as forensics, malware analysis, vulnerability testing, secure code development, etc.

Usual candidates that will benefit from these services are trainees and junior professionals with the drive, will and time required to develop further. After all, coming across former team members and confirming that they have progressed personally and professionally gives team leaders a feeling of usefulness and realisation and, why not, also some doses of healthy pride.

3.10 Care but No Intervention

Every human being is unique. We all perceive reality differently. Conflicting views, verbal collisions and clear disagreement will appear among team members. All team members need to accept this reality.[24] The leader's task is not to try to solve

[24] Chapter 6 provides complementary input on this fact.

Image 3.4 Leaders need to monitor closely their team

every single misunderstanding created within the team but to veil that the principles mentioned in Section 3.2 are always respected by all team members.

The leader's intervention is required only in those episodes when a team member has a valid reason to ask the leader to take part on it or when it is patent that the basic principles of respect and coexistence have been neglected (Image 3.4).

3.11 Design of Easy Processes and Assignment to Wise People

Following steps within any process is not a task that human beings perform well and at ease unless there are a certain degree of interest and a certain extent of repetition. This is why important processes happening at critical moments, such as a plane taking-off and landing, are performed following checklists and agreed procedures. Pilots follow precisely these checklists on every occasion.

Within IT security there are also critical processes that teams need to perform with high quality, be it responding accurately to a security incident, providing the requested access rights to an end-user or reacting to a security monitoring alert.

Complexity will arise in reality from unexpected sources. Processes in place should not add on to this complexity. It is the leader and their senior colleagues' task to design and establish easy-to-follow processes and to place wise professionals in key positions to foster their implementation within the team[25] with the objective to manage encountered complexity.

[25] Mallol (2008), p. 202.

3.12 Public Praise Sessions and Private Criticism

Everybody makes mistakes. Team members and leaders will also make plenty of mistakes. Everyone needs to accept mistakes and failures made by the team. The leader's smart move on this topic will be to make the team, as a collective entity, and team members, as individuals, learn from mistakes.

The problem is not that the team make the same mistake twice or even more times. Team leaders always need to support the ability to rectify, learn from mistakes and show understanding to all team members. The real issue arises when mistakes are accepted as a common way of working and even institutionalised within the team. The leader's role is to avoid that situation.

There will be occasions when the team leader needs to have a serious conversation privately with the author of a mess. Leaders should objectively criticise, always based on facts, not on personal traits. In order to be able to demand a change of action for future occasions and obtain the team member's commitment, leaders need to take written record of the agreed mitigating and improving measures and the date when a follow-up session will take place.

The other side of the coin is much more pleasant. There will be successes to celebrate within the team. When there is a clear achievement thanks to a team member's decisive action and resolution, the leader needs to praise them in the next group meeting and add a basic learning point in order to make the team aware that similar efforts and behaviours will always be rewarded during their leadership.

Rewards can take multiple forms, from a more flexible working schedule arrangement (depending on the organisation's guidelines, leaving early on certain occasions or allowing tele-working during valley seasons could be two effective examples) to full support for a team member to obtain a wished training measure. Leaders should not underestimate nor forget the need to reward their best performing members. Being forgetful on this topic can lead to a generalised lack of motivation.

3.13 Support of Team Members

As stated in Chapter 1, IT security professionals keep a complex relationship with the organisation they work for. They should make the organisation's decision-makers aware of the risks they run and provide advice on risk-mitigating measures when actually the basic nature of every business is taking risks.

Each team member requires the leader's support in any potential conflict with colleagues outside IT security. This support is a pre-requisite for the continuity of the leader.

If the team leader finds that some security measures proposed by the team member are actually going too far and, given the nature of their organisation, they really

hamper critical business processes, it is the leader's task to make the team member see the gap between their theoretically impeccable stance and the organisation's reality. However, leaders should always perform this Socratic exercise privately and not in front of other colleagues outside the IT security team.

The leader's full support to the team member, specially when working parties external to the team are present, is key to show non-IT security colleagues that the leader cares about their team members' work. Full support does not always mean to start with an open confrontation against the other party. A good example to show non-conflicting support can be applied to those chains of nasty emails in which one of the team members' proposal is challenged, but not based on facts, by a project manager or someone in the middle management layer within the organisation, with simply different objectives than the IT security team.

Even though the leader's first reaction (coming from the reptile side of their brain) would be to fire back with a blunt email, it is key that leaders let time to the rational evolved side of their brain to simply relax, sleep over the topic and advise the team member not to embark on those endless time-consuming email chains. Effective IT security leaders should encourage the use of the email exclusively to convey facts and to appreciate a colleague's work.

Some of the conflicts affecting the team will disappear without the need to apply any energy to them. They will simply lose momentum or become obsolete. Some others will stay and will require the leader's attention. We recommend high doses of meditation and strategic fact-based decisions to solve or just to skip them.

Resourcing the Team

3.14 New Team Members Joining the Team

In this chapter we have suggested ways to optimise the relationship among team members and the leader as a necessary foundation to obtain high-value performance. The proposed recipe started with some basic co-existence principles and continued with assessments based on motivational theories and an attempt to comprehend balance in human beings based on three dimensions.

Given the importance of the leadership role, we have suggested a set of guidelines for the team leader. The last element to introduce in this team-individual puzzle is how to identify potential new team members. These last sections of the chapter deal with key points to consider when welcoming new team members and when saying goodbye to current team members.

It is healthy to keep a flow of professionals joining and leaving the team. Newcomers' motivation is unique and the experience leavers gather outside the team is valuable for the entire team, should they return.

3.15 Profile Preparation for a New Team Member

A pre-requisite to welcome a new team member into the team is to design the position they are going to occupy. The design includes the following aspects:

1. Activities the newcomer will perform.
2. Length of the engagement.
3. Technical skills required.
4. Soft skills to benefit the team's balance.
5. Name of the mentor and guide through the organisation.
6. Physical location.

The main source of answers for questions 1–3 is the strategic plan[26] the team follows. Points 4–6 refer to the overall results of the assessment exercises proposed in earlier sections of this chapter.

3.16 Advertising the Vacancy

Once there is a definite design of the profile, the team needs to advertise the vacancy. Our recommendation is to spread the word through every team member's formal and informal networks: Professional communities, former colleagues, former managers, former teachers and professors, relatives, neighbours, etc. 'Word of mouth' can save time and potentially provide an optimal candidate.

Good professionals, like good students, leave a halo behind them that people remember and professional communities are not so numerous. There is always a chance that someone in the team knows a person who could match the position's requirements and that person is available or, simply, willing to take up a new challenge. Chapter 9 in this book talks about the intricacies of networking inside and outside the organisation.

The second way to announce it is by posting the vacancy in reputable fora. These vary from general purpose mass newspapers or professional magazines to online IT security job sites. The organisation itself, inside and outside the IT department, is also a valid source of applicants, especially considering the learning points proposed in Chapter 2.

3.17 Assessing Applications: Three Basic Principles

The effort required to go through all applications received depends on the number and quality of the applying candidates. If there is no budget planned to advertise the position and team members are not 'sufficiently networked',

[26] Chapters 4 and 5 provide additional input on strategic plans: What an IT security team needs to do in an organisation and how to do it.

maybe no application is received or just a handful of them that do not really meet the requirements.

A golden principle is not to be satisfied with non-matching applications. The temptation to quickly fill up the vacancy and finalise the selection process is attractive but experience shows that this type of non-matching candidates distract the team and require additional attention and guidance from the leader and other senior team members.

It is preferable to wait a few weeks and use the same channels to advertise the vacancy again. Maybe this time the right candidates would be available and attracted by the offer.

A second principle to follow is to pick only someone that the team needs, not someone, with no skills, that the leader thinks they need the position the most. This type of noble acts endangers the good spirit and working terms created within the team. On the long run, these candidates prove to be detrimental for the professional development of the team members.

Finally, a third principle is not to overgrow. Contrary to current business trends, that value importance and relevance of groups, and specially 'organisational weight' of managers, purely based on headcount figures, effective IT security teams can only grow at a certain slow pace. The degree of cohesion required and number of shared goals in an IT security team does not connect well with excessive growth rates.

We suggest that security teams should not grow more than 30% in headcount per year. Higher growth figures mean that a new team is created and hence, an entire team building process, starting from step 1, will be required.

3.18 Preparing the Selection Process

The team member who will mentor and guide the newcomer through the organisation leads the preparation of the selection process. The selected mentor, together with two or three senior team members will form the selection panel. The presence of a colleague coming from a business area or from a different IT team is also recommendable, even if they only act as observers. Given the central role that the team leader plays in setting up the team's culture,[27] they need to be one of the panellists in the first processes and for those vacancies designed to be occupied by senior professionals.

The selection panel, as a collective body, should have the skills demanded in the vacancy. Maybe this is not the case on a specialised technical aspect, but at least the panel needs to have a sufficient degree of knowledge to identify valid answers to the technical questions posed to the interviewee.

Once the selection panel is formed and the candidates potentially matching the required criteria have been short-listed, the future mentor shares with the rest of the panel the selection process that they have designed. The more effort and care

[27] See Section 3.2.

frontloaded in the preparation of the assessment process, the greater the possibility to succeed in the selection of the new team member.

The assessment process should verify these points:

- Required technical skills are present in the candidate. As a minimum, if the newcomer did not show mastery of those skills, the selection panel needs to be convinced that the newcomer is in the position to acquire them in a short period of time, given their proven IT background and their demonstrated learning skills.
- Soft skills required to work in the team and to keep up with the team spirit are present in the candidate. Although specific technical skills can be quickly learned if there is a strong technical foundation, sufficient analytical skills and a great dose of willingness, soft skills are much more difficult to improve in a short period of time. Though possible, we do not recommend this soft skill learning process taking place within the working environment of an IT security team.
- The candidate's ability to analyse and synthesise are sufficient to fill the vacant position.

3.19 Elements of the Selection Process

This section introduces a set of example tests that could be used in selection processes. They do not pretend to be comprehensive but they constitute a handy toolbox, already put into practice for selection processes.

3.19.1 Day 1 Test: Phone Interview

After the application filtering process, the panel runs a phone interview with a handful of short listed candidates. Each candidate is given a 30–45 min slot for the phone interview. Schedules are organised several days in advance. This gives the interested candidate the chance to gather information about the organisation. Equally, we recommend gathering intelligence on the candidate using the Internet to search for details presented in their resume.

The entire selection panel is present and the interview consists of the same elements for all short listed candidates to ensure objectivity. The future mentor leads the interview and the rest of the panellists always participate asking clarifying questions. An element in the mission of the interview leader is to make the interviewee feel comfortable during the entire conversation. The skeleton of the phone interview could be the following:

(a) To start with, the candidate is asked to walk through their resume in 3–5 min. The panel assesses the adequate length and the content quality of the answer. Usually, the main points mentioned in this summary are good leads to establish a good understanding channel with the candidate afterwards.

(b) The following 5–7 min are devoted to clarify with the candidate those points that seem somehow obscure or confusing from the reading of their resume or from their introductory exercise.
(c) The interview continues with a description made by the future mentor of the vacant position to set the scene and to confirm the candidate's real interest to it.
(d) All panel members now proceed to ask a series of technical questions. These questions are prepared and agreed beforehand among all panellists. Questions and answers are distributed to the entire panel before the interview. We suggest to raise two types of questions:

   – A few questions that the candidate can answer with a 3–4 min speech if required.
   – A battery of short questions whose answer is only a word, a sentence or a brief reference to a concept. These quick questions should be asked at a fast pace.[28] They are designed to find out whether these are concepts the candidate masters and uses on a daily basis.

(e) The interview goes on with two or three situational questions to try to find out about the candidate's soft skills. These questions are set in the past tense and they look for concrete examples. When the candidate talks about a specific episode is much more telling than when they provide generic statements. This is only an initial and rudimentary attempt. It is easy for candidates to make the panel believe that they are terribly nice people. Nevertheless, these questions are a useful tool to discard clear cases of arrogance, lack of team spirit, lack of commitment or simply lack of understanding. Examples on these questions are:

   – *Tell the panel how did you react that recent past day when you were the last team member leaving office on a Friday evening and just when you got out of the building, your top manager came across you and asked you to amend a firewall rule in production. If you have not experienced this situation, imagine you did. How would you feel about it?*
   – *How did you recently deal with a working colleague that always tried to escape from real work? In several occasions you did cover up their mistakes claiming authorship in front of your manager. If you did not live this episode, how would you react if you would?*

(f) Finally, the panel leader gives the candidate the opportunity to ask the panel about the job, the team and the organisation. Motivated candidates use to ask smart questions in this section of the interview.
(g) The phone conversation concludes with the commitment from the panel leader to revert back to the candidate, preferably by phone rather than via e-mail, on a specific date with the result of the assessment. It is important to fulfil this commitment.

[28] With enough time, some candidates could make use of Internet tools such as Google.

3.19.2 Day 2 Test: Tests and Face to Face Interview

A subset of the candidates interviewed through the phone will reach the second part of the selection process. This time candidates come to the team's facilities where they take a series of written tests and a face to face session with the selection panel. We propose three exercises. Each of them with a time limit of 45 min:

(a) A first written exercise assesses the candidate's reaction to an information flood. Currently, it is part of every IT job to research on a topic using public databases and resources, such as the Internet, and to construct an informed decision based on ad-hoc information produced out of filtering through vast amounts of data in a very limited time. The panel can take the chance of this exercise to deal either with a very specific technical topic or with a non-technical topic that could serve as a valid excuse to afterwards scan the candidate's views on determined soft skills or human dynamics. In both cases, the panel should provide the candidate with vast quantities of data and ask them to make sense of them within a short time.
(b) The second exercise consists of a case study. The candidate has to choose one out of three different proposals related to the technical content of the position. All panel members know the case study and the possible answers in advance.
(c) The third exercise consists of a face to face interview with the selection panel. They give the candidate the opportunity to clarify their answers given throughout the first two parts of the written exercise. The selection panel normally requires about 30 min to gather together and assess the candidate's answers. During this time, we recommend that someone from the team, a trainee or a junior professional, looks after the candidate and offers them some small talk to relax. Afterwards, smart panel leaders would also seek feedback from the team member minding the candidate. Day 2 tests end with this clarifying session. The panel leader informs the candidate about future steps of the recruitment process. These are some useful questions for the panel in this final session with the candidate:

   – *What is your impression about the entire selection process?*
   – *How did you deal with a permanent lack of time to answer exercises today?*
   – *In your view, does this assessment process reflect the best of your profile? Is there anything you wish to add?*

(d) We recommend panel members to hold a brief wrap-up session right after the interview to share impressions about the candidate.

After interviewing all pre-selected candidates and scoring their answers, the panel members will gather together and share their ranking of selected candidates. The panel leader will contact the first preferred applicant to confirm their final interest in the position. Should the offer be declined, then the panel leader will contact the second preferred candidate and so on and so forth.

3.20 How to Say Goodbye to the Team

It is healthy for the team to let members come and go. Team members need to stay in the team because they like what they do and what they experience and not because it is difficult to leave the team or to find another job. The same way new professionals join the team, current members, sooner or later, some of them, due to promotion, personal needs or different career development paths, will leave.

The learning point here is that the world is very small, and specially a professional community such as IT and IT security. It is very likely that professional paths will converge again in the future. Team leaders should avoid criticism when a team member leaves. It is the ideal occasion to offer the leaving colleague the possibility to air their impressions on the experiences gathered during their working time in the team, the proposals to improve the team and also, if the situation allows for it, their expectations on the new job (Image 3.5).

They will provide valuable information for the team leader and for those remaining in the team. The script to follow in this exit interview is simple: The leaver organises a meeting with the leader some weeks before the departure in a neutral place, a meeting room where both will be comfortable, not in the leader's office, with sufficient time for the chat. It is convenient that the leader takes notes in order not to forget key points of the conversation. In optimal cases, the team leader loses a colleague and, at the same time, wins a friend.

This section finalises mentioning that team leaders also leave teams. Many reasons can lead them to that decision (family, career changes, new opportunities, etc.). Our advice to leaders is that they should only leave when they feel that they have finalised their main task and not earlier (e.g. creating the team, streamlining

Image 3.5 Professional paths are inextricable

their processes, re-invigorating team members, etc.) so that they can close an entire chapter in their professional career and be proud of it. Nevertheless, every leader should prepare their succession from the first day they take up their position. We suggest team leaders to identify several potentials deputies and progressively assess them and prepare them to take up more responsibilities within the team.

Chapter 3: Learning points

- The team–individual contract sets the context for every team member.
- Respect, transparency and responsibility are basic principles.
- Every team member has their motivational factors and needs.
- We all have to balance our work, social and spiritual dimensions.
- Team harmony requires internal balance in individuals.
- Only motivated team members deliver lasting results.
- The assessment of the individual helps the leader to build the team.
- Team leaders need to communicate and act by example.
- The greater the effort to select newcomers the better chance to succeed.
- IT security teams should not overgrow rapidly.
- Leaders should welcome newcomers and thank leavers properly.

Link to MBA Management Models

In Section 3.3 we have used two HR-related models to assess the individual's motivation and needs.

Herzberg's hygienic and motivational factors (1968).
Maslow's hierarchy of needs (1987).

See references provided in Section 3.3.

Chapter 4
What to Do: The IT Security Roadmap

Chapter 4: What will the reader learn?

This chapter answers the following questions:

- What do IT security teams need to do?
- Which principles should team members follow?
- How vulnerable is the customer organisation?
- What are the organisation's threats and who are their adversaries?
- How should IT security teams prioritise their activities?
- Which security services should an IT security team provide?
- Which teams exist within the IT security team?
- Which activities should IT security teams avoid?

Chapter 1 has dealt with the mission of an IT security team that provides real value to the business. Chapter 2 has described the technical and soft skills that the team requires and Chapter 3 has suggested a possible way, anchored in motivation and internal balance, to make a team out of a group of professionals. Chapter 4 provides guidance upon the specific activities to perform in the team and Chapter 5 will complement these learning points with practical recipes on how to accomplish these activities.

A. Partida and D. Andina, *IT Security Management: IT Securiteers - Setting up an IT Security Function*, Lecture Notes in Electrical Engineering 61,
DOI 10.1007/978-90-481-8882-6_4, © Springer Science+Business Media B.V. 2010

Founding Activities on Principles

4.1 IT Security Teams Should Not Occupy Their Days Mostly with "Fire Alerts"

Nowadays IT security teams' working days, especially in teams with a recent creation date, often resemble those of a fire brigade: They are ready to engage in any security incident or topic that unexpectedly affects the organisation. The trigger could be a real security incident, and this is certainly a valid reason to jump on it, but frequently the sudden action request comes from a relentless management layer or project team, especially few days, or even hours, before their initial go-live date.

It is possible to maintain this hectic approach in a team for several weeks or even months. However, in the long run, the mandate and continuity of the IT security team are in danger with this "firemen brigade" way of working. This "modus operandi" results into many unsatisfied customers and very soon into frustrated team members: They feel themselves overloaded, discontent and under an extreme degree of pressure exerted by their customers and managers. Eventually, their stress makes them frequently sick and it even invites them to leave the team and the organisation.

We have hinted smart ways to avoid this reality.[1] The following sections of this chapter go deeper into the activities on which an IT security team need to focus. A team with a smart portfolio of activities soon produces visible outputs and let every decision-maker in the organisation understand that they would obtain a higher value if the IT security team work following a roadmap rather than a sudden request of questionable importance.

4.2 Basic Security Principles: The Foundation of the IT Security Activities

Chapter 2 includes the concept of "security principles" as a piece of knowledge that IT security profiles require[2] and mentions some of them such as segregation of duties, four-eye principle and least required business privilege.[3]

A pragmatic way to select what to do in the team starts with the enumeration of the basic security principles that an IT security team should follow. The list presented here, though not comprehensive, covers most of the aspects to work at.

There are occasions when IT security professionals are questioned about the reason why a measure needs to be implemented. Referring to these security principles

[1] See Sections 1.14–1.19.

[2] See Sections 2.2 and 2.3.

[3] See Section 2.5.

constitutes a plausible answer. They are part of ancient foundations in military strategy and information security.

These are the two main principles to guide the IT security work.

4.2.1 Defence in Depth

This is a traditional security principle[4] that states the need to rely on a series of security measures, preferably distinct in nature or mitigating risks in a different manner, and not only on one single security feature. The reason to follow this principle is to have a higher guarantee that there will be no breach even if one of the security measures fails.

It is easy to witness this notion outside the IT world, e.g. to withdraw money from an ATM, we first insert our credit card and enter our pin number (something we know). If someone steals our credit card, they would still need to know the pin number to get cash from an ATM. These two security measures (something we have and something we know) are easily defeated if thieves clone our card and record the keys we pressed. This is why the principle of defence in depth needs to be applied for possible and probable threat vectors.[5]

4.2.2 Protection of the Crown Jewels

On the one hand, not everything in an organisation has the same value. A company could continue its business processes without, for example, two TV monitors but maybe it would struggle to survive without its customer database. Consequently, assets with unalike values require different protection measures. We all follow this principle unconsciously: We maybe leave our winter gloves visible and unattended in the car but we do not normally leave our brand new mp3 player unattended in the car seat while we go shopping.

On the other hand, there are never sufficient resources to protect every asset with an endless number of security measures. It is central to identify the "crown jewels"[6] of the organisation and to apply appropriate security measures based on the "defence in depth" principle with the budget that is available. The IT security team

[4] The SANS Institute training philosophy is also based on this principle. See Stephen Northcutt's Security Laboratory: Defense in Depth Series at http://www.sans.edu/resources/securitylab/threat_vector_did.php. Last accessed 20-09-2009.

[5] A threat vector is the way a potential cause of an incident may result in harm to a system or organisation (Adapted from ISO 2004, pp. 1–28).

[6] SANS Institute training philosophy also includes this principle.

Image 4.1 The onion approach: different layers to defend the "crown jewels"

have to protect these "jewels" with care and attention.[7] They are the reason why the organisation, and the team as such, exist.

Team members also need to be aware that there are assets in the organisation with relatively low economic value but with great "reputational relevance".[8] We take an example of "emotional assets" present at home: Our digital photos are only a set of bits in a memory device but, for most of us, their theft would mean a big loss, probably even more significant than the loss of the hardware where they are stored.[9]

Organisations have very few "emotional assets" but they do have a number of "reputational assets" whose loss, modification or exposure could damage their public image (Image 4.1).

4.3 Additional Security Principles

Together with the described basic principles, there are other tenets, mostly coming from information security techniques, which are also worth mentioning.

[7] See Section 1.17.

[8] See Section 1.18.

[9] Applying the defence in depth principle in this scenario, we would recommend to keep a backup of these photos in a different physical location, e.g. in a relative's home.

4.3.1 Least Business Privilege Required

This principle proposes to provide business users only with those access rights they require to perform their duties. Its implementation requires breaking down the access right model into single fine-grained units that represent each of the different access rights used in the organisation.

The objective of this principle is to avoid users having access to systems or data they do not need for their daily functions, fostering data confidentiality. For example, only certain HR-related colleagues would have access to staff members' personal records.

An extreme application of this principle can bring an organisation to a real paralysis, where there are as many different access rights profiles as users exist in the system. The management of these rights becomes resource-intensive and error-prone. This is why current identity management practice proposes the use of a role-based access control model.[10]

In some business areas, IT system administrators must not have access to business data. This requirement brings additional efforts and cost, e.g. implementing encryption for data areas while keeping system areas accessible to administrators so that they can support and make the system available.

Depending on available resources, alternative mitigating measures could be to set up an IT system administration access based on a four-eye principle (we talk about it further in this section) and building up a robust monitoring infrastructure that will send data access alerts, not modifiable by IT system administrators, to business area representatives.

4.3.2 Segregation of Duties

This principle applies to critical business processes that consist of several steps. If the same unique entity (individual or group) performs all steps, the possibility to misuse the process for their benefit is bigger than if detached and unrelated entities perform a subset of the steps.

Eventually, the process finalises, but in a situation in which no unique entity has full control or the possibility to modify the outcome of the entire process. Two typical fields of application for this principle are:

- Accounting procedures, where the party spending the budget is different to the party assigning and approving it.
- User management tasks,[11] where there are three different actions performed by three distinct players: Someone requests access, someone else approves the request and finally a user access administrator implements[12] it.

---

[10] See the "*blue team*" in Section 4.10 and RBAC model summary in http://en.wikipedia.org/wiki/Rbac. Last accessed 20-09-2009.

[11] NIST (2002b), pp. 3-3 and 5-2.

[12] See Section 2.3.

Image 4.2 Critical actions require different players working together

4.3.3 Four-Eye Principle

This tenet is a specific application of the segregation of duties principle. A process follows the four-eye principle if the only possibility to accomplish it requires the participation of two different individuals. Ballistic missile facilities follow this principle: Missile launching activities require two different keys, watched over by two different individuals.[13]

Split passwords are a simple way to practice this principle in IT security: A password is divided into two halves. One entity keeps one half and another entity keeps the other half. Access to a system requires both entities to insert their half. This means that at least two individuals (four eyes) knowing different credentials are present to operate the system (Image 4.2).

4.4 Software Development Security Principles

The Open Web Application Security Project (OWASP) has collected a set of security principles for application developers.[14] They are useful in the design of any security device. Apart from the principles we have already described, the most prevalent ones are:

[13] At least war films show this point.

[14] See http://www.owasp.org/index.php/Secure_Coding_Principles. Last accessed 20-09-2009.

Image 4.3 IT security should keep complexity away: it is the gate to encounter risks

- Minimise attack surface area: Every new feature increases risk and complexity.
- Establish secure defaults (among them, fail securely[15]): Security configuration should come by default.
- Avoid trust on alien services or input: Filter user and third party services input.
- Avoid security by obscurity: Secrets will eventually be disclosed or known.
- Keep security model simple: Complexity adds risks.
- Fix security bugs correctly: Focus on the source of the vulnerability.

The IT security activities that the team will perform in the organisation can be based on IT security professional experience and, more importantly, on at least one of the principles mentioned in Sections 4.2–4.4. These principles constitute a strong argument when we need to justify our proposals of action (Image 4.3).

Stock-Taking Exercise and Prioritisation

4.5 Vulnerability Analysis: Inventory Exercise

When a small organisation is born, the first IT equipment is procured and installed usually with no IT security participation. Eventually, when there is an individual or a group in charge of IT security, they will first need to action changes. Once leaders

[15] Should the device fail for any reason, the device should revert to a secure state.

have prepared their "principle-based hotbed", the first hands-on step is to gather information on the "state of art" of IT security in the organisation. What is there already in place in the customer organisation?

We propose to follow some of the steps present in generic penetration testing[16,17] methodologies: Planning, discovery, attack/exploitation and reporting.

4.5.1 Planning

Step zero is to obtain written management approval and sponsorship for the inventory and plan the resources required for the entire activity.

4.5.2 Information Gathering/Discovery

There are no two organisations alike. Therefore, leaders need to customise the stock taking exercise for their organisation. They start with a basic intelligence-gathering analysis: Finding out the vision, mission, objectives, strategy and tactics (using the VMOST[18] model) of the organisation.

This high-level location of the organisation helps them identifying where to place their analysis efforts.

An initial division[19] of elements to analyse is the following:

- Networks.
- Data.
- Systems.
- Applications.
- Identities (of users in systems).[20]

There are limited time and resources to perform this analysis. The checklist below will help to identify the priorities in each of the five elements:

- How many elements are there?
- Where are they?

---

[16] NIST (2003), pp. 3–13 and 3–14 and Long et al. (2006), pp. 2, 3 and 96.

[17] Backtrack proposed technical steps to pen-testing are: Information gathering, network mapping, vulnerability identification, penetration, privilege escalation, maintaining access and covering tracks.

[18] VMOST model. See Section "Link to MBA Management Models" in this chapter. Harding and Long (1998), p. 116.

[19] Proposal coming from a conversation with Jess Garcia, IT security professional and SANS trainer. See http://www.one-esecurity.com. Last accessed 18-11-2009.

[20] Identity management in organisations is a challenge: Find out how long it takes to create an identity, how long it takes to rename an username and what happens with identities of users leaving the organisation.

– Which technology are they based on (software and hardware)?
– How are they supported?
– How are they related among them?
– Which ones are holding the "crown jewels"?

4.5.3 Vulnerability Identification/Attack

The suggestion is to seek answers using two sources: Interviews with professionals working in the organisation and first-hand empirical research to confirm the input given in the interviews. Once the team members have gathered the answers to the interview questions, they need to come up with a plan stating the IT security actions to perform. These actions consist of hands-on security tests aiming to identify, and exploit, if possible,[21] existing vulnerabilities.[22]

4.5.4 Reporting

Subsequently, the team need to prepare a brief but condensed management report in few pages presenting findings and priorities, accompanied by real demos to show management existing security holes. A demo is worth much more than a verbose report.

4.6 Threat Analysis: Military Strategy Revisited

Military theory, especially defence-related episodes, is a central source of knowledge for IT security.[23] We have delved into a vulnerability analysis of the organisation in Section 4.5. With this, the IT security team are closer to identify potential sources of risk. We suggest complementing this vulnerability analysis with a threat analysis using adapted fragments of a military strategy planning technique[24] to identify the organisation's ***adversaries***.[25]

The first step requires knowing who are the attackers of the organisation and what are they doing (i.e. an adversary and threat analysis). A useful tool will be the collection of published IT security incidents currently happening in the world and specifically

[21] Business processes in production could be affected. Exploitation phase requires pre-announcement, backout possibilities and, more important, prior to it, business owner approval.

[22] See definition in Section 1.1.

[23] See Sections 4.2 and 4.3.

[24] Thompson (2005), pp. 399 and 400.

[25] See definition of threat in Section 1.1.

in the industry where the team is located. The incidents database we proposed to keep in Section 1.15 is a starting point. It will help the IT security team to gather intelligence to understand their potential adversaries: Those entities aiming at becoming threats that will take advantage of a vulnerability to damage the organisation.

The second step concentrates on setting up a strategy to neutralise adversaries: We suggest using the team's IT security knowledge to make adversaries find other targets more attractive and vulnerable than the organisation that the team protect.

Once team leaders have a strategy, they should go down a level deeper, to tactics, and decide their operational planning, i.e. when and how they need to act, what resources are required and which control measures need to be put in place to follow their strategy.

The answer to what to do starts to be shaped with the inward-looking vulnerability analysis and the outward-looking threat analysis introduced in Sections 4.5 and 4.6. The next hurdle to overcome is to know which priority to assign to each of the candidate activities.

4.7 How to Set Priorities

The main objective is to provide business value with the IT security actions. Which actions will provide higher value? Where to start with a list of activities? A basic pre-requisite, as already mentioned in Section 1.19, is to have the mission of the organisation always in mind. We propose a systematic approach to set priorities.

Filter 1: In Chapter 1 we presented an initial ranking exercise applying the Pareto principle (the 80–20 rule[26]). We advised to focus on activities mitigating risks with a high (Fig. 4.1):

- Impact for the organisation (if they materialise).
- Probability to materialise.
- Profit to risk ratio for the attacker.

This exercise provides the IT security team with a first list of targets. However, any activity they could set in motion requires resources and they can only use a limited amount of them. The proposal is to add the resourcing dimension to their prioritisation exercise with the help of an additional filter:

Filter 2: Locating the list of targets coming out from filter 1 with a similar priority in a three-dimensional grid. The dimensions to consider are:

- Resources required (people and equipment, internal and external).
- Complexity of implementation (number of players involved and activities required).
- Deterioration of user experience.

[26] See Section 1.17.

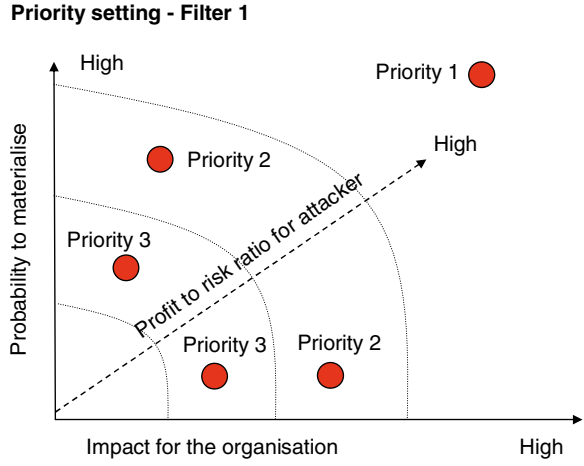

Fig. 4.1 Priority setting. First step

The first places in the priority list will be activities scoring very low at least in two out the three dimensions. The last dimension presents a special trait: The portfolio of activities needs to keep on scoring low in user experience deterioration if we work in organisations whose culture includes a high degree of user friendliness on IT systems, even at the expense of a less secure environment (Fig. 4.2).

Filter 3: There is a third filter, especially in times when headcount and budget are in question: Visibility. From those activities coming out from filter 2 with a similar priority, we propose to select those that spread either:

– A positive image for the organisation among customers, or
– A positive image for IT security throughout the organisation (more on this topic in Chapter 7).

They are effective marketing measures raising brand or security awareness. For example, all customers and users will welcome that they can access different services seamlessly using a unique credential (basic type of single sign-on).

Filter 4: There are other prioritisation filters to consider: Depending on the industry in which the team works, the organisation will probably have to comply with legal and regulatory requirements. Some of them will require the implementation of specific security measures.[27] This will have priority over other security actions. It is clever to take the chance to implement regulatory compliance to implement value-adding and effective security controls and not only to pursue a successful audit result.

[27] For example, HIPAA is a US Act that addresses the security of health data and PCI DSS sets security standards for the payment card industry.

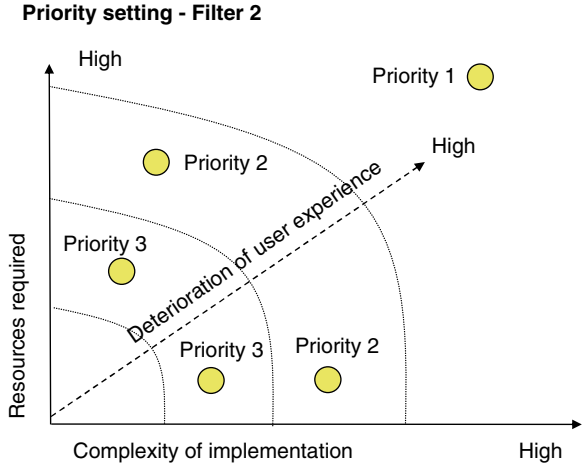

Fig. 4.2 Priority setting. Second step

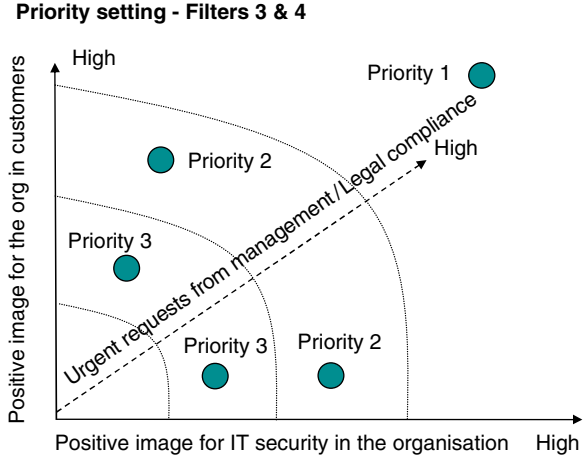

Fig. 4.3 Priority setting. Third and fourth steps

The last prioritisation filter to mention is simple but worth-remembering: Urgent requests coming from management (more on this on Chapter 8). Hierarchies still exist in organisations. We need to accommodate management requests within the team's priorities to guarantee the team's continuity. The smart move is to channel the implementation of those requests through already planned activities to avoid any feeling of improvisation (Fig. 4.3).

As a final note, we recommend devoting maximum 10% of IT security resources to innovative or visionary security projects that do not come out as priorities using the ranking method proposed in this section.

Provision of Security Services

4.8 Security Services

Previously in this chapter, we have proposed that the IT security team should not become an 'IT fire brigade', we have described the principles to base activities upon, what the organisation needs in security terms and how to prioritise a list of security activities. The following sections focus on the actual deliveries that the organisation requires.

The IT security team have to deliver services. IT security is a service provider, a support area within the organisation. A security service consists of three elements:

- A ***deliverable***, any product, be it a user interface, a token, an identity, a guideline, a policy, a hardening script, an assessment, a set of requirements, a report, etc. The product can be delivered once or following a frequency. It is something the team have built, customised, configured or elaborated for one of their customers, e.g. a business area, a user, a project team.
- A ***process*** to keep the deliverable current, a collection of steps that the organisation needs to follow, starting from the moment they receive the first deliverable. Depending on the type of product delivered, a process can consist of few simple steps or of a series of precise actions requiring synchronisation among different groups.
- A way to ***measure*** and ***improve*** the provided service. Following the management mantra "what cannot be measured, cannot be managed", the team need to provide a mechanism, preferably automated, to measure the effectiveness of the service and, if possible, to constantly improve it (Image 4.4).

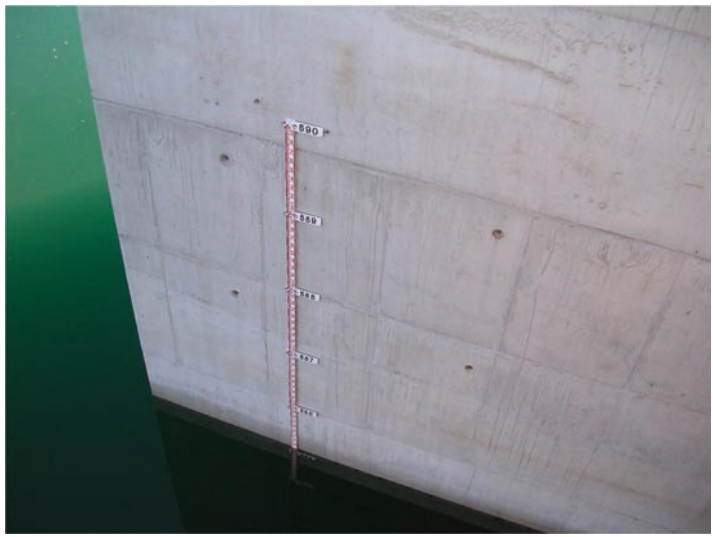

Image 4.4 What cannot be measured, cannot be managed

Two examples of security services are:

- Security policies: Once the team deliver it and management approves it, the team should periodically revisit and update the policy and assess the compliance of the target systems with the policy.
- Security tests: When a security test report highlights vulnerabilities in a business system and the IT security team propose the corresponding mitigating measures, the IT systems department should agree with the business area how and when the system is hardened and patched.

4.9 How to Build the To-Do List

The activities to perform need to be understandable and add value. The organisation and the team need to understand why they do it. To introduce the to-do list, we use the security categories proposed in Section 4.5[28]:

4.9.1 Networks

Every organisation has IT networks, some of them are probably connected to the Internet. The IT security team need to know those networks, the IP addressing schema that they use, the protocols and the flows that traverse through. More importantly, the IT security team need to participate in the daily operational network support process, normally led by the network team. The team need to know when their network colleagues create new segments or when they change IP addresses or add new routers into the network, in order to provide security value.

The IT security team need to analyse network traffic ingressing and egressing the organisation's networks, especially in those corporate networks connected to public networks. They need to discover standard network traffic patterns and be ready to react almost real-time when they find strange traffic through the networks:

- Intrusion detection systems help detecting malign traffic patterns.
- Firewall, router, proxy and web server logs provide useful data on what flows through the networks.

We propose, as a quick-win exercise, the analysis of web traffic originated in users' browsers[29] going to the Internet. For example, those requests to IP addresses that are not using domain names are worth a deeper study. Maybe they belong to a piece of malware trying to connect to a command and control centre.

[28] Once the team have the answers to the questions suggested in Section 4.5.

[29] As there is personal data protection legislation the team have to abide by, they need to seek legal advice before performing actions involving user data.

We use the metaphor of the human body to summarise every aspect of the to-do list: Networks in an organisation are its blood vessels. The IT security team need to analyse the blood going through those vessels, the bits and bytes flowing through the networks to identify harmful elements.

4.9.2 Data

Business data constitute an important element of the organisation's "crown jewels",[30] if not the main one. The team need to understand data access patterns. A valid way to do it is to monitor data traffic coming to and from databases where data reside. This way, they can tell whether abnormal quantities of data leave the organisation's data repositories.

Business data are similar to the memories collected in our brain: We try to keep them safe in our neuronal connections so that we can access our experience and knowledge. So far, we are the only ones with access to them. However, data access is not so restricted. In the organisation, the IT security team need to know:

- Entities, users and applications, which have access to data.
- Type of access they enjoy: read-only or read and write.
- Duration and reason for the access.
- Process in place to reconcile data access.
- Data lifetime features (creation, modification, deletion and criticality changes).

4.9.3 Systems

Most IT services use the client-server paradigm: A client requests something to a server and the server answers back. We can draw two simple conclusions from this question–answer approach:

- Servers do not start any communication. They just answer back when asked.
- Clients start communications with their queries. They do not wait for requests.

We propose to monitor traffic flows and devote attention to scenarios that deviate from this paradigm, i.e. clients acting as servers and servers acting like clients. A pre-requisite for this proposal is to distinguish network-wise between servers and clients. A way to achieve this is to locate them in different network segments and preferably to connect those segments via OSI layer-4 or higher firewalls[31] to filter communications. Once the team know which IP addresses act as servers and which

[30] See Section 4.2.

[31] Examples of OSI Layer 4 protocols are TCP and UDP.

ones do it like clients, they can use open-source network scanners such as *nmap*[32,33] to perform and even automate real-time monitoring.

Continuing with the resemblance to the human body, the team need to constantly check that arteries carry blood from the heart to all parts of the body and veins do the opposite.

4.9.4 Applications

Most business applications are currently based on web technologies. Also most of them are connected to other applications. The team need to understand their architecture, how they exchange data and how users access them. Team members should provide a continuous testing service for critical applications. They will initiate the testing with manually crafted actions. We propose to explore the possibility to script most of those actions so that they can set a permanent testing service. This way, application security complements network and system security.

Secure application development requires to "think security" right from the inception phase. At the design and building phase, development groups should follow secure guidelines like the OWASP[34] development guide.[35]

OWASP can also provide application development teams with a code review [36]guide and security pen testers with a testing guide.[37] A joint effort by developers and security team members contributes to creating applications with less security breaches.

The same way doctors advise patients to follow preventive measures to avoid unnecessary surgery, the IT security team need to convince development teams to produce secure code from the start. And equally, the same way doctors monitor vital signs in a patient, they need to use application testing scripts to regularly check the status of their critical applications.

4.9.5 Identities

The team have to follow the lifetime of every identity. They need to create it only with the necessary access rights and always follow the real life events happening to

[32] Servers would have open UDP and TCP ports listening and clients would be initiating the TCP handshake in their communications and would have no port waiting for connections.

[33] See Section 2.4.

[34] The OWASP development guide can be downloaded from http://www.owasp.org/index.php/Category:OWASP_Guide_Project. Last accessed 20-09-2009.

[35] See Section 4.4.

[36] Available at http://www.owasp.org/index.php/Category:OWASP_Code_Review_Project. Last accessed 20-09-2009.

[37] Available at http://www.owasp.org/index.php/Category:OWASP_Testing_Project. Last accessed 20-09-2009.

the user of that identity: For example, if the user leaves, a team member disables the identity, if the user changes jobs, a team member takes away previous access rights and grants new ones or provides business users with the necessary tools for them to do it and for the team to keep an audit track of it.

What is more important, the team need to collaborate with the colleagues in the HR department and probably also in the physical security department to set into motion easy processes that will guarantee that the IT security team are informed of any event affecting identities (sabbatical breaks, parental leaves, newcomers, change of positions, etc.). Regular user identity reconciliation exercises are an example of the inter-departmental collaboration we propose.

As it is advisable that our medical record (medical identity) is updated and available to relevant doctors, our IT identity needs to be kept updated so that it provides us exclusively with the necessary access to perform our business duties.

4.10 IT Security Specialities: Teams Within the Team

What are the different fields on which an IT security team will embark? We put forward a cluster of specialisation fields that need to be covered by the skills present in the team. These are applicable regardless of the team size and they are in line with the profiles proposed in Sections 2.3 and 2.4.

In small teams, the same individual is probably the contact point for more than one topic. However, in middle-sized teams, composed of more than eight people, it is advisable to break out the big team into mini-teams, each of them working on risk management but specialised on specific IT security fields. This piece of advice follows the fact that human beings prefer to be in groups of five to eight members.[38]

We use colours to name the cluster elements proposed.[39] All these teams require documented and easy-to-follow procedures[40] and they need to communicate among each other:

4.10.1 The Red Team: Security Testing and Incident Response

A number of security members devote their efforts and passion to perform frequent security testing activities and respond to IT security incidents whenever they happen:

[38] See Section 3.7.

[39] In an attempt to achieve some name stickiness. Concept coined by Gladwell (2000), pp. 19–25.

[40] See Section 3.11.

They are the security testers and the incident handlers. There are three pre-requisites for the *red team* regarding security testing:

- Written business owner approval to carry out tests.
- An approved methodology[41] and corresponding testing scripts and checklists.
- A realistic resource and time plan to perform penetration tests in applications in production.[42]

And two requirements with regard to incident response:

- Proven checklists detailing the necessary steps to respond to the typical security incidents that happen in an organisation, like a forensic analysis of a workstation, analysis of a fake website that is using the organisation's brand, data retrieval from a printing server and from an email server, etc.
- Regular drills to exercise incident management and response capabilities.

4.10.2 The Blue Team: Identity and Access Management

This team cares for running and changing user identity management in the organisation. They design, manage and provide identities and audit data access within the organisation. Identity reconciliation is one of their services. User access administrator and web developers with experience on user repositories are members of this team.

The business data owner is the player with the highest interest to implement the minimum data access rights required by the business. They know who should have access to the data and why. They also know for how long. On the contrary, user access administrators in the team do not have that business-related information in mind. Therefore, we propose to follow a decentralised user access right granting model with a strong centralised audit and supervision function.

The *blue team* create user identities and compose the required business roles. Subsequently, a group of selected business area users, provided with easy-to-use tools,[43] assign those roles to the requester upon their management approval. The task to audit all granted access rights remains with the *blue team* (Image 4.5).

A business role is a collection of access rights bound either to a function in the organisation (functional role, e.g. Alice creates a monthly sales report) or to a position in the organisation (organisational role, e.g. Alice works in the accounting department).

---

[41] An example of methodology for web applications is the OWASP_Testing_Guide. Available at http://www.owasp.org/index.php/Category:OWASP_Testing_Project. Last accessed 20-09-2009.

[42] Security tests can affect business processes. They need to be organised and prepared to minimise that effect.

[43] This is why we recommend that this team has some web development and user repository knowledge (e.g. knowledge on Active Directory and LDAP). This way they can customise these decentralised access right management tools.

Image 4.5 Business users need the right tools

4.10.3 The Green Team: Security Device Administration and Monitoring

They administer, monitor and support security devices such as firewalls, authentication servers, VPN terminators, certificate authorities, intrusion detection and prevention systems and any other device installed in the organisation networks or systems that is related to IT security requirements. Security device administrators and monitoring operators are members of the *green team.*

Networks teams have traditionally taken care of firewall administration. Firewalls are security network devices. There is no clear cut between network and security responsibilities, the same happens between IT system administration and security (more on this topic in Chapter 9). In those scenarios where harmony reigns among different IT teams, we promote joint administration tasks, e.g. network colleagues can propose changes to commit in the firewall and security colleagues can assess them, implement them and regularly audit the rule base.

However, in hostile environments, where the network team was probably created in the organisation earlier than the "recently created security team", these topics can lead to endless discussions. We recommend abandoning the fight, letting the network team run the firewall while the IT security team can devote their energy to audit regularly the rule base and monitor the firewall logs on a daily basis. There are many other security activities in which the security team can excel.

The second central task for the *green team* is monitoring and reacting to defined security alerts. The logs and alerts that security devices and many other IT components

can produce constitute the best way to have an understanding on what is happening real-time through the vessels of the organisation. Alerts can have a business, application or infrastructure-related meaning.

The *green team* requires close interaction with the *red team*. A security alert coming out from a monitored system can unveil the occurrence of a security incident that the *red team* need to handle.

4.10.4 The Yellow Team: Security Governance, Compliance and User Awareness

They provide security governance services to the organisation in the typical form of guidelines, policies, recommendations, configuration and hardening scripts, etc and they check their compliance. They also lead security awareness initiatives among business areas and customers. The team consists of security policy writers, security testers and communicators.

System security policies need to become much more than a nicely formatted paper that few people in the organisation read and most IT systems do not comply with. Policy compliance requires the production of accompanying hardening configuration guides. They describe how to securely configure IT systems present in the organisation (for example, operating systems, databases, web servers and routers).

Together with these hardening guidelines, the *yellow team* need to provide scripts, usually provided by security testers, that will check compliance so that IT system administration groups can measure potential gaps between the way real systems are configured and the security policy. This is a typical key performance indicator for the IT organisation.

4.10.5 The White Team: Changing Security

The *white team* provide IT security consultancy services to the organisation, mostly to IT project teams and they also "change security", i.e. they add value by incorporating "security commodities" to the organisation, mostly following a quick-win approach. Some examples of these "security commodities" are services such as full hard disk encryption, secure mobile devices or network access control.

The actual implementation of the *white team* varies among organisations:

- Sometimes they are a virtual team, consisting of a percentage of time from most of the IT security team members.
- Some other times, some members of the other mini-teams, like the *red* and the *yellow* teams, move to the *white team* for a limited period of time to provide a specific "security commodity" to the organisation.

Table 4.1 Allocation of profiles in the mini-teams within the IT security team

IT security profiles and team allocation	
Nature of activities	Mini team within IT security
Technical	
Security tester	*Red team(and possibly yellow and white team)*[44]
Incident handler	*Red team*
Security device administrator	*Green team*
User identity and access administrator	*Blue team*
Security monitoring operator	*Green team*
Governance	
Security policy writer	*Yellow team*
Security communicator	*White and yellow team*
Generic roles	
Security coordinator	IT security team
Security team facilitator	IT security team
Security trainee	All mini-teams

Depending on the tasks the *white team* is entrusted with, the team leader will staff it with the required technical, non-technical and generic roles, possible also complemented by IT system experts and analysts.

Table 4.1 links the IT security profiles proposed in Section 2.3 with the colour teams we have proposed.

4.11 Activities That an IT Security Team Should Avoid

We have extensively discussed the tasks of the IT security team. We finalise this chapter reminding what the team should not do. Currently, some departments in organisations attempt to load the IT security team with activities that are far away from their mandate.[45] These additional tasks exert extra pressure to team members in their daily work. Team members and leaders require big doses of assertiveness to kindly turn these offerings down. Some examples are:

Assessing web content: Careless Internet browsing is a source of malware infection, disrupting business processes in the organisation. Every day, more companies take the white-list approach, i.e. users can only browse sites or download content from those sites that have been labelled as trusted by the IT security team.

Assessing the technical IT soundness of an Internet site falls under the IT security team's mandate. However, evaluating the content of the site and whether the staff member should be allowed or not to browse those pages while working is an HR-related task.

[44] Testers can provide value in technical compliance activities (yellow team) and change activities (white team).

[45] Providing IT security value.

Warning final users: The *yellow team*[46] drafts and elaborates final user security policies but it is the organisation's top management who eventually approve and make them mandatory. Certainly the IT security team need to provide HR with information on who is breaching policies but the task to warn users not following those policies is also an HR-related task.

For example, IT security teams normally are in charge of configuring antivirus and anti-malware software present in the organisation and of issuing the corresponding final user security policy. IT security can provide HR officials with information on who connects infected USB flash drives to the corporate network and provide security awareness briefings to the entire organisation, or even customised sessions to those users, to make them see that it is a risky behaviour. If additional measures are required, then it is up to the HR department to take action.

Change management: It is critical for IT security that the organisation follows strict change management processes when new IT implementations go live. In young organisations, where change management is still an immature process, IT security is one of the only voices in IT preaching for further testing and additional security measures before a system goes into production.

The IT security team need to be involved in the change management process, evaluating the risk posed by proposed changes. However, IT security representatives should not lead the process or act as a change manager. It certainly adds value to the organisation but change management is not only IT security related.

This chapter has presented the activities that the IT security team need to accomplish to deliver value to the organisation to which they provide their expertise (Image 4.6).

Image 4.6 Change management is a keystone in IT

[46] Providing IT security added value. See mandate in Section 1.19.

Chapter 4: Learning points

- The team needs to avoid the "fire brigade" mode.
- They need to follow the defence in depth and "crown jewel" principles.
- Military theory and code development provide additional principles.
- The first step is analysing the vulnerabilities of the organisation.
- The second step is analysing the threats and the adversaries.
- The team will prioritise according to impact, probability and profit to risk ratio (PRR).
- The team will provide security services: A product and a process.
- The IT security team consists of different mini-teams.
- The team should avoid becoming an HR arm or an IT change manager.

Link to MBA Management Models

We have selected four MBA-related models that could help us when analysing our organisation and setting a strategy for the IT security team:

VMOST

Vision, mission, objectives (long-term goals):

– What the organisation is trying to do.

Strategy (long-term plans) and tactics (short-term plans):

– How the organisation is trying to do it.

Porter's generic strategies *(1980)*

Tool to select a strategic direction: Differentiation, cost leadership or focus.

Porter's 5 forces *(1985)*

Useful to analyse the attractive of an industry:

– Competitors, suppliers, buyers, substitutes and entrants

Ansoff matrix *(1987)*

Growth strategies according to product and market states:

– Current market and product: Market penetration.
– Current market and new products: Product development.
– New market and current product: Market development.
– New market and new product: Diversification.

See reference: Harding and Long (1998).

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

Chapter 5: What will the reader learn?

This chapter answers the following questions:

- What threatens the team's performance and what can leaders do?
- What is a "SMALL baby step" and how can leaders assign it?
- Who is responsible for the "baby steps"?
- How much time of the team's working day do leaders plan?
- What should team members consider when planning?
- Who are the IT security team's main stakeholders?
- How should the team communicate with them and report progress?
- How do team members track activities?
- What should the team do with externally driven deadlines?
- What happens with small tasks?
- How should the IT security team deal with red-tape?
- How should the team communicate their plans and achievements?

We have introduced in the first three chapters the basic concepts of risk management (Chapter 1), the profiles of the IT security team (Chapter 2) and the contract between the security team and the individual (Chapter 3). Chapter 4 has provided details on the activities to perform and the way they can be justified, prioritised and distributed within the team. Chapter 5 provides leads on how to perform IT security activities and on how to organise actions so that the IT security team can fulfil their mandate.

A. Partida and D. Andina, *IT Security Management: IT Securiteers - Setting up an IT Security Function*, Lecture Notes in Electrical Engineering 61,
DOI 10.1007/978-90-481-8882-6_5, © Springer Science+Business Media B.V. 2010

Shaping the Daily Reality

5.1 Threats to the Performance of the Team

The IT security team need to satisfy three objectives:

- To deliver added value to the organisation.
- To build an environment where team members can develop professionally and personally.
- To enjoy the days working for the organisation.

The vulnerability and threat analysis on the IT security team that we proposed in Chapter 4 helps to better understand the team's capacity and attitude and to organise their work.

The motivation and internal balance assessment tools we presented in Section 3.3 facilitate the search of the team's vulnerabilities. The team leader would discover the state of their team members and how they can look after the team.

The threat analysis requires focusing on those external actors that could play a detrimental role on the performance of the team. They can use up all team's energy and this energy is precious and limited. Team members will identify three threatening energy consumers:

- Service requests.
- Organisational confusion (politics).
- Time thieves.

5.1.1 Service Requests

An excessive number of service requests can become the main threat to the performance of the team. The same way we can damage a muscle or a ligament if we overstretched them, a permanent over-utilisation of the team's working capacity can disrupt, or even literally, break a team.

We can only work over the capacity limit for a very limited period of time. There can be an urgent and important matter every now and then, but neither a team nor an individual can work under stress[1] on a permanent basis. Neuroscience has demonstrated that the size of the hippocampus, a major human brain component essential for the memory, decreases and can even suffer atrophy in individuals under constant stress.[2] A stressed brain stops being creative and innovative.

[1] Additional input on stress in Chapter 6.

[2] Eduard Punset interviews Professor Gary Marcus, psychologist at New York University. http://www.smartplanet.es/redesblog/?p=460. Last accessed 20-09-2009.

Clear signs of overstretched teams are higher numbers than usual in:

- Sick leaves of team members.
- Collisions among team members and between them and other colleagues.
- Mistakes due to lack of attention or motivation.

5.1.2 Organisational Confusion (Politics)

Any big enough and organised set of human beings display a whole range of human behaviours with regard to power.[3] This is also the case for organisations. Individuals working for them tend to pursue different objectives. If organisation leaders do not devote required care and attention to align those objectives, soon they enter into what we refer as "organisational confusion".

When the organisation is confused, the energy required to justify IT security actions is similar to the real energy required to actually perform those actions. This scenario constitutes a threat to the existence of the IT security team and certainly to their capacity to live up to their mandate.[4]

5.1.3 Time Thieves

We consider "time thieves" all those daily communication elements around the team's work that take from team members more energy than the value they obtain from them. We find two types of "time thieves" related to information exchange:

5.1.3.1 IT Based Communication Tools

IT provides nowadays tools to accomplish more tasks in less time but also to waste time miserably. Team members have to use email, instant messages, blog posts, social networks, "tweets,[5]" etc. wisely and, when possible, avoid that they become their main daily activity.

5.1.3.2 Meetings

Organisations are made of individuals. As individuals, we communicate among us to solve problems and move forward. Face to face communication is much richer

[3] Machiavelli published in 1532 "The Prince". A treaty on how to most successfully obtain and maintain power.

[4] To provide IT security expertise, see Section 1.19.

[5] A "tweet" is a posting on tweeter, a micro-blogging service.

and comprehensive than any other means.[6] However, equally to what we showed with emails, the threat that meetings, workshops, conferences, etc. become the main daily duty exists, leaving very little room for real IT security work.

As the ultimate goal of the team leader is to create and maintain an IT security team with a long-term vision, they need to keep their focus and apply mitigating measures to avoid these threats affecting to their team. We propose to:

- Manage the inflow of service requests. Leaders should be transparent on the allocation of team resources and on the management of service request queues. If there is no possibility to control the service demand, they should manage customer expectations by providing realistic service delivery dates. They need to agree on their prioritisation criteria[7] with their customers.
- Focus available energy on delivering IT security services and let the quality that the team provide be the main marketing (and lobbying) tool in the organisation.
- Follow a schedule[8] to check IT communication tools such as email and avoid endless discussions.[9]
- Limit the length and number of meetings. The meeting organiser should prepare an agenda beforehand and distribute follow up points among meeting participants afterwards.

With these measures, the IT security team will be closer to create a reality where they can really perform and provide business value (Image 5.1).

5.2 Plan in "SMALL Baby Steps"

Once we have shaped reality with the measures proposed in Section 5.1, we are ready to organise the work for all mini-teams within the team presented in Section 4.10. We introduce the use of an easy-to-handle planning unit: A "***baby step***". It is a small task that team members can comprehend, manage, plan, budget and, most importantly, finalise.

5.2.1 Every Trip Starts with a First Step

This Chinese proverb summarises our proposal to plan our activities. The IT security team leader needs to break down activities into "baby steps" and elaborate a plan to implement them.

---

[6] See Section 3.6.

[7] See Section 4.7.

[8] Unless the IT security team are monitoring devices real time.

[9] See Section 3.13.

Image 5.1 The team need to enjoy the reality they create

This dissociating activity requires knowledge, experience and reflection. The team leader and senior team members will organise and supervise it. Subsequently, they will allocate concrete “baby steps” to junior team members.

These “baby steps” need to be “SMART”.[10] We would customise the acronym and change it into “SMALL”, i.e. specific, measurable, achievable, light and (time-) limited to obtain “SMALL baby steps”.

Every IT security task has a certain degree of complexity but, when we break it down into “SMALL baby steps”, this complexity is manageable: A “baby step” is a specific, achievable activity that will be evaluated and it will take only some hours or days.

There are many valid ways to decompose an activity into “baby steps”. The team leader should allow for some controversy and brainstorming time when shaping “baby steps”. Lateral thinkers,[11] team members with alternative ways to see reality, will come up with different ideas that could potentially be easier to implement. The best brain in the team is the team’s brain.

Once the “baby steps” are defined, we do not recommend re-visiting their existence until they are finalised. IT security teams cannot afford changing the guiding

[10] This is a project management acronym for specific, measurable, achievable, relevant and timely objectives.

[11] Lateral thinking is a term coined by Edward De Bono in a book published in 1970 with the same title. ISBN 0-14-021978-1.

Image 5.2 The team base their plan on "baby steps"

direction on a daily basis. However, a brief "lessons learned" session after the conclusion of the entire activity is a valuable way to verify whether the defined steps were successful and adequate for the team (Image 5.2).

5.3 Baby Step Assignment Within the Team

Which criteria should team leaders follow to assign "SMALL baby steps" to team members? We propose two:

- Ability to do it.
- If possible, preference to do it, i.e. the team member likes the activity.

Although, in the short term, leaders can deviate from these criteria, in the long term and having always in mind the continuity of the team, leaders need to give team members tasks they can do and they like to do. Only then team members will be motivated and have a real possibility to excel on what they do while they provide the organisation with IT security advice. This is their ultimate goal.

There are some routine tasks disliked by veteran team members that, however, need to be accomplished.[12] These are good candidates for junior members, provided that they have received enough guidance from the veterans. Nevertheless, the team need to adopt a fair task assignment method once junior members get an

[12] See Section 4.7 for a collection of potential sources of activities for the team.

understanding and experience on those tasks. We propose two complementary approaches to deal with non-attractive routine tasks:

- Rotation among team members with similar skills (fair distribution).
- Progressive "partial release" from routine tasks to those team members improving their skills and, consequently, adding more value to the team, but only as much as overall team resources allow for it.

Both approaches require a clear communication of assignment criteria to all team members.

IT security cannot afford having team members who are not comfortable working in IT security.[13] Should that be the case, we advise team leaders to seek a way out of the team for that member using any possible means the organisation could offer: Job mobility, position swaps or simply not renewing their working contract.

There are many tasks to accomplish[14] and there is hardly any time to reinforce motivation. Although sometimes this is not a pleasant duty, team leaders need to look after the team's critical mass[15] and help uneasy team members to evolve somewhere else.

We add two actions for team leaders to consider on the art of task assignment:

- They need to provide motivated team members with the necessary tools[16] to excel in their assignment.
- They should offer (but not impose) their knowledge and experience, from which team members could benefit.

5.4 Responsibility Transfer

The assignment of a "SMALL baby step" conveys a clear transfer of responsibility. The selected team leader and senior team members need to offer support and guidance, but the selected team member is responsible for the successful accomplishment of the "baby step". They need to feel themselves owners of the success or failure that the completion of the step will bring. This is why the team member, responsible for the task, needs to feel comfortable with the assigned step and be proud of their achievements, or aware of their failure, and learn from both accordingly.

A good leader makes out of the failures of the team their own failures and out of their successes the successes of the team. Every team member needs to feel that their work made a difference in the team.

---

[13] See Section 3.5.

[14] See Sections 4.8 and 4.9.

[15] See Section 3.3.

[16] The concept of tool we use here is very broad: It ranges from hardware or software equipment to training measures such as on-the-job training, access to specialised fora or collaboration with experts on specific topics.

The final note in this section: Team leaders need to inoculate the spirit of "underpromise and overdeliver"[17] to all team members. The team reputation is only made of each team member's reputation.

5.5 How to Plan the Team's Time

Our proposal for the IT security team is to follow a set of added value priorities.[18] However, we have also warned about the fact that unexpected tasks will regularly land on the team and the need to accomplish them swiftly and effectively, especially if there is a regulatory, legal or managerial trigger behind them.

Therefore, IT security teams cannot abandon completely the "fire brigade" working mode we suggested to avoid in Section 4.1. The leader's goal will be to progressively reduce the time the team devote to put off "urgent and unexpected fires" and, simultaneously, increase the time they use to build their security foundations.[19]

Consequently, we suggest planning only a certain percentage of time and resources available in the team. This percentage will grow as the organisation and the IT security team mature. A proposal could be:

- Year 1 planning time <30% total available time.
- Year 2 planning time <40% total available time.
- Year 3 planning time <50% total available time.
- At cruise speed,[20] planning time <70% total available time.

Leaders need to be extremely careful with aggressive planning exercises. They endanger the continuity of the team as a group of motivated professionals.[21] The way we propose to organise the team's planned time is simple: "Baby steps" take time and require resources. For every step, team members can build a "step label" that consists of:

- Description: What needs to be done?
- Start and end date: When will it be done?
- Author: Who will be doing it?
- Requirements: What will they require to do it?
- Duration: How long will they take?

[17] Giuliani (2002), p. Contents.

[18] See Section 4.7.

[19] See Section 4.7.

[20] In organisations with a strong strategic alignment.

[21] See Section 5.1.

The team leader and other senior members have to assess the proposed "step label" and confirm that it is a realistic forecast. We advise to include some buffer time in the plan of every "baby step" to accommodate possible delays. These buffers will appear in the team's internal time plan as "room for delays" and not as part of the activity. This way, leaders can measure delays, see how they develop throughout time and propose actions to reduce them.

5.6 Compulsory Ingredients for the Planning

Together with the requirement to insert some buffer time in our "baby step" based planning to cater for unforeseeable delays, we mention two indispensable ingredients to factor in within the team's planning:

- A strong internal quality assurance process based on peer review.
- A culture of commitment to deadlines.

IT security is mandated to deliver first-class quality in all their services. Poorly delivered services and mistakes can have a great impact to critical business processes and, ultimately, to the organisation's reputation. Everyone is prone to make mistakes. Therefore, we propose to follow in the service delivery process one of the security principles described in Section 4.3: the four-eye principle.

Security deliverables, before they leave the team, have to be reviewed, checked and complemented by a second team member that can provide value to it. Extremely busy security teams that skip this ***quality assurance*** measure deliver less quality than those teams that allocate time for peer reviews for at least all their critical services.

Team members also need to adapt to their organisation's stance on project deadlines: Are they religiously respected or just an optional and movable milestone? In those organisations with strict and fixed deadlines, team leaders need to incorporate them well in advance into their planning and to monitor activity progress accordingly.

Should a delivery date be at risk, team leaders have to report it immediately to their key stakeholders, including the reason why this is happening to them and their analysis on how to avoid this situation in the future, proposing preventive mitigating measures such as increasing resources and skills present in the team or improving organisational alignment.

If the team work for an organisation with a soft approach towards deadlines, we propose the IT security team to become the exception. They will seriously commit to a delivery date for those services that depend uniquely on the team and they will make all team members aware of it.

For those products that depend on the collaboration with other groups, the team need to act as effective whistleblowers and report delays to decision-makers as early as possible, being factual about the causes so that they can treat them accordingly.

5.7 Multiple Tasks at One Time

The number of activities that each team member will perform simultaneously is an aspect that we need to consider. Team leaders can fine tune it based on two facts:

- Multitasking brings along time inefficiencies coming from the time required to switch between tasks.
- Some team members require multitasking for their daily way of working.

Switching times need to be shorter than times devoted to each real activity. Our recommendation is to follow a linear approach[22]: A team member starts an activity, performs it, finalises it and, only then, the team member starts a new "baby step". Exceptionally, for those team members willing to practise multitasking, they can work at a small number of "baby steps", provided that they have their switching times under control.

5.8 Finalising Baby Steps

In both approaches, linear monotasking and multitasking, team members strive for finalising all "baby steps" having always in mind the overall security service that they eventually aim to render. They seriously need to finalise their "baby steps" and deliver the service as planned. The organisation and their main stakeholders have to benefit from it (Image 5.3).

The ability to finalise a task is usually a real challenge for IT security teams.[23] We suggest three incentives for team members to reach the "finalised state" in their "baby steps":

5.8.1 Provision of "IT Security Win Rides"

A team member has spotted a gap in a security topic that they feel comfortable working at. They are certain that they can provide a real additional "quick win" for the organisation and they are willing to embark on this activity once they have finalised their assigned steps. The best "win rides" take place when these two drivers convene: Personal interest and value for the organisation.

5.8.2 Increase in Levels of Self-management and Independence

Successful team members require gradually less daily coordination efforts from senior members or from the team leader. They need guidance, support and

[22] Team members could use unavoidable waiting times to prepare the start of a new step.

[23] See Sections 2.6 and 5.2.

Image 5.3 Team members need to close doors before they open new ones

coaching but, certainly, no daily micro-management. These solution-oriented team members are good candidates to lead a mini-team within the team we proposed in Section 4.10.

5.8.3 Increasing Comfort Levels

In line with Section 3.12, team leaders need to reward brilliant team members that succeed in their assigned tasks. A simple but very effective way to reward them is to provide them with a higher level of daily comfort. Provided that service levels are guaranteed by the team, every organisation offers possibilities to reward team members such as flexible time arrangements, possibility to tele-work or the traditional bonuses and salary rises.

Managing Expectations

5.9 Stakeholder Analysis

We suggest performing a stakeholder analysis to identify to whom the team need to report progress. Team members need to know which clusters of individuals could influence their actions or be affected by them. This is the first step for the team to be able to:

- Customise their reporting so that they can manage stakeholder expectations.
- Successfully channel the actions that the team could exert on stakeholders.

In particular, the team need to use effective ways to report progress, especially to those stakeholders with power to influence the team's daily life and with high interest in the team's activities.

We distinguish the following stakeholders of the IT security team:

5.9.1 Top Senior Management

Most IT security teams are located within the IT department. This means that they report to senior management in the IT department. Top senior managers definitely have power on IT security teams. It is the team leader's task to find out whether they are also interested in IT security activities.[24] They need to sponsor and back IT security.[25] They play a decisive role to request and achieve the budget that the IT security team need.

5.9.2 Line Management

Although the current trend is to place the IT security team in the organisation chart reporting directly to senior management, there are still many teams reporting to middle management. In that scenario, their line management is also a powerful stakeholder for the team. Again, team leaders should discover the degree of interest that they will have in the team. Line managers need to support the team.

5.9.3 Business Areas

Core business areas are powerful stakeholders in the organisation. The team need some of them showing interest in the team's activities. Team leaders have to align the strategy[26] of the team with the strategy of the business area to provide them with real business value. For those business areas with lower level of interest, the

[24] Should that not be the case, then it is the IT security team members' task to raise their interest (see Chapters 7 and 8).

[25] See Chapter 8.

[26] See Section 1.20.

team need, at least, to inform them about the team's activities and achievements using a language that the business areas understand. Business areas need to accept the team.

5.9.4 Final Users

They can be internal or external customers. Individually, they enjoy low levels of power and the interest that they can have in the team varies greatly. Team members need to create effective ways to communicate with users showing interest in IT security.[27] They can eventually become the team's reason of being.

5.9.5 Other IT Teams in the Organisation

They constitute a key cluster of stakeholders that IT security teams often neglect. A common mistake among security practitioners is not to set effective communication channels with other IT teams in the organisation and, even worse, to set priorities for the IT security team without counting on them. We propose to change this scenario with two different types of IT teams:

- IT operational teams (IT professionals responsible for systems in production): They definitely have power over the IT security team. The security team need either their agreement or even their active collaboration to implement most technical initiatives. Traditionally, operational teams have shown low interest in collaborating with security teams. Their history, as groups of IT professionals, is usually older than the security team's and, unless security team members are successful in their communications and marketing actions,[28] operational teams tend to consider security colleagues as a threat.[29] Operational teams need to collaborate with the security team. To achieve that, we call for clear communication channels and security teams reporting their activities to operational teams.
- IT project teams (IT professionals working in a project that responds to a business requirement): They usually have less daily contact with security than operational

[27] See Chapter 7.

[28] See Chapter 7.

[29] Two examples:

- IT security teams taking over firewall management activities.
- Proposing new and more secure (but less comfortable) ways to work with privileged system accounts.

teams. A late interaction with security can cause unwanted project delays. Normally, they have different objectives than the security team, i.e. their number one priority is to finalise the project first on time, second on budget and third, if possible, with the required level of quality.[30]
- Project teams need to involve IT security at an early stage in their project. This way, they avoid inserting late, and more expensive, security measures as an afterthought in their systems. Project managers need to front load required IT technical and operational security elements in the requirements and design phases.
- Consequently, IT security teams need to communicate with project teams so that they understand each other's mandate and they can agree to work on a win-win basis. The security team also have to organise their service provision based on the fixed deadlines that the project has.

5.9.6 IT Security Teams Members

They are certainly key stakeholders. We have talked about how to approach them in Chapter 3.

5.9.7 IT Security Team Members' Social Circles

Finally, the last group of stakeholders to comment are team members' families and close friends. Team members need to let them understand why they work in IT security and what security means for them. The firm support of team members' social circles outside the working environment is of great help, especially as team members go through tough moments at work that can easily bring them momentary frustration and unhappiness.

Where does frustration come from? Throughout this book we present a series of behavioural, professional and communication measures to mitigate the fact that the nature of the security work resides on the not so popular task of making decision-makers aware of the risks they take when making business: Following always this security mandate, IT security team members pose difficult questions, they can make some of their colleagues' work more cumbersome and they can even reject changes.

Therefore, it is advisable that IT security team leaders look after team member's families by sharing with them, in non-IT words, what they are working at and the efforts that their loved ones are making. We suggest to organise, once or twice a

[30] We include security as an essential part of the quality package.

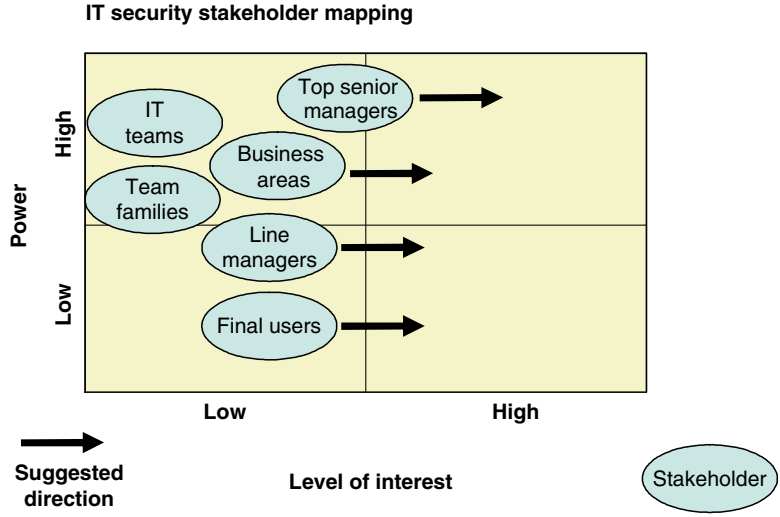

Fig. 5.1 Stakeholder analysis and suggested movement direction

year, a social event,[31] open to all colleagues in the organisation, in which families can meet each other to share experiences and diminish the difficulty of living with an IT security professional (Fig. 5.1).

5.10 How to Communicate with Stakeholders

Different stakeholders require different means of communication and different content. Activity progress reports coming from the IT security team should follow three guidelines:

- *Early warning*: Regardless of its content, delayed communication conveys already a negative message by itself. Good news can exceptionally be deferred, however bad news need to be communicated as soon as they occur.
- *Consistent information* to all stakeholders: Even if the format and the content of the communication differ among recipients, information provided by the team need to reflect the same reality.
- *Understandable*: Team members should carefully select the language for each communication process. The recipient stakeholder group need to understand it. Team members should learn the language that their stakeholders talk and use it in their communications.

[31] Maybe it could also be aiming at collaborating with local communities.

Two examples on comprehension:

- When team members address business managers, they will use business language. For this, they will need IT-business translation skills in the team.
- When team members address all their colleagues in the organisation,[32] they need to use non-IT terms so that all recipients understand the message.

A basic pointer to successfully communicate consists of elaborating a script using typical questions that journalists try to answer when reporting:

In general-purpose communication:

- What do we communicate?
- Why do we communicate?

In activity progress reports:

- What have we achieved?
- How does it affect the recipient?
- Did it occur as planned?
- What is the next "baby step"?

In security incidents reports:

- What and how did it happen?
- Why could it happen again?
- What do we recommend?
- Why do we recommend it?

Managing Activities

5.11 How to Report Activity Progress

There are three main reasons for the IT security team to report:

- To show the added value that the team provides to the business.
- To justify the budget that they are using (and the budget they will be using).
- To guarantee the continuity of the team in the organisation.

We recommend elaborating written reports that can be filed and retrieved if needed. The reports show the progress that the team have made and link their activities with the strategic work programme followed in the department where they are located. The format of the reports should be simple and the reporting frequency regular.

[32] For example, to warn all users about a potential piece of malware they could receive in their mailboxes.

For the team's key stakeholders, we propose to accompany the written report with a corresponding face to face meeting with them. Preferably, the team will send the report some days before and present it during the meeting. In those meetings, they can solve doubts and link their achievements with current developments taking place in the organisation.

5.12 How to Track Activities Internally

Apart from reporting to their line management and to their budget-granting authorities, team leaders need to set up an easy way to follow up the progress that team members make in the activities they perform. All team members should report using the same format and a similar frequency.

The selection of the method to track activities is crucial. Leaders need to devise a tracking system that fits their team's requirements. The threat to mitigate is that a majority of team members consider this internal reporting as a bureaucratic element with no added value for them. Whatever proposal that leaders put forward, it requires team members' conviction that it is useful for them to inform their peers on their activities and to know what other team members are doing.

There is a myriad of possible systems but the two alternatives presented here contain elements that could be used in any human team.

5.12.1 The Morning Gathering

Every working day, at the same time, some minutes after the members' arrival time, the team gather together in a stand-up meeting and each member, in 1 or 2 min, mentions what kept them busy the day before and what they will do that day.

During the round of interventions, the team leader and senior members provide quick guidance that could benefit the team, prepare relevant questions that they will discuss bilaterally, after the meeting, with some team members and take note of the finalised "baby steps".

5.12.2 Online Weekly Reporting

Team members write their activities in a common place where all the team have access.[33] Depending on the nature of the tasks in which they are involved, they insert new developments every day or just at the end of the week.

[33] For example, a basic web-based forum or collaboration tool.

There are pros and cons for each of these two proposals. On the one hand, the morning meeting requires a daily physical gathering[34] and soon some team members will dislike it. However, it is an excellent way to spot sudden motivation drops and team inefficiencies as two members working in activities that overlap. On the other hand, the online reporting is more comfortable and it requires less energy but it is also easier to be misused by non-motivated team members.

5.13 External Deadlines

In Section 5.6, we already proposed to adopt a culture of real commitment to deadlines within the team. There is another aspect regarding deadlines that we would like to point out: Externally driven deadlines. These are dates when a specific system or service needs to be definitely life or a deliverable needs to be ready due to external commitments that have to be fulfilled.

The organisation will respect those deadlines even if, for whatever reason, the IT security team is not ready to deliver. Team leaders have to avoid this scenario, even if the security side of the delivery is minimal. The first obvious requirement is getting to know those external deadlines. Sometimes no one in the organisation communicates these deadlines early enough to the IT security team.

Once the team leader and the senior team members know the dates, they need to plan the necessary "baby steps" so that the days prior to the deadline the team do not plunge into chaos. Moreover, it is a priority for the team leader to place IT security as a recognised stakeholder in the organisation, deserving timely involvement in any IT project and planning exercise.

5.14 How to Invite Team Members to Perform New "Baby Steps"

Active and committed team leaders and senior team members come up daily with new possible tasks for the team. Some of these activities come from their IT security readings, some others from punctual requests coming from prominent stakeholders. They need to keep a list of these to-do actions so that they are not forgotten.

Senior team members should shape these tasks into compact, modular and feasible "mini assignments" requiring only some minutes or hours and assign

[34] There is also a problem related to the size of the team: If the team consists of more than, e.g. eight members, then each mini-team will do its own gathering and afterwards representatives of all mini-teams will have a collective meeting.

them to get them finalised by, possibly, a junior team member. They could be quick wins benefiting the entire team.

Instead of just forwarding the email or task description with a blunt sentence inviting the recipient to perform the task, we propose to use a message,[35] similar to the "step label" presented in Section 5.5, containing:

- A description of the activity to perform.
- Tips on how to perform the task.
- Input on how the tasks will be assessed.
- Time reference when the task should be finalised.
- Finally, request to include the completed assignment in the team's activity report.

This way, team members can keep a record of these "baby steps" or "mini-assignments" for future appraisal and reporting exercises and reward their authors accordingly.

5.15 How to Deal with Red Tape

Depending on the size and nature of the organisation, the IT security team will undoubtedly deal with processes and activities that fall under the bureaucratic maze that every organised group of people creates. Dealing with this burden is especially difficult for passionate IT security professionals whose desire is to work on an IT security topic hands-on. Nevertheless, these unattractive tasks exist and the team need to complete them as long as they wish to stay in the organisation, or keep the organisation as a customer.

Some of these bureaucratic tasks are essential for the continuity of the team (e.g. procurement requests both for consultancy services and IT security equipment, budget justification and forecast exercises) or, simply, input to a new corporate or IT initiative.

Our piece of advice about these tasks is that team members ought to see the opportunity hidden behind the burden. If they accomplish these tasks in a smart and consistent way, then they can probably obtain additional resources for the team or even a better strategic position within the organisation.

The only practical piece of advice that we add is that these activities should rotate among different team members. Even though most of these items require the team leader or senior members' attention and supervision, all team members need to collaborate, providing time and effort, to finalise them. No one in the team should feel that they are doing more red tape than other members, unless they have underperformed in their IT security assignments (Image 5.4).

[35] Regardless of the means that IT security leaders use to communicate these "mini assignments", be it e-mail, a phone call or a face-to-face conversation.

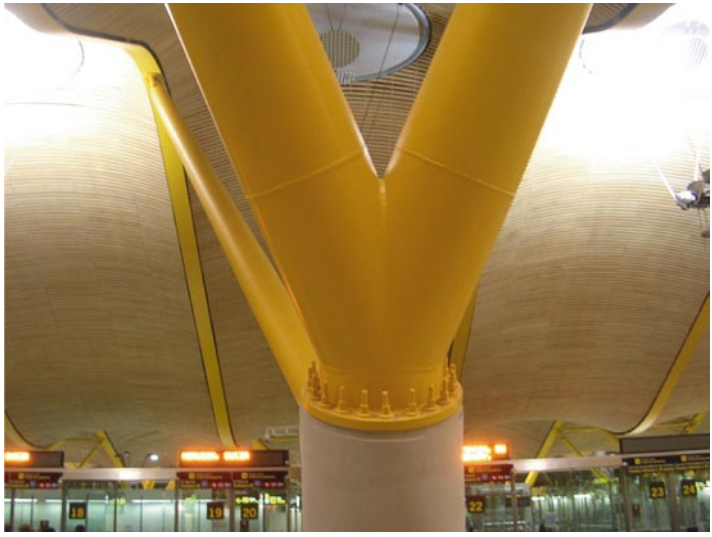

Image 5.4 Everyone in the team should share the load of bureaucracy

5.16 Basic Communication Tools for the Team and the Organisation

IT security is a support area for the organisation. They provide services to their customers. As a service provider within the organisation, they need two different communication tools.[36] Both require quick and easy ways to publish information:

- An internal site for the team to share information and procedures among team members with the objective to provide a consistent service, regardless of who in the team eventually provides it.
- A public site within the organisation, the "mass communication channel" to inform colleagues and customers, in an understandable manner, about IT security activities affecting them and, as an addition, about security tips that they could use at work and at home.

This is the end of Chapter 5, where we have provided leads on how to perform the activities presented in Chapter 4. We started suggesting to shape reality by mitigating potential threats to the performance of the team. We introduced the concept of "SMALL baby steps", easy-to-handle and easy-to-perform activities that constitute the steps for a major achievement. We also proposed a way to assign these "baby steps", together with how to transfer responsibility to team members. We continued the chapter advising on time planning, quality assurance, multitasking and finalisation of activities. Finally we introduced some points regarding communication and activity tracking based on a stakeholder analysis.

[36] Chapter 7 deals with communication and marketing strategies.

Chapter 5: Learning points

- Excessive requests, organisational confusion and time thieves threaten the team's performance. They need to be mitigated.
- Baby steps are limited in complexity and in time. Leaders assign them to capable team members.
- The team member doing the "baby step" is responsible for the success or failure of the assignment.
- Team members can only plan a percentage of their available time.
- The team need to commit to deadlines and plan peer reviews.
- Senior management and business areas are the main stakeholders.
- The team need to communicate using the stakeholders' languages.
- Team members need to accept and use a tracking method.
- Externally driven deadlines affect the team. Leaders need to plan accordingly.
- Team leaders need to follow up small tasks assigned to team members.
- All team members should share the load of red tape.
- The team need a communication platform to share information with peers and customers.

Link to MBA Management Models

We have selected two MBA-related models that could help us to organise activities in the IT security team:

Demand and supply *(by Begg, Fischer and Dornbusch, 1991)*
Demand is the quantity of goods buyers wish to purchase at a stated price. Supply is the quantity of goods sellers wish to sell at a stated price.
The lower the price, the higher the quantity of good demanded and the lower quantity supplied.

Economies of scale *(by Begg, Fischer and Dornbusch, 1991)*
There are increasing returns when average unit costs decrease (cost divided by output) as output and volume of production rises.

Stakeholder analysis *(among others, by George Eckes, 2003)*
We need to analyse expectations, interests and requirements from all the different entities affected by our actions. Depending on their degree of interest and power, we need to keep them:

– Closely managed (for those with high power and high interest).
– Satisfied (for those with high power and low interest).
– Informed (for those with low power and high interest).
– Monitored (for those with low power and low interest).

See reference: Harding and Long (1998).

Chapter 6
Team Dynamics: Building a "Human System"

Chapter 6: What will the reader learn?

This chapter answers the following questions:

- What is the IT security profession like?
- What does the IT "security castle" need?
- How do members interact within the team?
- How do technical members act together with non-technical colleagues?
- Which type of gurus does the team need?
- What makes the identity management team so peculiar?
- Work-related problems: How should the team deal with them?
- How should team leaders supervise working time?
- How can team leaders fine tune the "human system"?
- Which training measures should team leaders support and sponsor?
- How should leaders appraise team members?

In the first half of this book, Chapters 1 to 5, we have presented the foundations of information risk management (Chapter 1), the profiles required by an IT security team (Chapter 2), the basic aspects that guide the team-individual contract (Chapter 3), a list of security principles to follow and activities to perform by the team (Chapter 4) and some techniques on how to organise their IT security activities (Chapter 5).

The second half of the book provides additional insight to increase the possibility to succeed in creating an IT security team. Thus, Chapter 6 proposes a way to build an effective "human system" out of an IT security team.

A. Partida and D. Andina, *IT Security Management: IT Securiteers - Setting up an IT Security Function*, Lecture Notes in Electrical Engineering 61,
DOI 10.1007/978-90-481-8882-6_6, © Springer Science+Business Media B.V. 2010

The IT Security Paradox

6.1 Traits of the IT Security Profession

The outlook of the IT security job includes the following features:

6.1.1 Passion

Every human project is triggered by an emotion.[1,2] The decision, conscious or not, to work in IT security, or better said, to live security, is triggered by a strong emotion.[3] It is rare to find apathetic IT security professionals.[4] Most security professionals are passionate for their job and, with no doubt, renowned IT security experts currently leading the industry are definitely passionate "securiteers".[5]

6.1.2 Heterogeneous Background

There are "securiteers" with very different backgrounds. For example it is frequent to find professionals coming from:

- The military or any physical security discipline.
- IT system and network administration.
- Directly from a university with an IT or IT security or information assurance degree.
- The IT computer gaming industry.
- Software development (programming).
- A mixture of the backgrounds mentioned above.

Different backgrounds normally bring with them distinct, possibly complementary, working methods.

---

[1] Damasio (1994), Chapter 7, 'Emotions and feelings'.

[2] See Section 2.6.

[3] For example, the trigger for many IT security experts to develop their passion was the fact that they were victims of a hacking attack themselves.

[4] Should that be the case, then they need to find their passion or remain in the small non-passionate side of the team. See Section 3.5.

[5] See Section 2.7.

6.1.3 Brief History

IT is a young discipline. The first electronic computers[6] date from the 1940s. The job to secure IT was born immediately afterwards. Although IT security is already entering in the mainstream within the IT industry, compared to other fields such as architecture or medicine, we are still making our first steps as a profession.[7] IT security is an occupation in which the male gender is still a majority.

6.1.4 Continuous Change

New vulnerabilities appear almost every day in the IT systems we use. The number of security tools that we can use is also permanently increasing. IT security is a growing industry that is in constant change.[8]

"Securiteers" need to adapt to change when actually we know that human beings have difficulties to change.[9] Self-aid books such as "Where is my cheese[10]?" and "The Way of the Cockroach[11]" provide "securiteers" with tips to adapt to change.

6.1.5 Hacking Comes From Curiosity

IT security protects systems from being hacked. The first step towards protection consists of finding out those hacking techniques. Hacking consists of finding new unexplored ways to obtain value from a system in an exercise that attempts to outsmart system designers, users and administrators.

Babies hack all the time. Out of their intellectual curiosity, they find out how they can use what they have at hand. IT "securiteers" require a hacker mind to solve the defence puzzle. They need to master how hackers can compromise their systems in order to protect them.

All the traits we have exposed here constitute what we call the "IT security paradox": Security professionals come from different backgrounds with a common passion, i.e. outsmarting system designers. "Securiteers" transform their passion

[6] See http://en.wikipedia.org/wiki/Computer. Last accessed 20-09-2009.

[7] See Section 2.1.

[8] See Section 2.1.

[9] Leavitt et al. (1989), pp. 669–671.

[10] By Spencer Johnson. Published by G.P. Putnam's Sons (New York, 1998).

[11] The Way of the Cockroach: How Not to Be There When the Lights Come on and Nine Other Lessons on How to Survive in Business by Craig Hovey. Published by Saint Martin's Press (2006).

into a profession, firstly, to advise decision-makers in organisations about the IT risks they take when they make business,[12] and secondly, to implement mitigating measures according to their risk appetite.[13]

This arena is a moving target on which security professionals focus their passion, curiosity and effort with the ultimate goal to achieve a stable level of protection in the long-term.

6.2 How to Build the IT Security Castle

We have titled this chapter "Building a Human System". In the Middle Ages, powerful knights dwelled in impregnable castles where they could live safe from the attacks of their belligerent enemies. These fortresses offered protection to their owners and the peasants living nearby. They were pieces of security architecture.

Castles were built with security elements designed to deter threat agents from materialising the risks they posed to their inhabitants. Deterring measures such as the curtain walls, the moat surrounding the castle, the gatehouse, the drawbridge, the keep and the battlements were part of the defensive architecture.

The task of the IT security team is also to build a security architecture. This time, they are protecting an organisation from internal and external threats. Instead of stone and wood, as they used in the Middle Ages for their castles, team leaders employ a group of IT security professionals to build a "***human-based protection system***", the "IT security castle", with the following security elements (Image 6.1):

6.2.1 Archers Ready to Battle from the Battlements

The experience in technical topics and soft skills accumulated by senior team members and the leader guide the present and future of the team. They constitute what we call the "***team board***". Usually "*team board members*" are the leaders of the mini-teams created within the security team.[14] They need to attract talented and passionate IT "securiteers".[15]

The team consists of technical and not so technical team members. All interactions among all team members need to be based on respect.[16] The "***team board***" sets

[12] There is no business possible at zero risk.

[13] See Section 1.13.

[14] See Section 1.10. If the leader of a mini-team is absent, members of the mini-team can report to a 'selected' team member or to the main team leader.

[15] Peer pressure is much powerful than the concept of a boss. Gladwell (2000), pp. 70 and 186.

[16] See Section 3.2.

Image 6.1 Building the IT security castle

the pace of the "human system". They are responsible for inoculating a positive auto-dialogue to themselves and, consequently, to the entire team:

6.2.1.1 Thinking Positively

The following "change of mindset" is an example of a positive auto-dialogue:

Instead of sharing with junior team members the generic statement "no one cares about security in this organisation", even if leaders think it is true, they should shift the focus to more positive facts and use statements such as "the tasks we perform improve the security of the organisation and also our professional profiles".

It is a very subtle change, but very soon all junior members will replicate unconsciously this "positive auto-dialogue" and the team will focus on the positive side of things.[17] Especially in IT security teams, following this technique could mean avoiding frustration for a longer time.

6.2.1.2 Alternative Views

The "***team board***" is in charge of building the "IT security puzzle" in the organisation they work for. We advise to gather alternative, even opposite views in the "***team board***".

[17] Adapted from an interview the communicator Eduard Punset made to Professor Gary Marcus, psychologist at New York University talking about his book Kluge (2008). See http://www.smartplanet.es/redesblog/?p=460. Last accessed 20-09-2009.

They should be used to triggering brainstorming sessions and eventually agree on a unique[18] way forward after a fact-based professional discussion, similarly to what we proposed in Section 5.2 to break tasks down into "baby steps".

This way, the team achieves "the best homogeneity out of the best heterogeneity". After a decision is taken, the entire team need to maintain it. Otherwise, a team with fundamentally dissenting "board members" split up sooner than later.

6.2.1.3 Broad Technical Knowledge

"***Team board***" members need to cover technical expertise in all five dimensions mentioned in Section 4.9. In addition to that, the leader needs to share with the board the input they gathered from the motivation and internal balance assessments.[19]

6.2.2 The Keepers of the Gatehouse

Who can join the team? Sections 3.14–3.19 provide input on how to select the right candidate for the team. However, the team's selection panel could have hired brilliant applicants who aim to pursue a hidden agenda while they work inside the team (e.g. industrial espionage, secret services, intelligence gathering or, simply, an ill-intentioned individual). More generally, no selection process guarantees a candidate-position match.[20] The interviews and the tests performed could be sub-optimally designed or simply the candidate managed to give an impeccable but unreal impression.

IT security teams with operational responsibilities work with powerful tools, for example, in:

- Identity and access management,[21] they work with identities that have powerful access rights, enabling them to create fake users, provide additional access to existing users or potentially access business data themselves.
- Device administration and monitoring,[22] they could relax some firewall rules or disable alerts momentarily.
- Testing and incident response,[23] they could exploit an internal vulnerability they know and install a backdoor in a system in production.

---

[18] Even if afterwards they discover it is not the optimal path.

[19] See assessments proposed in Sections 3.3 and 3.5.

[20] Torrington et al. (2002), p. 188.

[21] See the "*blue team*" in Section 4.10.

[22] See the "*green team*" in Section 4.10.

[23] See the "*red team*" in Section 4.10.

Team leaders need integer professionals whom they can trust. Therefore, they need to have good keepers at the gatehouse screening candidates' backgrounds. We highlight three types of checks:

- Psychological tests to discard patent mental disorders and to assess their degree of resilience.[24]
- Criminal record evaluation to avoid hiring individuals with a recent violent or unlawful past.
- Financial organisations and institutions frequently perform credit checks on new hires to prevent individuals with frequent credit defaults accessing, e.g. payment system security-related positions.

Usually the physical security or the HR departments in the organisation carry out these checks. Although the "gatehouse keeper" role ends when the individual eventually joins the organisation, we propose to keep a probationary period for newcomers due to the critical roles that the IT security team play (Image 6.2).

The probationary period should be long enough to discover how the new colleague deals with their assigned activities. The "***team board***" will avoid assigning them crucial tasks. We recommend that a more senior team member will accompany them in their first endeavours for the first 3–6 months.

If the team size is embraceable, we suggest inviting the newcomer to shadow each team member for a day so that they familiarise themselves with the team tasks and, more importantly, they get to know personally all members. Interestingly, non-passionate team members usually dislike the "shadow exercise".

Image 6.2 The "gatehouse keeper" checks who joins the team

[24] See Section 2.6.

6.2.3 The Drawbridge

The IT security team requires a way to select which environmental elements reach the team and which elements they need to keep away from them, such as:

6.2.3.1 Time Thieves: Pull Up the Drawbridge!

We refer to any activity demanding more energy than the value it creates as a "time thief".[25] The team should avoid the "institutionalisation" of "time thieves", i.e. "time thieves" becoming part of their daily activities. Among others, discussions in endless meetings, email chains and "task switching time[26]" qualify as "time thieves".

6.2.3.2 Improvisation: Leave the Drawbridge Ajar!

Improvisation is a last-minute resource for the team to accomplish urgent or unplanned tasks.[27] They are either worth the effort or just organisation's emergencies[28] that need to be accomplished and the team could not plan them in advance.[29]

The team should be able to improvise but they should not resort to improvisation in most of their operational services.[30] Operational activities are significant enough to prepare operational procedures, test them and train team members in delivering those services with quality.

6.2.3.3 Rumors: Pull Up the Drawbridge!

Everyone in the organisation is exposed to hearsay. There are always rumours and legends on, basically, every individual in the organisation and certainly in the team. Team members should give no credit to any hearsay. The team and all members should cultivate their professional and personal reputation[31] and this is never achieved by contributing to extend hearsay through the organisation.

---

[25] See Section 5.1.

[26] Frequent when doing "multitasking" (see Section 5.7).

[27] Emergent activities.

[28] Sometimes IT security team members would have difficulties to consider them a real emergency for the organisation.

[29] Usually because the team was not informed on time by other players. IT security team members should try to avoid this scenario.

[30] Usually improvisation leads to more errors than when following a plan.

[31] More on reputation in Chapter 7 (viral marketing).

6.2.3.4 Personal Contact: Pull Down the Drawbridge!

What moves every team member every day to come to work? Team leaders need to know the answer to this question and share it with their peers. Every team member's motivation to work is deeply anchored on their "personal philosophy", on their system of ideas and values.

As the aim of an IT security leader is to build a "human-based protection system", every component needs to know every other element in the system. This is a pre-requisite, for individualities, to care about the group they belong to and, for the group, to eventually become a team. Time, work and non-work related group conversations, together with bilateral exchange of views, contribute to create a real team (Image 6.3).

6.2.3.5 Reality and Satisfaction: Pull Down the Drawbridge!

No one in the team should shut their eyes and reject reality. Reality must permeate into the team. There is no need to live inside an ivory tower. On this respect, the team have to keep most of the time the drawbridge down.

Team leaders should find out the needs of the organisation,[32] but also the "***team board***" should identify the basic requirements of team members (related to their

Image 6.3 Team leaders need to keep the team in contact with reality

[32] See Section 1.19.

working environment, to their family duties or simply to their hobbies) and work actively to satisfy them if they are practicable and have a demonstrable link to the performance of the member.

There will be moments throughout the year when the "***team board***" could be unavailable (sick leaves, holidays, trainings, etc.) and someone else in the mini-teams needs to "hold the castle together". While interacting with team members to learn about their personal traits and challenges, the team leader will gather valuable input to know who in the team is capable, and willing, to carry out a coordination role.

6.2.3.6 Clear Communication: Pull Down the Drawbridge!

Most of the new ways to communicate, like entertaining presentations, inspiring speeches or worth-remembering videos, start off in the organisation but outside the IT security team, be it in the marketing or in the public relationships departments. The security team need to keep the door and their minds open to communication.[33]

Interaction Patterns Within the Team

In the first two sections of this chapter we have presented the current traits of the IT security profession and we have proposed some elements that need to be present, and some others that need to be absent, when building a "human system" out of an IT security team.

The second part of the chapter identifies frequent patterns of interaction between team members that play different roles in the team, with a special attention to the way senior members and team leaders interact with other team members.

The foundation for the following sections resides on the basic respect that needs to reign among team members.[34]

6.3 Technical Versus Non-technical Mini-teams Within the Team

Section 4.10 introduced the idea of several mini-teams within the IT security team. They are led by senior team members, the "***team board***" and they focus on specialised, but closely related, IT security topics.

We add a third pillar to these two basic principles of mutual respect and humbleness: No one in the team is more intelligent than the team as a collective entity.

---

[33] See Chapter 7.

[34] See Section 3.2.

The threat to technical hands-on members is to consider that they provide much more value to the team and the organisation than their non-technical team peers, who write policies, procedures or support the team performing administrative tasks.

We do not recommend the creation of two classes[35] of professionals in the team. We propose to connect the tasks of the policy-related team[36] with the incident handler and security testing team.[37]

Introducing compulsory technical compliance checklists in system security policies is a way to achieve the connection between the policy and the testing side. This way, system owners have to engage the *red team* to confirm that their IT systems comply with the security policies enforced by the organisation and elaborated by the *yellow team*.

The *red team* will use their hands-on technical knowledge to test system compliance and they will liaise with the *yellow team* to try to automate most of the security checks proposed in the hardening guides that are attached to the security policies.

6.4 The Guru Working with the Non-gurus

The aim of the security leader is to place technically excellent IT security professionals with considerable experience in senior team positions so that they can lead the proposed mini-teams.[38] We call gurus to those experienced professionals excelling in their area of expertise, especially if they are really hands-on.

Team leaders have to identify any teaching and mentoring skills present in gurus working in the team. Gurus need to share their knowledge and experience with junior team members working with them in their mini-team.

Gurus have to understand that sharing their expertise with other team members does not decrease their professional value. The years of experience "under their belt" always remain with them. Excellent professionals recognise rather quickly the benefit to spread their knowledge among team members: It is a way to keep them technically engaged and challenged, especially by motivated and brilliant junior members.

When possible, in addition to knowledge sharing, gurus should like to mentor the gurus of the future, the junior team members. Mentoring requires patience, extra effort and time.[39] It is one of the most rewarding tasks that a professional can live. Very soon, mentored juniors emulate attitudes and behaviours that they observe in their mentor.[40] Both current and future gurus could be extremely helpful in security marketing campaigns within the organisation.[41]

---

[35] Later on in the chapter we discuss the user access administrator case.

[36] See the *yellow team* in Section 4.10.

[37] See the *red team* in Section 4.10.

[38] See Section 6.2.

[39] See Section 3.9.

[40] Torrington et al. (2002), pp. 430–431.

[41] See Chapter 7.

All technical aspects considered, team leaders should aim to hire non-arrogant technical gurus, able to lead their respective mini-teams, with a desire to share their expertise and to train young professionals. Consequently, we suggest gurus avoiding the "doctor effect", i.e. when a patient leaves their doctor's practice with the feeling that the doctor lacks understanding and interest in them.

6.5 Tasks for the User Access Administration Team Members

The mini-team in charge of identity and access management should also lead the role-based access control decentralisation initiative,[42] if they have sufficient resources. These two activities, though of different nature, the former "runs security" and the latter "changes security", have a direct benefit on each other if they are performed by the same actors.

Professionals with skills to change processes normally also show ability to run processes.[43] However, the opposite is not always feasible: There are individuals who are capable of following an established procedure but they are not ready to design or change processes.

We suggest following two possible approaches with operational identity management tasks ("running security") in the team:

6.5.1 Juniors Run the Identity Shop

Team leaders can assign the task, identity creation plus access right assignment, to junior team members as a way for them to get to work with user repository technologies and their administration tools.

The positive side of this approach is that junior team members are highly self-motivated professionals, with a drive to learn while they accomplish their assignments. However, they will soon get bored and be under-challenged with such tasks. By then, team leaders need to come up with a smart mix of tasks, such as user access management tasks plus some other more creative IT security activities like penetration testing. There is an aspect not to forget: Team members, whose assigned tasks require a very different set of skills, are more cumbersome to coordinate, and eventually, to keep in the team.

Identity management tasks are normally associated with stringent service level agreements. This means that when the team receives a high number of such requests, this "running activity" takes priority before the pursuit of any other security task.

---

[42] See the *blue team* in Section 4.10.

[43] Although running an activity for some professionals focused on changing is extremely unappealing.

However, from the security viewpoint, this task should not become the main destination of resources and time for any IT security team.[44]

In reality, it could mean that there is, literally, no time available for more challenging and value-creating activities in the team. If the scenario we describe becomes usual, junior team members will leave the team.

6.5.2 Release Skilled Members from Identity Management Tasks

Team leaders can also transfer identity management tasks to profiles that are not so skilled in other aspects of IT security. To do so, leaders need to agree with them clear game rules and objectives in order to avoid misunderstandings when they will appraise those team members tasked with identity management-related requests.

The data confidentiality[45] aspects of the activities assigned to the *blue team* justify definitely our proposal in Section 4.10 to decentralise user access management activities among business data owners throughout the organisation and automate identity management as much as possible. The *blue team* would design and implement the user access management decentralisation task and would audit identity management assignments performed by business users.

Life Always Finds Its Way: Working in the Organisation

Abandoning their tendency towards perfectionism, leaders should pay attention to the mood that they and their team members show, every morning, when they enter the organisation's facilities and when they leave in the evening. It is a clear sign of the soundness of the team. The third part of this chapter proposes a selection of HR and management methods to sustain the "human system" intended for a working security team.

6.6 How Team Members Deal with Problems: Using the Socratic Way

Every team member performs tasks. Together with the activity, the satisfaction to finalise it and the responsibility to steer it come within the assigned package.[46] When that team member faces a problem, the leader or a senior member has to support and provide guidance on the matter.

---

[44] IT security teams provide more risk-mitigating value to the organization in other IT security operational tasks.

[45] The most appropriate party to assign access rights to data is the data owner.

[46] See Section 5.4.

Senior team members should not take ownership of the issue unless:

– The initial assignee seems overwhelmed.
– The conflict threatens the mandate or the existence of the team.

Providing guidance and expertise without seizing problem ownership is a skill that the "***team board***" needs to acquire and fine tune. In a similar way as the Greek philosopher Socrates let his interlocutors find answers to the questions they had inside them, the leader needs to guide the team member, first, through a meditated thinking process and, second, through the elaboration of an action plan to solve, mitigate or, simply, skip the problem.

The proposal to keep the initial ownership of a problem applies also to team leaders. Whenever they face a problem, we do not recommend a direct delivery to their line or senior management unless team leaders also put forward a proposed way to proceed. No one in an organisation stays happily ready to receive and own a problem created by someone else.

Remaining focused is crucial in the guiding process proposed in this section. The team member has to keep their attention to the mandate of the team[47] and deliver. Focus prevents IT security teams from finding themselves in an awkward position, such as being stuck in a personal confrontation against someone in the organisation or just caught up in confusing secondary activities.

6.7 How to Manage Working Time

Workers in an assembly line signal when they need to leave the line so that someone else can take their position and production continues. They normally work in shifts with defined start and end times. Supervisors control presence and working time.

Apart from possible shift work[48] that could exist within the team, as it happens in alert monitoring or access requests,[49] the IT security team should not be controlled like an assembly line.

We propose to follow a ***result-based supervision method***. Team leaders need to guarantee the provision of services by the team, as agreed with the customers. For example, the organisation requires the team to provide their operational services and that means that the team need to be present during certain working hours. This is the only time control we suggest to maintain.

IT security does not need leaders measuring the time that their team members are present in their cubicles. The way to supervise team performance pivots on

[47] See Section 1.19.

[48] Torrington et al. (2002), pp. 157–159.

[49] See the *red*, *blue* and *green team*s in Section 4.10.

delivered results and subsequent quality checks using security key performance indicators. However, for some employers, applying a result-based supervision instead of a time-based control still constitutes a real breakthrough.

When it comes to manage leave requests, we suggest following basic principles that would make the team an attractive place to work at. Every team member should take leave when they desire provided that three conditions are met:

– Services rendered by the team are guaranteed.
– No pending task is left without a proper handover to another team member.
– Leavers should indicate their potential availability during their absence.

The first two conditions seem common practice but experience shows that team leaders need to reinforce them so that they become accepted routine within the team. The third condition refers to a potential contact with the team member on leave only in very exceptional occasions, such as a pandemic or a critical security incident.

Those three conditions also apply when the team need to decide which members will attend a training course, a conference or any event to which all of them have been invited.

As everyone in the team should take some leave every year, a consequence of the second condition we mention is that there is no task in the team depending solely on one individual.[50] Every team needs to stay away from depending on one

Image 6.4 IT security teams require result-based control towers

[50] One-person teams require the collaboration of at least another colleague in the organisation.

single individual. Otherwise, just a simple sick leave and the team could be out of the running game (Image 6.4).

6.8 How to Fine Tune the "Human System"

In this section we enumerate several techniques to achieve cohesion and re-invent the team every now and then:

6.8.1 Task Rotation

This is an instrument that team leaders can use to keep freshness in the team: Two colleagues swap the activities they perform so far. We distinguish three types of rotation:

- Within the team: It is somehow easy to implement and it constitutes a minor change for the team.
- With other IT teams: It is an opportunity to get closer to other IT colleagues and discover synergies.
- With business areas in the organisation (or even with other organisations): It is more difficult to find a potential candidate but, if successful, it positions the team closer to business areas or to other organisations.

The swap of tasks should offer a return ticket. It is not a way to get rid of a disturbing team member but rather a reward to those colleagues with curiosity and will to learn new skills. They will increase the team's resourcefulness upon their return.

6.8.2 Trial and Error

Will anyone in the team be ready to take over a task? Team leaders will only know if they assign the task to a member, guide them through the journey of trying to accomplish it themselves and finally assess with them the result.

No team member should be afraid of failure.[51] Human beings normally learn more from failure than from success. Team members can take the risk of failing in their task assignment if, on paper, they are certain that it could work. It is the only possibility that they have to check whether junior members can excel on a certain IT security topic.

[51] See Section 3.12 on mistakes.

6.8.3 Competition in the Team

The team needs to welcome signs of healthy competition among their members. Competition is, by itself, a magnificent tool to keep team members focused and to sharpen their skills. We only add three limitations to internal competition:

- Competition has to be transparent and limited to a specific professional topic.
- Competitors should first work for the team and second for their competitive motive.
- Winners commit themselves to train team members on their "successful arts".

6.8.4 Types of Contracts in the Team

It is very rare to find teams whose members have all of them the same type of contractual relationship[52] with the organisation they work for. Typical sorts of affiliation we find nowadays are:

- Staff members with an unlimited contract.[53]
- Staff members with a limited contract of employment.
- Internship agreement (typical for trainees).
- Consultancy agreement (company to company or company to freelance relationship).

Team members' attitude, drive and degree of responsibility vary according to which type of contract they have with the organisation. The leader and, in general, the entire "***team board***" should interact with every team member on equal terms, regardless of the type of contract they use. The only differentiating parameter will be the length of their stay within the team. Those remaining in the team for a short period of time should not lead long-term activities.

There is a series of thoughts that team leaders and members can use in their daily coordination tasks:

- No one in the team should decide on important topics under stress.[54]
- Everyone should avoid a permanent status of anxiety. We can stay outside our comfort zone only temporarily.
- Finally, they should start looking for another job only when they are comfortable in their current job. Otherwise, they will simply try to leave a place.

[52] Torrington et al. (2002), pp. 154–156.

[53] This is almost an extinct species.

[54] See Section 5.1.

Team Member Development and Appraisal

The team leader should convey a feeling of transience to all members. Nothing is permanent, seating plan and task allocation grid included. An ideal instrument to convey this learning point is the training strategy for the team. At the same time, the leader should perspire calmness and reflection in their acts within the team. The appraisal process is an activity where the leader can show that calmed reflection. This final part of the chapter discusses training and appraisal measures.

6.9 Training Measures

We live in a lifelong learning society.[55] Information technology (IT) is constantly advancing and with it, IT security follows even a faster changing path. Every IT security professional must embark on a continuous learning and self-development journey.

Passionate team members train themselves in the use of new techniques, new tools and new defensive and offensive approaches. The leader can only encourage them to continue their journey and reward their learning habits.[56]

Those team members with not so much time available or will to follow a continued training path require support to follow some lightweight training measures just to avoid losing their technical, procedural and organisational skills.

We suggest team members themselves,[57] with some guidance from the leader or from senior team members, to be the main decision-makers when selecting a training measure. There are many possible training measures available for team members:

6.9.1 On-the-Job Training

Although it does not consist of attending a conference in a fancy venue, it is definitely one of the most effective ways to learn. When a junior team member shadows a senior colleague working in a specific IT security topic, the team increase available skills in three ways:

---

[55] A UNESCO report on education, titled "Learning to be" (1972), also known as the Faure Report, foresaw lifelong education as a transformative and emancipatory force in the entire human society. Read more at http://education.stateuniversity.com/pages/2181/Lifelong-Learning.html. Last accessed 20-09-2009.

[56] See Section 3.12 on rewards.

[57] We learn something we like or something we consciously choose in a quicker and easier manner. Adapted from interview by Eduard Punset to psychologist Walter Mischel, professor at Columbia University. Interview available at http://www.eduardpunset.es/index.php?vim=46&pageNum_vim=0. Last accessed 22-09-2009.

– The junior team member acquires new technical skills.
– The senior member sharpens their technical skills.
– The senior member also trains their teaching skills.

In addition to this, teams increase cohesion and communication among their members. Junior and senior members can swap their roles if the former masters a new technique that the latter would like to learn.

6.9.2 Certified Trainings

Attending training sessions that offer the possibility to pass an exam afterwards and receive an industry-demanded certificate is a sensible training measure,[58] especially at the beginning of an IT security career.

It is crucial to provide the "recently trained" team member with the real possibility to apply what they have just learned from the first day they are back in the office. This includes a summary presentation to the rest of the team. This way, team leaders avoid:

– Losing the investment that the member and the organisation made on the training measure.
– Team members believing that, given their recently acquired skills, they are "under-challenged" in the team.

6.9.3 Security Conferences

Conferences are an excellent training measure especially for those team members that are willing to sharpen their skills, to look after their networks,[59] and to share knowledge with the IT security community.

Leaders need to encourage team members to participate in security conferences such as Defcon, Blackhat, RSA or OWASP by presenting papers that could be of interest for the entire community. This is certainly a challenge for team members, only few high-quality up-to-date technical papers will go through and be accepted by conference editorial boards.

Writing and publishing technical papers on reputable magazines and sites, developing open source tools for the security community and discovering new vulnerabilities, place senior team members within the prestigious group of renowned IT security professionals.[60]

---

[58] An example of certified training is the Sans GIAC offering. See http://www.giac.org/overview/. Last accessed 20-09-2009.

[59] More on networking in Chapter 9.

[60] More on personal branding in Chapter 9.

6.9.4 Product-Related Trainings

These training measures are unavoidable, especially for teams with operational responsibilities.[61] However, we recommend taking extra care in their design (duration, content, labs, etc.) and to request qualified but, above all, highly communicative trainers.

Product trainers need to trigger passion for IT security or, more specifically, for a tool such as a firewall or an intrusion detection system (IDS), among team members. Boring and dull product-related trainings are detrimental to raise the team's morale and interest in new topics.

From the planning point of view, team leaders need to include them in the annual team work plan so that the provision of the team's daily services is not affected by the fact that some members are attending a training session.

Finally, we suggest introducing a common principle for all team members: Upon their return from a training measure, they will prepare and offer, to interested team members, a summarised version of the training that they attended. This suggestion is especially relevant when the team have a scarce training budget. Briefing the team on a training measure is both beneficial for the trained member, who has to review and to summarise the material and becomes a trainer for a while, and for their peers, who get to know the most decisive points of the training sessions.

6.10 Appraising Team Members

We propose leaders to follow a simple ***fact-based*** and ***result-oriented performance management*** model: The performance cycle.[62] It consists of three stages:

6.10.1 Performance Planning

The team leader agrees with the team member the planned activities that they will have to perform in the next cycle. It is the right time to add facts (requirements), figures (duration and costs), performance indicators (KPIs) and assessment patterns that will be used to evaluate the activity.

6.10.2 Supporting Performance

The team member briefs the leader regularly on the developments in their assigned activities and receives their required support. Both are able to identify potential

[61] Operational security teams need to run a range of security tools.

[62] Torrington et al. (2002), pp. 297–302.

delays and issues upfront. The team member organises the follow-up sessions throughout the year. They can be formal or informal meetings, whatever suits best both players. Their frequency will depend on:

- The complexity of the activity.
- The relevance to the team.
- The seniority of the team member and leader.
- The required level of active support by the leader in the activity.

6.10.3 Reviewing Performance

At the end of the performance management cycle, usually after 6 or 12 months, the team leader organises a session to review and evaluate the performance against the agreed quality parameters. This session is accompanied by a written evaluation report.

We stress the fact that leaders should objectively appraise task-related performance and not the team member's human traits or soft skills. To follow a fair approach, proactive leaders will use the appraisal session to give appraisees the chance to evaluate the leader's performance on the activity and, more broadly, on the team coordination task.

Leaders can make use of the sessions devoted to assess the team member's motivation and internal balance[63] to review their performance following the performance cycle method presented here (Fig. 6.1).

To sum up, in this chapter, we have delved into the dynamics present within the team, the necessary components to build a "human system", typical interaction patterns present in most teams and useful tools for leaders and members to deliver results while enjoying their time together.

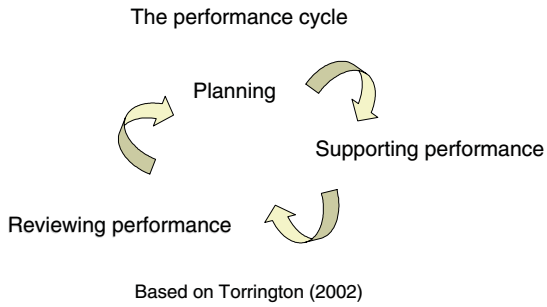

Fig. 6.1 A fact-based result-oriented performance management model

[63] See Sections 3.3 and 3.5.

Chapter 6: Learning points

- IT security professionals are curious, passionate and heterogeneous.
- The "team board" sets the pace in the team and guide members.
- Respect and lack of arrogance are the foundations of team dynamics.
- Technical and non-technical colleagues should work together.
- The team need understanding gurus who are willing to share and teach.
- Identity management tasks deserve special organisational attention.
- Problems should not be simply handed over.
- Result-based management takes priority over measuring presence time.
- Task rotation, trial and error and internal competition are useful tools to fine tune the "human system".
- Different team members require different training measures.
- Appraisals follow a fact-based result-oriented performance management method.

Link to MBA Management Models

We have selected two MBA-related models that could help leaders to assess their leadership role in the team:

Action-centred leadership *(by John Adair, 1983)*
Leaders need to manage three types of needs in a group of people:

– Tasks needs (need to deliver).
– Group needs (working culture and spirit).
– Individual needs (understanding people).

A good leader achieves balance among the three types.

Managerial grid© *(by Blake and Adams, 1991)*
A manager style is plotted in a grid according to two dimensions: concern for people and concern for production. An effective manager needs to adapt their style according to circumstances. The five different types are:

– Country club management (concern for people but not for production).
– Impoverished management (no concern).
– Task management (concern for production but not for people).
– Team management (concern for both).
– Pendulum (lack of definition).

See reference: Harding and Long (1998).

Link to Nature Management Models

For this chapter, in addition to the MBA models, we provide three references that describe behaviours found in animals that provide some light on ways to make decisions, work in teams and stay calm:

The Best Decisions Are Those One Comes to Profiting from the Cleverness of Rats
Rita Pohle proposes to look at the way rats act when we are confronted with change in our lives. Published in German by Ariston (2009).

Our iceberg is melting
John Kotter and Holger Rathgeber deal with change and how a team is always stronger than an individual. Published by St. Martin's Press (2006).

"Die Bärenstrategie" [The strategy of the bear]
Lothar Seiwert suggests being as calm as a bear to gather and increase our strength. Published in German by Heyne (2007).

Chapter 7
Viral Marketing

Chapter 7: What will we learn?

This chapter answers the following questions:

- Why should IT security teams communicate?
- To whom should they communicate? Who is their audience?
- Which communication principles should they follow?
- What should they communicate?
- How do they go from awareness to marketing?
- What is the "extended marketing mix" for IT security?
- How do IT security teams position themselves in the organisation?
- Which type of marketing style should they practise?
- What does a viral marketing sample look like?
- Who are the "security connectors"?
- How can the incident response team market IT security?
- Which "security stories" do IT security teams need to sell?
- How can security teams benefit from human psychology?

This chapter points out who is the IT security team target audience, why and how they should communicate their message and which messages they should propagate. We complement these three aspects with references to marketing and psychology literature that provides security leaders with useful tips to sell security.

A. Partida and D. Andina, *IT Security Management: IT Securiteers - Setting up an IT Security Function*, Lecture Notes in Electrical Engineering 61,
DOI 10.1007/978-90-481-8882-6_7, © Springer Science+Business Media B.V. 2010

Communication to Sell IT Security Services

The following sections introduce the reason why IT security teams have to communicate to accomplish their mandate, who are the recipients of those security messages and, hence, of the security services. We also describe the principles that security teams should follow when they convey those contents.

7.1 Why Should IT Security Teams Communicate?

IT security is a support area within the organisation.[1] They provide services to customers, who can be colleagues working in business areas or final clients outside the facilities. As any service provider, they have to market their products and position their team either in the internal market (within the organisation) or in the commercial market (if they sell managed security services). There are three main reasons why IT security teams need to sell their products:

- The organisation is better protected against IT threats if they manage to engage everyone in a meaningful information assurance[2] initiative.
- They have a greater chance to accomplish their objectives[3] in the organisation if their colleagues in the business areas and other IT teams are aware of the threats affecting the organisation.
- The team need to provide convincing arguments in budget negotiation exercises to guarantee the continuity of the team.

There is an additional reason that is not directly related to the organisation but it can be an attractive argument for many colleagues: Individuals with some IT security awareness, working for the organisation, are also better protected against IT threats appearing in their digital lives outside work, e.g. at home or at their local community.

7.2 To Whom Should the Team Communicate? Their Audience: Their Stakeholders

The stakeholders we identified in Section 5.9 are the recipients of the security messages. Security teams require stakeholders, to a greater or lesser extent, to:

- Accept their existence in the organisation and their services.
- Ratify and use their security services.
- Become their convinced relays and potential security practitioners.

---

[1] See Section 1.12.

[2] Information assurance, a broader term than information security, delivers a suitable level of protection for the organisation's information (Ezingeard et al. 2007, pp. 96–118).

[3] To support the business with their IT security advice and actions. See Section 1.19.

Every stakeholder cluster demands different marketing measures and approaches. From the cluster we identified in Section 5.9, we re-visit the following ones:

7.2.1 Top Senior Management

They define the organisation's risk appetite.[4] Their support and commitment is decisive for IT security and the survival of the organisation. Chapter 8 expands on the relevance of management support.

7.2.2 Line Management

If they are not an active, and preferably IT savvy, player working for security, team leaders need to make them understand their ideas and plans so that line managers become their first convinced supporters, since they are usually part of the organisation's middle management layer.

7.2.3 Business Areas and Final Users

They are the team's main customers. The team need to orientate their marketing actions so that business areas will accept or even embrace security services. Business areas' assent will facilitate the realisation of the security team's mandate.[5]

7.2.4 IT Teams in the Organisation

The security team have to make them see that security activities complement the work of other IT teams in the organisation, i.e. the security team provide value and even a sounding board for their professional activity.

The main objective of the security team is twofold:

- To focus on stakeholders with high power regardless of the level of interest they display.
- To raise the level of interest in IT security showed by their stakeholders.

Realistically, with this objective, the security team need to focus on all stakeholders. An action from any of them could potentially affect the entire organisation.[6]

---

[4] See Section 1.13.

[5] See Section 1.19.

[6] For example, an unaware user double clicking on an email attachment could set into motion a destructive piece of malware in the corporate network.

This is the reason why we need to raise the interest of all security stakeholders. Any of them, being interested or not, given the ubiquitous nature of information technology nowadays, could potentially accumulate enough power to hamper any business process running in the organisation.

Raising risk awareness is the first line of defence of any information system and network.[7] The three most common mistakes that IT "securiteers" make in this field are:

- They give little priority, in terms of time, effort and resources, to communicating with their stakeholders.
- They think this activity is only a one-way communication from them to their stakeholders.
- The few marketing techniques that they use are primitive and not effective.

If team leaders follow the Pareto principle presented in Section 1.17, they soon realise that it is smart and convenient to look after their ***stakeholders***. A successful positioning strategy and communication programme by the IT security team may transform those stakeholders that demand and receive services, their customers, into the most relevant implementation engine they need to accomplish all their plans.

It is a win-win deal. Security customers and hence the organisation benefit from the security team's expertise while they keep on sponsoring and supporting the team, enabling the realisation of the team members' IT security passion and, simultaneously, the team members' professional career development (Image 7.1).

Image 7.1 Security should explain why, not scare

[7] ENISA (2006), p. 52.

7.3 Communication Principles to Follow

The messages that team members will broadcast throughout the organisation follow basic principles we are all familiar with. How do we explain a 5-year old kid why they should not accept any sweet from strangers or just walking away with them? We identify five key stages in this communication:

- We seek the kid's attention.
- We use a language they can understand.
- We convey the message, containing three main points:
  - What they should or should not do
  - Why they should act that way
  - What could happen if they do not follow the recommendation
- We check whether the kid understands the explanation by asking them to repeat the message with their words, for example by proposing them how they would tell the message to their buddy in kindergarten.
- We provide evidence of the benefits that they will obtain if they follow our piece of advice (we could continue playing with them every afternoon when we are back from the office).

We suggest the security team adopting this universal schema in all communications with their customers with three slight modifications:

– They should ***explain but not scare***.
– They should show a demo so that customers can easily understand their message.
– They should provide information about real cases[8] where the risk materialised.

By following the above, security teams move from the one-way communication paradigm commonly used in security awareness campaigns to a much more comprehensive marketing concept. The required resources are greater than those needed in traditional awareness activities but the leverage that the team will obtain is worth the effort. In the following sections of this chapter we will make IT security and marketing techniques converge into a comprehensive and effective communication initiative (Image 7.2).

7.4 What Should the IT Security Team Communicate?

The to-do list of the team is always full, as we have shown in Chapter 4. The three central reasons stated in the introduction of this chapter call IT security teams to embark on a permanent communication initiative. There is a variety of communications

[8]The IT security incident database we proposed in Section 1.15 could be of help in this scenario.

Image 7.2 Users will understand risks only by experimenting themselves

that the team need to broadcast. Each message deserves a tailor-made marketing design and implementation which should rest on the following pivotal ideas:

- All individuals working for the organisation are responsible for protecting the organisation's information.
- The task to protect corporate information requires everyone's participation and commitment.

These points are better received when they are inserted into a series of fine-grained communication elements that team members will bring to their stakeholders, i.e. their intended audience.

Each of the services that the security team provide is an optimal vehicle to broadcast their messages. A successful communication exercise will facilitate the delivery of their IT security services and, consequently, the security stance of the organisation will improve.

In this first part of the chapter we have introduced the target audience of the security team, the principles that should lead their interactions with their audience and the reason why they need to communicate. The second part of the chapter proposes to move from "just raising awareness" to "marketing IT security".

From Raising Awareness to Marketing IT Security

How can IT security be marketed? The majority of the security products are services. Nowadays, it is a common practice to make use of marketing strategies to sell services. This is exactly what we propose: IT security teams should market their security services to potential customers.

7.5 Characteristics of Services: From Awareness to Marketing

The provision of services[9] have different characteristics compared with the delivery of physical products:

- There is no change of ownership between the provider and the customer.
- Intangibility: There is no physical object exchanged.
- Inseparability: Services cannot be broken down into smaller pieces.
- Variability: Services are variable, there are no two identical service acts.
- Perishability: Services can only be provided when its provision starts.

IT security activities such as penetration tests, vulnerability assessments, security advice provision or access and device management, fall under the category of services and they are intangible, inseparable, variable and perishable.

Team leaders have to consider those features when they design their marketing strategy and implementation programme. The Chartered Institute of Marketing defines marketing as "the management process responsible for identifying, anticipating and satisfying customer requirements profitably". The steps included in this process coincide with our proposal to identify, anticipate and satisfy security requirements of the security team's customers so that their organisation survives, and even more, accomplishes its mission.

The similarities that we find between the marketing and the security communication activities justify our proposal to shift from a traditional security awareness programme[10] to a real marketing campaign for IT security services targeted to the security team's stakeholders, and more specifically, to their customers.

7.6 The Extended "Marketing Mix" for IT Security

Professional marketers talk about a set of four elements to define a campaign: Product, price, place and promotion. They call these elements the "marketing mix"[11]: The sale of a product at a specific price, in a determined place and after certain publicity actions.

Given that most security products consist of services and not of isolated physical items, we suggest following the extension of the "***marketing mix***" for services with three additional elements to conform the 7 P's model of the "extended marketing mix"[12]:

- Physical evidence: How is the physical environment involved in the provision of the service?

[9] Kotler (2003), pp. 443–452.

[10] One-way communication. See Section 7.2.

[11] According to Kotler (2003), p. 15, the marketing mix is a set of marketing tools (product, price, promotion and place) that a firm uses to pursue its marketing objectives in the target market.

[12] The 7 Ps of the "extended marketing mix" of Boots and Bitner expands the number of variables to control from four in the original marketing mix to seven. Extracted from http://www.12manage.com/methods_booms_bitner_7Ps.html. Last accessed 28-09-2009.

– Process: Which processes surround the provision of the service?
– People: How are the people providing the service?

We postulate the communication of the pivotal pair of ideas presented in Section 7.4, using the marketing concepts we have described. While IT security team members provide their services, they should tacitly propagate their security mantra: They are all responsible for the protection of the organisation[13] and everyone should be committed to safeguard its information.

How do security teams customise the "extended marketing mix" to their needs?

7.6.1 Product/Service

Any service provided must be a result of a tested and documented process. If the service is directly provided to users, the security team need to involve them and to interact with them. The offering of the team should be based on simple measures that do not require many resources.[14]

We frequently find IT security literature produced for final users using an admonitory and negative style, simply putting final customers off by telling them what they are allowed or not to do.[15] In the approach we propose, security teams should collaborate with their users and offer them the security-based added value that they require.

7.6.2 Price

Including security upfront when a new project starts is much more cost-effective than trying to secure an IT system in an isolated way days before, or even after, it goes live. How can security leaders show this fact to their organisation's decision-makers?

Although the security team's customers are possibly internal to the organisation, we propose to attach a price to each of the security services. Depending on the cost centre allocation policy present in the organisation, this could mean a real bill that the customer department has to pay or simply a piece of information, a figure, to include in the team's or their customer business areas' budget.

How will security teams charge their services? Simply put, they just allocate the real costs they incur in each service they provide. They come from the cost of the resources they use, e.g.:

[13] Albrechtsen and Hovden (2009), pp. 477 and 487.

[14] Albrechtsen and Hovden (2009), p. 484.

[15] Albrechtsen and Hovden (2009), p. 481.

– IT security professionals' working hours.
– Equipment (software, hardware and accessories).
– Logistics (facilities, maintenance, cleaning services, etc.).
– Corporate services provided by the organisation (HR, payroll, administration, etc.).
– Plus, in an IT security provider company, a certain profit.

7.6.3 Place

How do security teams bring their IT services to the market? We advocate for a "pull strategy",[16] i.e. for those services that the team provide directly to the users, security team members need to involve them in the design and in the provision of the service so that they actively demand their services instead of passively receiving them.

We propose to awaken users' desire to adopt IT security practices. Inviting customers to attend a demo of what can happen to their information and sharing some Q&A sessions with IT security professionals is an effective way to achieve their interest. Sending them an email with a new admonitory message about what they should not do provokes just the opposite effect on users.[17]

The security team's customers and, in general, their entire market also live within an endless information overload.[18] This fact obliges security team members to prepare messages for their services with a simple packaging. Customers need to accept what they have to do and understand why they should do it.

7.6.4 Promotion

Thanks to the team's marketing activities, customers will comprehend that the organisation's public image benefits from their IT security aware acts.[19] Security services need to be attractive for customers.

Team members can make use of security incidents covered by mass media and collected in the database[20] we suggest to build. Journalists are increasingly reporting about IT security breaches. Final users are really exposed to the magnifying effect

[16] The manufacturer uses advertising and promotion to induce customers to ask intermediaries for the product (Kotler 2003, p. 511).

[17] See Section 10.13.

[18] Albrechtsen and Hovden (2009), p. 484.

[19] Albrechtsen and Hovden (2009), p. 483.

[20] See Section 1.15.

that mass media create on the topics they report on. IT security news is not an exception. Customers are much more sensitive to risks they know or they have heard about.[21]

Consequently, security teams should build their "selling story"[22] having in mind the "risk experience" that customers have already acquired through news appearing on mass media. The aim is to make the most of the fact that customers pay more attention to risk impact than to risk probability when they evaluate risks.[23]

7.6.5 Physical Evidence

IT security team members, "***team board***" included, need to be physically present and visible within the organisation.[24] They all need to be accessible and interact with colleagues from other business areas or other IT groups. Proximity[25] to the business areas makes it more difficult for users to prioritise functionality, profit and productivity goals without considering their security dimension.

The accessibility we propose costs time, effort and resources to the IT security team. Team leaders have to account for them in their yearly activity planning.[26] When users put a face to IT security in the organisation, they will find easier to get their IT security questions and doubts answered. Attentive IT security communicators[27] should incorporate the answers that customers demand in their communication plan.

If the facilities where the IT security team reside are worth exhibiting, for example operational rooms with real-time monitoring systems showing security alerts such as intrusion attempts on big shiny displays, we suggest to take the opportunity and make them an element of the team's marketing campaign.

Every time that team members physically interact with their customers, they should offer an image of focused professionals, concentrated on providing added value services. Trivial details such as tidiness, order and elegance contribute to the shaping of the security team's image and reputation.

Customers need to trust their IT security teams. Whenever a security incident involving users takes place, security team members need users to provide them with reliable information. If they directly trust IT security team members, all subsequent interactions will be easier (Image 7.3).

---

[21] Albrechtsen and Hovden (2009), p. 488.

[22] See Section 7.11.

[23] Albrechtsen and Hovden (2009), p. 487.

[24] Albrechtsen and Hovden (2009), p. 484.

[25] Proximity outpowers similarity (Gladwell 2000, p. 35).

[26] See Chapter 4.

[27] See Section 2.3.

Image 7.3 IT security facilities can be a marketing element

7.6.6 The Emergency Room Effect

Whenever there is a disaster or an incident in the real world, the notorious physical presence that emergency services deploy at the spot sends a vivid message of "we have the situation under control" and "we are here to help". The team needs to look after the image they "imprint" on their customers in any interaction they have with users, but especially in visible security incidents that involve customers.

7.6.7 Processes

The team provide their services through processes. We suggest involving key motivated users in the design, or at least in the acceptance, of customer-facing services.

Every IT security team member can contribute to identify those security aware colleagues working in business areas who show willingness to cooperate with IT security. They can happily provide their experience on business processes and their daily contact with the business.[28]

[28] Albrechtsen and Hovden (2009), p. 478.

7.6.8 People

Chapters 3 and 6 go deep into the traits that team leaders will gather and develop in their team to create a reliable "human system". In this section, we stress the fact that each team member should become an ambassador of IT security and the IT security team.

7.6.9 Power to the Users

The bet we make with this element is to convey the power that IT security teams claim to have in the organisation to the final users, so that they are really responsible for following IT security principles during their everyday work. Actually, extensively accepted operational risk frameworks[29] propose to ensure that risk management is part of everybody's job description in the organisation.

7.7 How to Position the IT Security Team

Where would team leaders like to see their team in the organisation's landscape? Together with a strategy to sell their services, they need to set up a strategy to promote the team within the organisation. The team need to offer innovative services in a business world where good performance and product quality are deemed as commodities.[30]

The same way a company needs to position itself in the market[31] to earn investors' confidence, the team should occupy a distinctive place in the mind of their target audience. Before defining the IT security team's positioning strategy, we focus on their market.

7.7.1 The Market

Broadly speaking, everyone using any information technology-based system in the organisation where the security team provide their services, belongs to their target market.

---

[29] Such as the case of COSO (2004), pp. 1–103.

[30] From marketing lectures prepared by Stephen Lee and Robert Hattemer (Henley Management College MBA, 2006).

[31] Kotler et al. (2004), p. 183.

Marketing theory proposes to identify groups of customers with similar needs, wants and priorities. Each group is called a ***segment***.[32] Every segment has its relevance[33] and its specific demands. Security teams need to identify them. To avoid superfluous complexity, a first distinction will be to consider each stakeholder cluster a separate segment they need to serve with customised services.

Once the market is known, we suggest to use the 4 C's model to position a brand[34] for the IT security team:

7.7.1.1 Clarity

Security teams need to be extremely clear with the value proposition for each of their segments:

- Top senior management (the organisation's executives): The IT security team provide expert IT security advice and help to manage risk complexity.
- Line management: The security team contribute to the mission of the organisation and, at the same time, to the continuity and success of line managers.
- Business areas and final users: The security team help them in all their IT security matters and secure their business processes.
- IT teams in the organisation: The input of the security team increases the value they render with their services.

7.7.1.2 Consistency

All security messages need to be founded on identical security principles.[35] However, the security team will provide IT security expertise to all their stakeholders in the form, and at the pace, they require.

7.7.1.3 Credibility

The security team will focus on real risks with real and documented occurrences,[36] avoiding "cry wolf" stories. *Raising unjustified and frequent alarms brings anxiety and distress to the organisation*. The team will grow in credibility and trustworthiness if they grant attention and priority to possible and probable risks.

---

[32] Kotler et al. (2004), pp. 181–183.

[33] Based on its potential to contribute to a secure organisation.

[34] See Blythe (2006), p. 204.

[35] See Sections 4.2, 4.3 and 4.4.

[36] See Section 1.15.

7.7.1.4 Competitiveness

The security team should identify who are their competitors. Even if there is only one IT security team in the organisation. There are external competitors like providers of managed security services[37] and internal ones such as other IT groups willing to take over or already carrying out security activities.

When the team design their services, they need to offer any value that their potential competitors cannot offer. For example:

- A broad experience and knowledge of the intricacies present in the organisation. This can be an argument to skip outsourcing initiatives.
- Dedicated focus and expertise on IT security topics.[38]

7.8 Viral IT Security Marketing

Relationship marketing aims to identify, maintain and enhance relationships with customers and stakeholders at a profit.[39] The concept of profit in the case of the IT security marketing refers to the level of security the organisation can achieve. Therefore, we propose security teams to create and nurture strong links with their customers to better provide the IT security expertise the organisation demands.

The two basic requirements for relationship marketing are[40]:

- Objectives of all parties, business areas and security, are met.
- Promises are mutually exchanged and fulfilled.

Both requirements depend on a clear, understandable and fully customised communication channel between customers and IT security.[41] We suggest creating a new communication paradigm making use of pre-existing ***social networks*** that are available in the organisation.

Following the spirit of viral marketing, i.e. individuals with high social connectivity[42] within the organisation will use their personal contacts to increase, in this specific case, IT security awareness and acceptance throughout the organisation.

If the security team spread, through word-of-mouth, few, but smartly selected, messages, their customers would be much more aware of security. We label this type of marketing as viral, i.e. IT security messages infect the organisation similarly to biological or computer viruses. We refer to message broadcasters as "infected users".[43]

---

[37] The threat to outsource IT and IT security services is growing.

[38] A potential argument against security tasks taken over by other IT teams.

[39] Adopted from Kotler (2004), pp. 13 and 29.

[40] According to Gronroos (1996), pp. 5–14.

[41] See Section 5.10.

[42] Gladwell (2000), pp. 38–46, refers to these individuals as connectors.

Contrary to natural viruses, this replication mode is not infinitely sustainable in marketing. Viral marketing campaigns "infect" new individuals only for a certain period of time. However, security teams can make use of the time limitation to their benefit:

As they have a number of messages to convey, they can launch consecutive viral IT security marketing campaigns, each of them focused on a specific "IT security story". These are examples of typical "security stories" whose distribution requires much more effort than a poster or a long memo hanging on a bulletin board in a public place within the organisation:

- Users checking email attachments before clicking on them.
- Locking the screen in the workstation before leaving the desk, even if it is for some minutes.
- Avoiding the distribution of personal information in public fora such as social network sites.
- More in general, understanding the risks taken beforehand.

7.9 An IT Security Viral Marketing Example: Identifying Socially Connected Colleagues

This example of a security awareness campaign is based on viral marketing techniques.

The IT security team need laptop users to understand and follow a basic "security story": Corporate information needs to be kept confidential at any time, including when users work with their laptops on the road, like in an airport lounge or while they commute. Consequently, the security team propose the use of privacy filters on laptop screens to prevent third parties from shoulder surfing and accessing corporate information. There are different ways to promote these filters:

Placing a catching poster that invites to obtain a screen filter from the storage room is a conventional security awareness measure that the team can put into practice, but its effectiveness is limited. Alternatively, the team can make use of viral marketing to extend the use of privacy filters among their customers following these steps:

- The security team identify the most frequent laptop users in the organisation.[44]
- For those users with older laptops, the security team maybe can offer them to swap their machines for new lighter ones with more memory.
- The security team install those privacy filters in the new laptops provided to the users.

[43] More about viral marketing in wikipedia. Available at http://en.wikipedia.org/wiki/Viral_marketing. Last accessed 20-11-2009.

[44] A possible way to obtain this information could be checking the logs of the remote access infrastructure: Who access it most frequently?

– The security team provide users with those new laptops, together with a 5-min briefing session where their "security communicators"[45] explain them the threat posed by shoulder surfing and the protection[46] screen filters offer.
– Several days after, security team members phone those users with new laptops with a privacy filter installed and ask them for their initial feedback and whether they will continue using it.
– If their feedback is positive, the security team member asks the users to provide a name of another laptop user that could benefit from the use of a privacy filter.
– If their feedback is negative, the security team go back to square one and devise a new measure that could both satisfy user and security requirements.

An additional aspect to consider is the "social connectivity" of the laptop users that the security team have contacted. Seth Godin[47] calls socially connected people that spread ideas "sneezers" and Malcolm Gladwell uses the term "connectors"[48]. Whatever the name, the IT security team need to identify and target those individuals with dense social networks. Consciously or unknowingly, they need to be carriers of the "security story telling activity".

Using a marketing term, we suggest creating a "spiral of prosperity"[49] for those "security connectors" by answering their security needs while the security team perform their IT security mandate.[50] "Security connectors" are a key to secure the entire organisation.

7.10 The Role of the Incident Response Team in Guerrilla Marketing

Guerrilla marketing[51] relies on innovative, or at least unconventional, promotions based on a burst of time, energy and imagination. IT security incident response teams[52] share three non-content related features with guerrilla marketing teams:

– They are normally of small size.
– They invest time, energy and imagination to live up to their mandate.
– They base their actions on experience, judgement and some portions of guesswork.[53]

---

[45] See Section 2.3.

[46] Privacy filters also benefit users' sight. Although not security related, team members can also use this argument.

[47] American author of business and marketing books.

[48] Gladwell (2000), pp. 38–46.

[49] Win-win deals that increase in value between the provider and the customer (Bird 2000, p. 30).

[50] See Section 1.19.

[51] Term coined by Jay Conrad Levinson (1984) according to http://en.wikipedia.org/wiki/Guerrilla_marketing. Last accessed 20-09-2009.

[52] See the *red team* in Section 4.10.

[53] Guerrilla marketing teams revolve more on human psychology than current incident response teams do.

We encourage security incident response teams to become a guerrilla marketing team when the incident or the response brings along interaction with customers. To succeed in this endeavour, we provide in the next sections of this chapter two complementary work elements:

– A collection of basic messages, i.e. the "security stories" with which an IT security team need to infect the organisation.
– Tips on human psychology that IT security teams should consider for their viral and guerrilla marketing campaigns.

Security Stories to Sell and Human Psychology Aspects

Security teams need powerful stories to sell their security services to their customers. The remaining sections of this chapter present some of those stories and introduce some hints on how human beings make decisions and react to their environment.

7.11 The Security Stories

Messages have to be sticky, memorable and they have to move to action.[54] This is the way security can succeed by "word-of mouth".

7.11.1 Stories for End Users

There is a current threatening shift towards client-based[55] attacks in the Internet. This is the reason why security teams need to focus their attention, even more than they did in the past, to user behaviour in Internet. They have to sell the "security story" so that users incorporate recommended IT security practices into their daily activities.

The central story to share with end users is difficult to transmit. Client-based technology, not only operating systems, but also basic tools such as browsers, word processors, presentation assistants or spreadsheets are becoming increasingly complex.[56]

All this client software poses new threat vectors, not only to home users connected via broadband to the Internet, but also to organisations. Security teams are obliged

[54] According to Gladwell (2000), pp. 25 and 139.

[55] Cyber-attacks that target software installed on users' workstations. See SANS (2009b). Last accessed 29-09-2009.

[56] See Section 10.5.

to include technical tips in their stories, which are useful both at work and at home, to attract their attention.

Curiosity in users will always be more attractive than following any IT security recommendation, e.g. "they would double-click on a little nice and enticing icon appearing on their desktop before reading a security note that they should just delete it". To mitigate this fact, security teams need to show users, in practice, the damage that a simple additional double-click can provoke to their workstations, and subsequently, to the entire organisation, before they have the chance to do it.

As already stressed in Section 7.6, security messages should not be threatening but didactic and fact-based. An alliance with the organisation's physical security colleagues could be a viable option to increase the IT security team's credibility.

7.11.2 How to Approach the Elaboration of Security Policies

We suggest elaborating one-page long security policies for each of the topics affecting the organisation. Once a team member proposes a first draft, we suggest engaging non-IT colleagues working inside or outside the team to peer review the one-page policy with a twofold objective:

- To confirm that the policy is understandable and, above all, that it can be followed.
- To check that every policy is consistent with the other policies delivered in the past.

The skeleton of user-related security policy should be lightweight. We propose to start off with the following elements:

- Purpose of the policy, e.g. "*This policy deals with the need to avoid the installation of additional software in workstations*".
- Reason of its existence, e.g. "*The organisation patches and updates all pieces of software installed in all workstations. This way, the IT department provide users with updated functionality and reduces a threat vector. Additional software installed in workstations poses new risks to the workstation and hence to the information stored or flowing through the organisation's networks. This new software is not automatically patched nor updated.*"
- Point of contact for possible alternatives or further information, e.g. "*For additional information or to request any new software, please contact the IT security team hotline. They will answer your questions and channel the request to install new software in corporate workstations*."
- Author and reviewer of the policy, e.g. "the *yellow team*[57] in the IT security team".

Apart from following a simple template for user policies, the security team should not surprise users with a sudden change in a security policy that could hamper their routine or affect their daily working experience. Otherwise the team run the risk to be flooded with questions and complaints from users.

[57] See Section 4.10.

7.11.3 Stories for Managers

Management in the organisation need to understand and appreciate the actions of the security team.[58] We identify two marketing deliveries that could convey the "security stories" for managers:

– Security-related figures provided in the form of key performance indicators. They can be part of their management dashboard. Those indicators, smartly presented, could show the evolution of IT security in the organisation, e.g. average number of passwords per user, number of security incidents handled, number of security policies breached, number of vulnerabilities found in servers, etc.

Visual aids such as traffic lights, statistical pies, level gauges, etc. are useful tools to present data to managers.

– A regular and brief delivery of a list of IT security improvements performed by the team, highlighting the three top ones. The list could answer the question of what the IT security team have done in the last, for example, 4 weeks, that benefits the organisation and hence management. The authors of the list should always avoid the use of IT jargon.

7.11.4 Stories for Other IT Teams

The main story to sell for the colleagues working in other IT-related teams is the simple message that IT security is there to provide them with IT security expertise[59] but not to conquer their "plaza". We propose the creation of work groups consisting of IT professionals from different teams to achieve a "smart" objective.[60]

7.12 Behavioural Economics to Consider When Marketing IT Security

7.12.1 Decisions, Cheating and Ethics

Human beings do not always follow logical paths when they decide and when they act. Their environment, their beliefs and their expectations, and hopefully their rational mind, influence their perceptions and their acts in a mixed manner.[61]

[58] See Chapter 8.

[59] See Section 7.2.

[60] See Section 5.2.

[61] Punset (2007), pp. 40–47.

Human beings see things within a context and try to go for the middle range choice[62] and, given the opportunity, even very honest people will cheat, however only what they consider "to cheat a little bit", even if it is evident that they will not get caught.[63] It has been attested that remembering an ethical oath has a positive influence on us if it is just before we are faced with the opportunity to be dishonest.[64]

We suggest having those psychology observations in mind when we design IT security marketing campaigns:

- "Security communicators" should place the security policies next to their users' working places. If users can read the "ten principles of a secure Internet browsing" while they are using the Internet, then the security team will have a higher chance that they will follow those recommendations.
- The security team could also identify those users that will not follow any security policy at all and apply additional preventive and detective measures on them.[65] They will only be a minority of users. The majority will deviate from a secure behaviour, but, probably, only a little bit (Image 7.4).

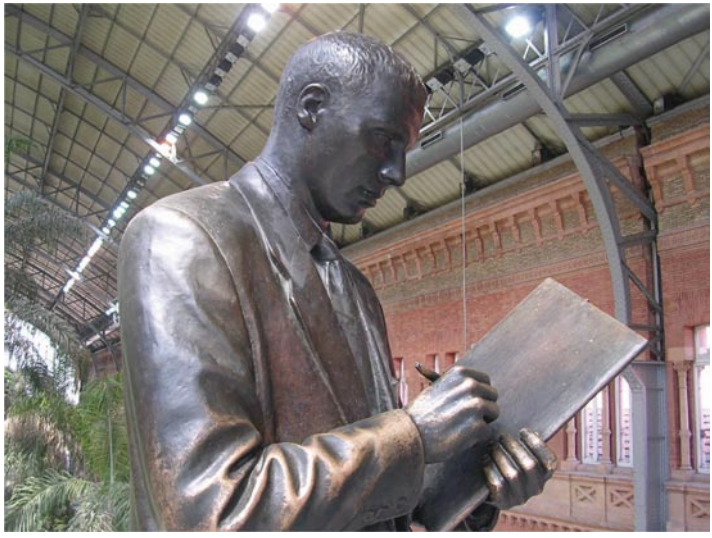

Image 7.4 Security should take note of how human beings tick

[62] Ariely (2008), p. 4.

[63] Ariely (2008), "The context of our character", Chapters 11 and 12.

[64] Ariely (2008), p. 212.

[65] Always following the personal data protection legislation that applies to the organisation. We recommend to seek legal advice beforehand.

7.12.2 Subjective Expectations About Money and Prices

The relationship that human beings have with money and with prices is very specific[66]:

- We feel very attracted by the notion of something being free.
- An expensive price makes us think and feel that what we buy is better.[67]
- We feel happy when we do things voluntarily but, however, not so much when we are paid to do them.
- We are loss averse, i.e. we are more sensitive to losses than to gains.[68]

We apply these learning points to the IT security marketing mission and we come up with the following ideas:

- Security teams could provide free security gadgets to their users, e.g. they will welcome a free encryption-enabled USB memory stick even if it is more cumbersome to use than current ones.
- Security teams could communicate the cost of the security incidents they handle and even the cost of having an IT security team. Those figures will provide everyone in the organisation with a feeling of how expensive "lack of security" and "security services" can be.
- Security teams need to consider human beings' higher sensitivity to losses when they elaborate risk assessments.
- The observation about voluntary work justifies the proposal to gather passionate professionals for the IT security team.[69]

In Chapter 7 we have explained why IT security teams should communicate with their stakeholders and perform a continuous marketing campaign to sell their services to their customers. We have articulated possible selling strategies and we have suggested the basic content guidelines and how we can anchor these guidelines in characteristics of human psychology.

Chapter 7: Learning points

This chapter answers the following questions:

- If security teams communicate, they have a greater chance to succeed.
- Different IT security stakeholders need to receive different messages.
- Security teams need to explain and to show, not to scare.
- Everyone in the organisation is responsible for security.
- Services are intangible. Security deliverables are mostly services.

[66] Ariely (2008), Chapter 2, "The fallacy of supply and demand", and Chapter 3, "The cost of zero cost".

[67] This happens for example with medicines.

[68] Kahneman and Tversky (2000), p. 301.

[69] See Section 2.7.

- Security teams need to market their services as any service provider.
- They will customise the "marketing mix" to the security requirements.
- Their message should be clear, consistent, credible and competitive.
- Viral marketing techniques help raising security awareness.
- IT security campaigns require the aid of "social connectors".
- "Security connectors" will spread the security messages.
- The incident response team could perform guerrilla marketing.
- Users, managers and IT teams need to receive "security stories".
- IT "securiteers" need to understand the way human cheat and deal with money.

Link to MBA Management Models

We have selected three MBA-related models or concepts that could help communicators to market security services in the organisation:

Customer bonding: The seven key stages *(by Jill Griffin, 1995 and 2002)*
The author outlines a process to create loyal customers. Customers need to go through different stages until they become advocates of the offered services:

- Suspects.
- Qualified prospects.
- First-time buyers.
- Repeat customers.
- Loyal clients.
- Advocates.
- Finally, even partners.

Marketing promotion instruments *(by Lee and Hattemer, 2006)*
How can teams disseminate information about their services to potential customers? These two Marketing lecturers at Henley Management College MBA mentioned:

- Advertising: Non-personal presentation by an identified sponsor.
- Sales promotion: Short-term incentives to encourage trial/purchase.
- Public relations: To protect or promote the company's image.
- Personal selling: Personal presentation.
- Direct marketing: Direct communication with individuals to obtain an immediate response.

From marketing lectures prepared by Stephen Lee and Robert Hattemer (Henley Management College MBA, 2006).

Customer lifetime value *(by McCorkell, 1997)*
Concept that focuses on the value a customer creates during their entire relationship with the service or product provider and not just on a punctual interaction. This idea is useful for IT security customers. The suggestion is to use the concept of the "security lifetime value" for customers.
See references: Griffin (1995) and McCorkell (1997)

Chapter 8
Management Support: An Indispensable Ingredient

Chapter 8: What will the reader learn?

This chapter answers the following questions:

- Who are decisive stakeholders for the IT security team?
- Which dichotomy should IT security leaders save to managers?
- How do current risk-related references see the role of managers?
- Which risk sources and risk types affect the organisation?
- What is operational risk?
- What is enterprise risk management (ERM)?
- How can IT security link with ERM?
- Which risk management strategy should we follow?
- How can the risk house model help managing risks?
- How could IT "securiteers" and managers work in harmony?

Management support is a pre-requisite for any IT security team to survive, evolve and provide value to the organisation. This chapter explains why IT security teams need line, but most importantly, senior management sponsorship, understanding and backing. We link IT security with the concept of ***information security*** and ***operational risk management*** and we introduce an overarching management initiative in the organisation, ***enterprise risk management*** (ERM). We proceed to locate the role of IT security within operational risk management and ERM through a management model presented in this chapter: The "***risk house***" model.

Every manager and risk management professional could use the "***risk house***" model to understand the variety of risks that are present in business processes and the corresponding risk management frameworks running concurrently across the organisation. The end of this chapter connects with the business-related aspects we mentioned in Chapter 1.

A. Partida and D. Andina, *IT Security Management: IT Securiteers - Setting up an IT Security Function*, Lecture Notes in Electrical Engineering 61,
DOI 10.1007/978-90-481-8882-6_8, © Springer Science+Business Media B.V. 2010

Executives in Organisations Need to Manage Risks of Different Nature

8.1 Managers: Decisive Stakeholders of the IT Security Team

Top senior management and line managers are key stakeholders of the IT security team.[1] Top executives have a higher degree of power on our team than line managers but the team require both stakeholder groups to show high interest in IT security activities.

The task of the security team leaders is to enable business processes and avoid that managers find themselves in an "unpleasant crossroad" situation, i.e. when they are left alone with the decision to "run the shop" or to "support security". Most managers have more urgent objectives than security. They will opt to let the shop run rather than stopping a project because it might be insecure. Business reality will compel most managers to start a new endeavour, even if it brings risks to the organisation. IT security team leaders would have failed if managers often experience that dichotomy.

Making business means taking risks.[2] The ultimate objective of this chapter is to equip management and IT security teams with a tool that includes the information security and the IT security dimensions on the organisation's agenda.

We base the content of this chapter on two simple but powerful premises:

Management, especially top executives, hold the leadership role required to achieve the organisation's mission.

Consequently, we will identify top senior managers with the real leaders[3] of the organisation. Throughout this chapter we will refer to them as *executives*.

A mindful management layer is a necessary but not sufficient condition for an IT security team to accomplish their mandate.[4]

In a survey performed in 2006 among 82 IT security and risk management professionals,[5] 42% of them agreed with the statement that "management is committed with information security". If we link this figure with this premise we conclude that still a majority percentage of IT security teams do not enjoy management support yet. This adversity creates enormous difficulties for IT security teams to perform their mandate.[6]

---

[1] See Sections 5.9 and 7.2.

[2] See Section 1.12.

[3] "Leaders in today's corporate world need to orchestrate complexity and chaos so that production outweighs destruction". Heifetz, R., Grashow A. and Linsky M. (2009), "Leadership in a permanent crisis", *Harvard Business Review*, July/August.

[4] See Section 1.19.

[5] From the five continents on Earth. Survey details and results available at http://securityandrisk.blogspot.com/2006/12/welcome.html. Last accessed 30-09-2009.

[6] See Section 1.19.

8.2 Risk Management Could Become a Management Innovation

A management innovation can produce greater improvement in any industry compared to any technology and product innovation.[7] IT security leaders need to prepare the field so that the organisation can achieve four cases of management innovation. Executives play a crucial role in all four:

- Being aware of the IT security risks faced by the organisation.
- Leading the process that would connect the different risk management practices in the organisation under the enterprise risk management umbrella.
- Making enterprise risk management a component of corporate governance.[8]
- "Smart risk seizure": Blending the idea that every business brings, intrinsically, some risks,[9] with the new idea that a risk can potentially score as an opportunity for the business. If the organisation takes some meditated risks, maybe it seizes new business opportunities.

Generally speaking, management sponsorship is an indispensable requirement to implement any organisation-wide process. Certainly, the adoption by an organisation of a risk management framework requires management support and leadership. Their intervention is key before, during and after the implementation. Table 8.1

Table 8.1 Management roles before, during and after the implementation of risk management in the organisation

When in the implementation process	Management role	Suggested by
Before the start	A major responsibility of management, vital to the success of the organisation, is the management of assets and its risks.	ISO (2004), pp. 1–24 ISO (2005), pp. 1–115.
	Management will determine how much uncertainty the entity is prepared to accept as it strives to grow stakeholder value (risk appetite).	COSO (2004), pp. 1–103
	Shareholders demand management reducing risks.	Birchall et al. (2003), pp. 1–51
	Solve the major governance challenge: Lack of clarity about responsibilities.	Appel (2005), pp. 1–8

(continued)

[7] Hamel (2006), pp. 1–12.

[8] As an example, other corporate governance processes are performance and quality management.

[9] As we already introduced in Section 1.12 and re-visited in Section 8.1.

Table 8.1 (continued)

When in the implementation process	Management role	Suggested by
During the implementation	Information security should be subject to board-level leadership.	Birchall et al. (2003), pp. 1–51 DeLotto et al. (2003), pp. 1–4 McFadzean et al. (2003), pp. 1–25
	If management do not understand risks, then their perception is not accurate (e.g. unsupported security initiatives) and risks are not properly managed.	Coles and Moulton (2003), pp. 487–492 Aabo et al. (2004), pp. 1–34 Scholtz (2004), pp. 1–4
Afterwards	Levels of compliance must be reported to executive management.	von Solms (2005), pp. 443–447 Bolton and Berkey (2005), pp. 237–246
	Risk reports must reach board agendas. They should shift from a technical discussion to a risk management comprehension understandable by management.	May (2002), pp. 10–13 Carey (2005), pp. 1–28 Sheffi and Rice (2005), pp. 45–47

reflects how current risk management literature contemplates the role managers need to play when overseeing risks threatening the organisation:

8.3 Risk Sources and Risk Types Affecting the Organisation

The risks that can affect the organisation come from a variety of sources. A risk materialises when a given threat makes use of a vulnerability and produces an undesired effect.[10] There are four areas in which organisations can be exposed to risk (Image 8.1)[11]:

- Human factors.
- Technology.
- Environment.
- Business processes.

[10] See definition of vulnerability, threat and risk in Section 1.1.

[11] Birchall et al. (2004), pp. 1–73.

Image 8.1 People and technology: two sources of risk

Executives in organisations need to adopt a risk management strategy. This strategy normally consists of a mix of the following ingredients[12]:

- Avoidance: Closing the activity that creates the risk.
- Reduction: Applying active risk mitigating measures.
- Share/insure: Conveying the risk to someone else.
- Accept: Knowledgeable risk acceptance.[13]

The quantity of these ingredients will depend on:

- The environment surrounding the industry and the organisation (Porter's 5 forces,[14] legal framework and industry trends).
- The strategy set by the executives (the risk appetite[15]).
- The culture of the organisation.
- The resources available to the organisation.

The four generic types of risks,[16] to which organisations are exposed, constitute an alternative to the four risk exposure areas we have previously mentioned.

- Hazard risks: Risks coming from the physical environment.
- Financial risks: Credit, inflation, market prices.

[12] COSO (2004), pp. 1–103.

[13] Preferably after a careful cost/benefit analysis.

[14] See Porter's 5 forces MBA model at the end of Chapter 4.

[15] See Section 1.13.

[16] See ERMC (2003), p. 10.

– Operational risks: Risks coming from the functioning of the organisation.[17]
– Strategic risks: Coming from business, social, political, economical, technological, and legal factors.[18]

Although this reference proposes a different division of risk types, risks mentioned in all of them are closely related. A special type of strategic risks are reputational risks: The "good standing" of the organisation can be negatively affected by the occurrence of any type of risk. A reputational risk is, therefore, a potential negative consequence of the materialisation of any risk event of any nature. An easy example of a reputational risk is the risk that a retailer bank runs when their online website is compromised: Some of their customers will definitely be negatively affected but also, if the incident is published, the bank's brand will suffer from the occurrence of this event.

Two Risk Containers: Operational and Enterprise Risk Management

8.4 Operational Risk

The financial world, more specifically the Basel Committee, defines operational risk as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events".[19] These are the risks that are inherent to the concept of making business.[20] We can apply this definition of operational risk to any industry. Risks posed by information technology (IT) based systems, including IT security risks, are, consequently, a subset of operational risks.

Executives in organisations manage business processes and hence, also operational risks arising from those processes, people, systems and from external events.

The IT security team need to accept the fact that they are only a "humble" piece within the operational risk puzzle. IT security is an increasingly relevant element but certainly not the only priority executives will consider.

IT security leaders need to design an IT security strategy with simple but strong links with the way executives manage operational risk through the organisation. In practice, this means that IT security professionals should understand:

– How risks coming from people, internal business processes, systems[21] and external events can affect the organisation.
– How executives have decided to deal with those risks.

And they should put into action:

---

[17] See Section 8.4.

[18] See PESTLIED MBA model at the end of Chapter 1.

[19] Basel (2003), pp. 2–5 and 8.

[20] See Section 1.12.

[21] Not only IT systems.

– A whole set of activities to mitigate the most relevant risks.[22]
– A plan to make IT risk management, i.e. IT security, consistent with operational risk management.

We propose that the IT security team analyse how operational risk management is positioned in the organisation[23] and afterwards align themselves to it. Simultaneously, executives managing operational risk should be able to manage all types of operational risk in a consistent manner. Regarding IT risks, the knowledge of the IT security team will be the tool that executives have to take risk-aware decisions, and, eventually, to reduce IT complexity.

8.5 Enterprise Risk Management: A New Dimension of Risk as an Opportunity

The first two sections of this chapter have presented the central role that executives need to play to manage risks while they run the business and, consequently, to ratify IT security actions and messages in the organisation. Sections 3 and 4 in this Chapter have introduced the sources of risk and the concept of operational risk.

This section introduces the concept of enterprise risk management (ERM), a risk management umbrella, an overarching framework, that deals with all types of risk threatening the organisation.[24] Enterprise risk management practitioners have the objectives of the organisation in mind and orientate all risk management practices towards the achievement of those objectives. There is a second dimension included in ERM that is far less known but highly promising. It refers to seizing opportunities[25] to accomplish the organisation goals and not only to the traditional aspect of managing risks globally. This way, ERM does not always constraint possible paths of action within the organisation, but it is also a tool for executives to find attractive and unexplored sources of business: ERM adopts the "smart risk seizure" concept. A distinctive ERM approach can become a competitive advantage for an organisation.

If we transfer this concept into the IT security field, we recommend that the IT security team apply this new paradigm of "smart risk taking" to their strategy. Those teams which will master this application will make executives more receptive to risk mitigating measures, since a smart IT security capability can also become a competitive advantage for the organisation.[26] This is the ultimate step to achieve management sponsorship. Executives will support and back IT security initiatives that help them taking "those known and meditated risks" they have decided to run.

---

[22] From the IT security viewpoint.

[23] For example, using the 4 C's model to position a brand mentioned in Section 7.7.

[24] According to CAS (2003), p. 8, "ERM is the discipline by which an organization in any industry assesses, controls, exploits, finances, and monitors risks from all sources for the purpose of increasing the organization's short- and long-term value to its stakeholders."

[25] See CAS (2003), p. 6.

[26] Such as product security testing.

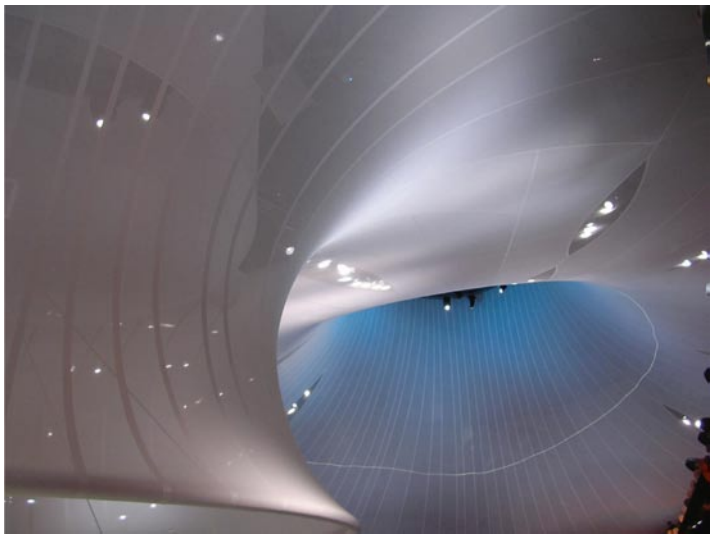

Image 8.2 IT security guide executives through the risk labyrinth

We have presented in this section what to do to obtain management's attention by transforming risks into opportunities, carefully explaining the risks and possible mitigating measures. However, how to materialise this proposal is a complex task. This book deals with this challenge through the creation, organisation, planning and marketing of an IT security team (Image 8.2).

The measures proposed in this book to manage IT security revolve around the idea that the expertise that IT security teams provide to executives to help them managing risks is precisely an opportunity to keep and increase the assets of the organisation, including its reputation.

A Model to Understand Risks and a Decalogue to Work with Managers

8.6 The "Risk House" Model: How Executives Can Treat Risks

The mandate of management is to lead and manage the organisation. They are the ultimate layer responsible for the achievement of the business objectives. In the previous sections we have justified why risk management is one of their tasks and responsibilities. We have also shown how complex is the management of such a broad variety of risks. In this section we propose a ***management model***, the "***risk house***" model, to facilitate the understanding of risk management within any organisation.

The "***risk house***" model connects all sources of risks and elements present in enterprise risk management. It is a conceptual tool that explains what risk means for the organisation.

The core of the model is the business idea. Making business means taking risks.[27] Those risks are present in the business processes. They can lead to a loss or to an opportunity depending on how they are managed and, especially, mitigated. Consequently, we combine in the core of the house the concepts of business and risk.

Before addressing any risk management idea, we add two elements to the house. Every organisation has certain objectives. In order to achieve them, management will follow a specific strategy. We reflect graphically these two ideas in the model with an "objectives bubble" that crowns the house and a guiding element, a triangle, as the strategy followed to reach the objectives.

The remaining building blocks of the model are related to risk. We represent all possible risk sources that can affect the business with the "risk flash of lighting": People, technology, environment and business processes.

The frame of the house consists of two complementary elements:

8.6.1 The Risk Management Block

An upper piece surrounding the business core with four risk management practices that deal with four generic types of risk[28] affecting the business: Strategic, financial, hazard and operational.[29] This block also entails:

- Reputation is a value that all risk management practices are mandated to protect.
- Enterprise risk management orchestrates the link among different risk practices.

We have depicted reputation on the top of the risk management block as a very special component and we have labelled the entire block with the function name "enterprise risk management".

8.6.2 The Information Block

A lower complementary piece of the frame represents information. The business itself and all risk management practices require information to function. It is a continuous block with no specific compartments. With that, we refer to the role that the information plays within the organisation as a connector of risk management practices. All practices need to share a common overarching risk language and certainly that requires sharing information. Given the criticality that the information has for the business, it is evident that the information security function needs to protect it.

---

[27] As we already introduced in Section 1.12 and re-visited in Section 8.1.

[28] These risks come from one of the risk sources mentioned above: people, technology, environment and business processes.

[29] See Section 8.3.

Once the role that information plays within the business is clear, we can connect this model with the subject of this book, IT security. Nowadays information resides in information technology based systems. The ultimate objective for IT security is to reasonably protect the confidentiality, integrity and availability of the information hosted in IT systems.

The following elements to add to the model are:

- Corporate governance is a solid component mandated to provide control and compliance in order to safeguard the present and the future of the business. It looks after the business strategy and the way risks are managed. We represent it with a "dome" that protects the "business strategy" triangle.
- Management commitment: A cohesive ingredient, the cement that glues together the business strategy with risk management. An indispensable element to keep the house up.

We complete the model with a dynamic mechanism that depicts the concept of appetite for risk.[30] Management will decide the exposure to risks that they are willing to accept for the organisation. The aperture existing between the risk management and the information blocks, through which risks threaten the organisation, represents the organisation's appetite for risk.

This model contributes to manage the complexity that risks bring to executives, stresses the importance of their commitment and locates the role that IT security plays in the overall risk management arena.

The "***risk house***" model can also be used as a visual information tool:

- The state of each of the elements of the house can indicate the progress made by the organisation in each of the risk management practices and related functions in the organisation.
- The relative size of each of the elements can indicate the need to allocate resources to the activities included in the model (Fig. 8.1).

8.7 The Ten Commandments to Transform Executives into Our Best Allies

From the executives' perspective, it is easy to explain the modest role that IT security plays in the organisation. Using the "***risk house***" model, executives could say that "the IT security team is not in charge of information security, they just take care that the IT systems in the organisation are well protected, that the information block relaying on IT systems is kept confidential, integer and available".

At the same time, it is also straightforward to explain the decisive role IT security plays in the organisation from the IT security team's view. Most, if not all, information

[30] See Section 1.13.

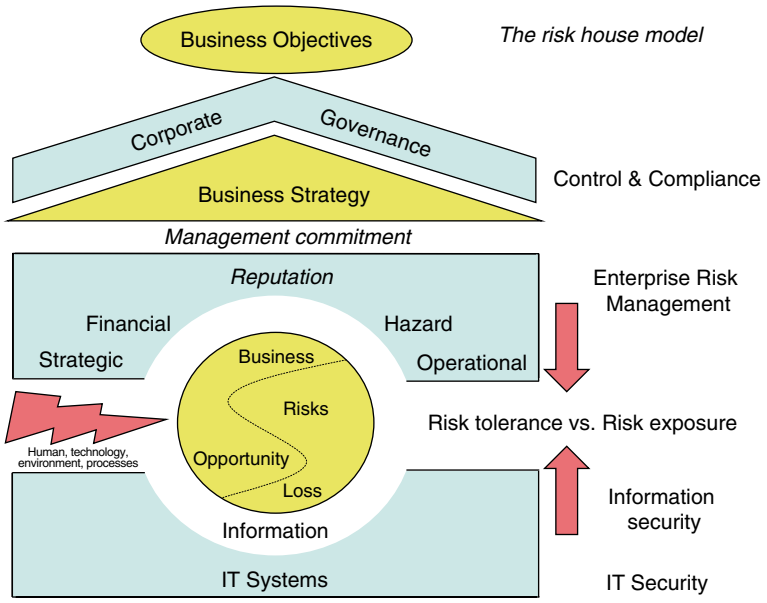

Fig. 8.1 The "risk house" model

is currently hosted in IT systems. IT security is mandated to articulate the protection of those systems. The IT security team would say: "Without IT security, the information block in the house is not stable and the house could fall down".

Those views are two sides of the same reality. Our proposal is that the IT security team should not devote energy to refute management statements, but focus on delivering value to the business and to the executives on what they best know how to do: IT security.

Although Chapter 7 has already provided a handful of suggestions to sell IT security, also to executives, we finalise this chapter with a compilation of ten recommendations, five for IT security professionals and five for management, to make out of the organisation's executives the loyal sponsors of the IT security team, and possibly, their best allies:

1. IT security will deliver risk-assessed scenarios to management with a proposed and feasible way forward.
2. IT security will let management decide on how to proceed once IT security brief them on the real risks that they and the organisation run. Those briefings will use business and not IT language and they will contain information and real demos on IT security incidents happening in the world.[31]

[31] See Section 1.15.

3. IT security will record the risk information provided to management and the decision taken by management.
4. IT security will seek and gather information, even in an informal manner, about the plans and the strategy that managers have for the organisation.
5. IT security will strive to action management's plans and strategy in a reasonably secure way and to report progress to them.
6. Management will provide the IT security team with the required human resources, budget and organisational independence to perform their IT security mandate.
7. Management will provide fact-based input on the risk they are willing to accept.[32]
8. Management will communicate with IT security, even if very briefly, on a regular basis.
9. Management will use IT security achievements as an element for their marketing strategy within the organisation and with their customers.
10. Should most of these recommendations not be followed by any party, we recommend looking for a new IT security team or for a new organisation with a different management,[33] depending on which party is not respecting these commandments.

We suggest the following exercise for IT security professionals: Assessing how many of these points are present in their current working engagements, either within their organisations or in the different customers.

The goal of every IT security expert should be to practice the first five points and to look for working environments where, at least, two out of commandments from 6 to 9 are reality. Finally, IT security professionals should always have point number ten in mind and act accordingly.

Chapter 8: Learning points

- Executives and line managers are decisive stakeholders for IT security.
- IT security leaders should not "corner" managers.
- Current risk-related references coincide on the key role of managers.
- People, technology, environment and business processes are risk sources.
- Hazard, financial, operational and strategic are types of risks.
- Operational risk is inherent to making business.
- Enterprise risk management presents risks also as opportunities.
- IT security teams need to apply the "smart risk taking" approach.
- IT security professionals should inform factually about risks taken.
- The risk house model helps managing risk complexity.
- IT "securiteers" and managers can work in harmony with mutual respect.

[32] See Section 1.13.

[33] Entrepreneurial IT security professionals could be their own manager.

Link to MBA Management Models

We have selected a popular MBA-related model and another one that is not so well-known. Both could facilitate executives and IT security professionals the understanding of the organisation's business processes:

Value Chain *(by Michael E. Porter, 1985)*
The model shows how activities in an organisation add value offered to customers through products and services. There are two main types of activities:

- Primary activities: Inbound logistics, operations, outbound logistics, marketing and sales and service
- Support activities: Firm infrastructure, HR management, technology management and procurement

To these activities, successful organisations add a profit margin to their deliveries.

Strategic triangle *(by K. Ohmae, 1982)*
There are three elements in the development of any business strategy:

- Customers: To whom the business provides value
- Corporation: All its units and its processes have a cost
- Competitors: Any competing stakeholder

The strategist aims to provide value to customers while controlling the cost of this value provision and performing better than competitors.

See reference: Harding and Long (1998).

Chapter 9
Social Networking for IT Security Professionals

Chapter 9: What will the reader learn?

This chapter answers the following questions:

- Why do IT security professionals need to network?
- What is the "spiral of new value" in networking?
- Who are the networking targets of the IT security team?
- Where can the IT security team practise networking?
- How can they proceed with networking?
- What is the IT security community like?
- Which are some examples of IT security fora?
- How can IT security professionals network with academia?
- How can they network with physical security colleagues and law enforcement agencies?
- How can they network in their local community?
- How can networking increase the value of the IT security professional?
- How can they build their IT security reputation?
- What could be done to build a personal IT security brand?

Once we have introduced the concepts of risk, threat and vulnerability (Chapter 1) and described the profiles that an IT security team requires (Chapter 2), together with a proposal on how a real IT security team could function (Chapter 3), we have presented our ideas on what an IT security team should do (Chapter 4) and how they could do it (Chapter 5). Subsequently, we have gone deeper into team dynamics (Chapter 6) and into possible paths to market IT security (Chapter 7), paying special attention to the need to achieve management support (Chapter 8).

A. Partida and D. Andina, *IT Security Management: IT Securiteers - Setting up an IT Security Function*, Lecture Notes in Electrical Engineering 61,
DOI 10.1007/978-90-481-8882-6_9, © Springer Science+Business Media B.V. 2010

In Chapter 9, we will delve into an increasingly relevant element to consider for an IT security team member: Networking inside and outside organisations to create value for both, the customer and the IT security professional.

Human Beings Are Social Beings

9.1 Reasons for Networking in IT Security

Human beings build relationships with each other. The strength of those links varies a lot depending on the environment and the purpose of the interaction. Similarly to the way an IT network joins two or more nodes, a social network is composed of a set of persons, the nodes, that share a ***specific purpose*** and ***exchange information*** about it.

Our stance for IT security professionals is that they need to be connected to a handful of social networks. Some of those networks will be related to IT and IT security, some others will be social networks that could benefit from IT security expertise.

There are three reasons that justify our suggestion to be connected:

9.1.1 Quicker Way to Learn New Tendencies

IT, and specifically IT security, is a subject that is in constant evolution.[1] IT security professionals have to keep abreast of the latest security incidents, tools and tendencies if they wish to maintain their value in the market. Professionals get to know about those resources much earlier if they are in direct contact with other professionals, if they are an active part on an IT security related network.

9.1.2 Easier Way to Understand Society

More generally, the industries in which IT security teams work also change. IT security professionals need to grasp where the industry, and the society in which they work, are heading for. Exchanging some words with an informed business colleague would provide very useful hints and facilitate a future provision of IT security services, adapted to the changing society.

9.1.3 Open Door for Future Professional Changes

More than half of the open job positions are filled without being advertised.[2] IT security professionals who are part of a relevant social network have a greater

[1] See Sections 2.6 and 6.9.

[2] McClure (2003), p. 154.

chance to work on their ideal position, be it as an employee in an organisation, as an independent consultant or as the owner and driver of a small security company.

9.2 Social Networking Foundations for IT Security: The "Spiral of New Value"

9.2.1 When Professionals Share Information, They Create Value

In IT security there is much information to share, such as new threats, new tools, new methods, new products, etc. Social networking is a two-way communication exercise. In an information sharing process, there is normally an active player who shares some new knowledge and sets a communication baseline with a receiver.

The receiver benefits from knowing something they did not know. Additionally, the beauty of sharing information is that the first active player, the transmitter, also benefits from the action of sharing, since the receiver usually provides a new viewpoint or a novel element, unknown by the first player.

This way, professionals in a network create a "***spiral of new value***" by sharing information and by building new constructs on top of those pieces of information. This "spiral" reinforces our suggestion for IT security professionals to "stay connected" within their IT security networks.

9.2.2 Networking Requires Time

Most professionals enjoy networking: They look after their contacts, exchange information, and, if possible, a laugh too. The main drawback of networking in our current society is that it requires a considerable amount of time. A terribly busy work schedule, family duties and other social commitments usually prevent IT security professionals from entering into this "spiral of new value".

This chapter highlights practical ways for professionals to obtain the most of their networks by making a smart use of the limited time they have to socialise.

9.2.3 The Significance of People and Not Organisational Charts

The rapport that an IT security professional will establish with individuals working close to them can be the differentiating factor between succeeding or failing in an IT security activity.

The networking approach we propose relies on regular, personal, preferably face to face, contacts. It is difficult to achieve rapport through a written memorandum,

a formal meeting or a hierarchical relationship. We refer to the creation of a person to person link based on respect and, as time goes by, also on mutual trust.

In the long run, the location in the organisational chart of the person contacted by the IT security professional is of no crucial relevance. The importance of the link resides on whether both individuals:

- Are able to speak a language that makes them understand each other.
- Share some basic values and a certain way of doing things.
- Consider that information sharing will benefit both of them.

Colleagues working in support positions, such as assistants, secretaries and operators, play an essential role in the organisation. IT security team members should develop a good rapport with them. For example, it is frequent to see how assistants can play a key role in viral marketing-based security awareness campaigns[3] especially if these two conditions exist:

- They are "social connectors".[4]
- They are approached by security members with sufficient interest and appreciation for their work.

9.2.4 A Smile Can Take IT Security Far Far Away

Scientists have cleared up that emotions matter to define and steer the ecosystem surrounding human beings. Relationships constitute an essential element of the environment.[5] The emotions that are present in our interaction between people influence the way the relationship will develop in the future.

Working in IT security sometimes entails the interaction with counterparts who go through moments of nervousness and agitation, such as parties involved in a serious security incident.[6] It can also imply to persuade a decision-maker to modify a course of action, for example, recommending measures to address findings collected in a security assessment before a go-live activity.

Emotions, both at the receiving and sending end, play a relevant role. If the communication is loaded with an authoritarian tone and a feeling of distrust, the outcome of the interaction can easily transform into a lose-lose situation.

---

[3] See Sections 7.8 and 7.9.

[4] See Section 7.9 and Gladwell (2000), pp. 38–46.

[5] Parkinson et al. (2008), p. 1. See list of publications from Brian Parkinson at his Oxford University web site, available at http://psyweb.psy.ox.ac.uk/social_psych/. Last accessed 15-10-2009.

[6] See Sections 2.3 and 4.10 on IT incident handling peculiarities.

Every IT security team member needs to train their social skills by taking an active participation in their networks. This way, they will have a chance to succeed in real IT security related scenarios. They need two complementary soft skills to establish an effective communication[7]:

- Empathy or ability to interpret other people's emotions and their corresponding facial and body expressions.
- Capability to understand up to which extent others can read their facial and body expressions.

After the justification of why IT security professionals need to become active nodes in valuable social networks and the introduction to the basic traits of networking for IT security, we deal in the following sections with communication aspects for IT security professionals in three different scenarios:

- Inside the organisation or the customer firm where they provide their security services.
- Outside the organisation or the customer receiving their security services.
- A final scenario dealing with the IT security professional as a personal brand (Image 9.1).

Image 9.1 Positive emotions facilitate human relationships

[7]Parkinson et al. (2008), p. 1.

Networking Inside the Organisation

9.3 Targets for the Networking Efforts of the IT Security Team

Networking in the organisation is an activity that is directly related to three topics that we have already mentioned in this book. We base our recommendations on them:

- The stakeholder analysis for the IT security team.[8]
- The viral marketing activities proposed for IT security teams.[9]
- The tuning that IT security teams need to achieve with management.[10]

With whom should team members build rapport? We distinguish three main networking targets that IT security teams need to contact:

- IT security customers (managers, business areas and final users).
- Other IT teams.
- Security colleagues, both in the IT security team and in other teams.

IT security professionals need to know their prospective customers in the business areas, their IT colleagues, the members of their team and any other party practising security in the organisation before they provide their IT security services to any of them. Thus, any future IT security service provision could be smoother and even more valuable for the customer.

9.3.1 IT Security Customers

We include senior and line managers, users in business areas and final users in the set of IT security customers. IT security professionals that establish an initial contact with their customers before they render their security services can reach higher levels of service quality and customer satisfaction. For example, when the team perform a security test to an IT system used by the marketing department, there is a difference between approaching the task with a brief statement as "there is another server to test" (with no other additional information) or to start the activity "in the server that holds the application named '*great ideas*', a marketing application heavily used by Alice and Bob, both co-workers in the brand awareness section, who are currently busy with the 'super secret' preparation of the campaign to launch a new gadget that will hit the market in the coming weeks. By chance, an IT security team member shared a table in the last Christmas party organised by colleagues from the public relations department".

[8] See Section 5.9.

[9] See Section 7.8.

[10] See Section 8.1.

9.3.2 Other IT Teams

A stable relationship between IT security team members and colleagues working in other IT teams present in the organisation, both with operational or project-related duties, facilitates the regular work-related interaction they have on a regular basis.[11]

9.3.3 Security Colleagues in the IT Security Team

With regard to the networking efforts targeted to members of the IT security team, the possibilities to interact with them are immense,[12] since they all share work activities, and probably, physical space at work.

Regarding any other colleague dealing with security topics in the same organisation but in different contexts, we distinguish two groups:

9.3.3.1 IT Security Colleagues Working in Other Groups or Departments Within the Same Organisation

It is still usual to find IT security professionals working in different teams within the same organisation. The existence of several teams typically responds to power-related demands coming from competing departments, rather than to a real business or compliance need. There are occasions when the most agile and reliable security services proceed from a team that does not carry the official label "IT security".

All IT security teams in the organisation, regardless of the department where they are located, need, first, to establish regular contacts, and second, to find common objectives and passions. The contact among IT security groups should be fruitful for all participants. Our suggestion is the creation of a unique, though virtual, "human team", under a consensus-based leadership.[13] All members of the "virtual team" will accept their leaders. The value proposition for this "virtual team" is simple to state: The bigger the group of people who share the common passion for IT security, the more relevance and consistency they can acquire within the organisation.

---

[11] See Sections 7.2 and 7.11.

[12] Chapter 6 describes interaction patterns within the IT security team.

[13] The existence of different leaders for distinct security aspects is possible, for example, a technical leader and an HR-related leader. Evidently, both leaders need to communicate and cooperate extensively.

9.3.3.2 Security Professionals Dealing with Other Aspects of Security That Are Not IT-Based

Security and safety[14] include many aspects that have nothing to do with information technology, like physical security and product safety, among others. Depending on the industry, organisations will employ security-related teams that are far away from information security and IT. Their expertise will certainly be different from IT security. However, most security fields base their actions in similar principles.

Nowadays, the tendency is to find merged threats: The conjunction of a physical threat with an IT-based threat to obtain a greater impact.[15] Our recommendation is to establish an open communication channel with security colleagues working in other professional fields. Sooner or later, there will be merged threats that will require a collaboration between security teams with expertise on very different aspects of security.

9.4 Locations to Practice Networking

9.4.1 Common Use Facilities

Almost any place and any event are susceptible to become optimal networking venues. Regarding places, the first contacts with colleagues working for the same organisation happen in common use facilities like meeting rooms, cafeterias, canteens or even relaxation rooms. Concerning events, any organisation-wide gathering, such as the celebration of a remarkable anniversary or a summer party, is an excellent networking scenario.

9.4.2 Meetings with Business Areas

IT security team members could network in any formal meeting that is attended also by business areas representatives or other IT colleagues. Maybe the agenda does not relate to IT security. However, there will be coffee or lunch breaks during which an IT security team member could establish a first contact with a new potential customer. That first contact could make a positive difference in a future security engagement that would involve that meeting attendee.

---

[14] According to wordreference.com, security consists of "the set of measures taken as a precaution against theft or espionage or sabotage etc.", whereas safety is "the state of being certain that adverse effects will not be caused by some agent under defined conditions". Most definitions convey the message that safety deals with accidental events and security treats intentional events. Extracted from http://wiki.answers.com. Last accessed 16-10-2009.

[15] More on this topic in Chapter 10.

Participants in that type of events use to limit their communication circle to those colleagues they already know. IT security professionals should abandon this tendency. Losing an occasion to meet new people can mean missing a "once in a lifetime" opportunity.

9.4.3 Any Interaction with Customers Is a Potential Opportunity

The steps taken during the investigation of an IT security incident are a less typical networking occasion. It can turn into an opportunity to meet affected business area colleagues and to show how a quality damage control job is performed. In general, the provision of any IT security service that includes a face to face contact with a customer is a possibility for networking.[16]

9.5 How to Proceed with Networking

Any type of optimal communication should be based on two basic principles: Respect for the interlocutor and clarity in the message. Networking is an open sort of communication. It is probably closer to a viral marketing activity[17] than to a common work-related daily interaction.

Which topics should IT security team members raise when talking with customers in the business areas or to peers in other IT teams?

The main difference between networking and a purely work-related communication is that, in the case of networking, there is no apparent immediate purpose in the exchange of information. Most networking situations include an exchange of ideas and views, more than facts and figures related to a specific topic at work or to the sale of a service. It is a way for involved interlocutors to identify, first, common professional or personal grounds, and second, potential value in a future relationship (Image 9.2).

When possible, we recommend "***face to face***" networking. This way, non-verbal communication can play its relevant role. Parties involved in the networking activity try to adapt to each other with their tone of the voice, their body language and their words.[18]

---

[16] An example of an excellent opportunity for informal networking is the face to face delivery of security tokens used in two-factor authentication to final users, if the IT security team is in charge of their handing over.

[17] See Section 7.8.

[18] See Section 3.6 and Atkinson (2005), Chapter 11.

Image 9.2 Face to face interactions build stronger links

For IT security team members, face to face interactions require, not only time, but also the effort to leave their desks and, probably, to take the stairs or the lift to visit a colleague working somewhere else in the organisation. Those co-workers in the system administration team or in the network team are optimal candidates to network with, due to the high dependence of IT operational security teams on those two teams.

Team members with a more reliable and expert network are actually making their future engagements in the organisation easier and more effective. Among some of their customers, they will find strong allies.

Networking Outside the Organisation

Besides the organisation where the IT security team deliver their services or, in the case of an IT security company, in addition to their customers, there are other networking scenarios where IT security professionals need to be present to obtain professional value and ideas for new activities.

In the following sections, we refer to four networking setups:

- The IT security community.
- Academia.
- Law enforcement agencies.
- Local communities.

9.6 The IT Security Community

The majority of business processes that run in any industry rely on IT systems. IT security teams work to protect data residing in those IT systems.[19] Consequently, IT security is present in most, if not all, sectors. There are many IT security teams out there and our call is that, if they network with each other, they create a "spiral of new value".[20]

9.6.1 The IT Security Community in the Same Industry

There are many IT security professionals, most of them working in security teams, living similar work-related experiences within the same sector. Typical examples of sectors using IT security teams are the banking, pharmaceutical and utilities industry.

Networking is a means to connect IT security peers. All these IT security professionals could benefit from sharing and exchanging IT security views, their "war stories", among them. It is an opportunity to increase their professional value but they first need to meet each other.

Organisations that play in the same industry usually compete against each other. However, IT security teams working in rival companies should not become competitors as well. They have similar challenges, therefore, they can learn and benefit from each other.

It is frequent to find IT security related events organised to bring closer teams that are working in the same industry. We recommend IT security team leaders to consider attendance of one or more team members to those security meetings. It can mean the first step towards the creation of tighter links with other IT security teams that work in the same industry for companies with, probably, a similar size or a similar target market.

The criteria to consider the participation in IT security gets-together should not only be the expected quality of the presentations scheduled for the event, but also the networking value of the occasion.[21]

9.6.2 How to Share Security-Related Information When Networking

IT security professionals, especially those working in incident handling, penetration testing or risk assessments, handle confidential information almost on a daily basis.

---

[19] The "risk house" model, presented in Section 8.6, shows the role of IT systems in organisations today.

[20] See Section 9.2.

[21] Sometimes networking objectives justify attendance to events with poor technical content.

Most of those professionals have signed non-disclosure agreements (NDAs) with their organisations that prevent them from sharing sensitive information with third parties.

Most of the times, there is a possible way to share experiences in IT security fora with IT security colleagues working for other firms without breaching any NDA[22]:

- Data can be anonymised.
- Figures can be modified.
- Identifiers, e.g. IP addresses, can be hidden, etc.

Once event participants overcome the reluctance to share information about incidents, vulnerabilities and detected threats, they will benefit from each other's experience on neutralising IT security risks and they will be more prepared to provide value to their customers when they are back at their offices.

9.6.3 The IT Security Community Working in Different Industries

The ubiquitous nature of information and information technology (IT) based systems holding valuable data make IT security a necessary component to protect information in many sectors.[23] An advantage for IT security professionals is that, every day, they are more demanded by players in different industries. Thanks to the growing demand,[24] security professionals can swap business while they are able to continue working on similar IT security topics.[25]

9.7 Examples of IT Security Fora

IT security experts from all industries, all of them members of the big IT security community, gather in fora with very different flavours and purposes. Similarly to the two main profiles[26] present in IT security, governance or policy-related and hands-on technical IT security, we make a first high-level distinction of professional networks.

---

[22] In addition to an NDA signed by professionals in an organisation, some networks of IT security professionals make all their members sign an additional NDA to prevent member data leaks.

[23] See Section 8.6.

[24] See Section 2.1.

[25] Phishing. An example of different industries suffering from the same threat: The three top industries targeted by phishers in 2008 were financial institutions (76% of all phishing lures), Internet Service Providers (ISPs, with 11%) and retailers' sites (8%), according to the XIV Internet Security Threat report from Symantec. Available at http://www.symantec.com/business/theme.jsp?themeid=threatreport. Last accessed 13-10-2009, pp. 75–77.

[26] See Section 2.2.

IT security leaders should be able to categorise potential networking possibilities into one of these two generic types: Governance-related or technical networks. Hence, they will be in a better position to propose participation of each team member in the most appropriate forum.

For example, a hands-on technical team member joining a network of professionals or attending an event that focuses on governance or high-level IT security strategies, will not enjoy the contact and, what it can be more detrimental to the team, they will not bring value back to their colleagues.

In the opposite scenario, a policy-related team member, who attends a live demo of the latest modules for a security testing tool, will not retain as much valuable information of the exercise as an experienced hands-on member.[27] Certainly, the optimal case will be when team members have both profiles or, at least, the motivation and ability to acquire them. However, not all IT security teams offer that possibility.

We list some examples of existing IT security fora.[28] Although we label these examples as governance-related or technical hands-on, it is becoming more common to find some traces related to security policies and governance in technical fora. The following names offer, not only certification or security-related content, but also a chance to network within the most renowned IT security community.

9.7.1 IT Security Governance-Related Networking Possibilities

9.7.1.1 ISACA[29]

The Information Systems Audit and Control Association (ISACA), with more than 86,000 members worldwide,[30] provide IT governance-related content. Their two products are the COBIT and ValIT frameworks. Although their resources are only accessible to ISACA members, they also release many IT governance-related papers in the public pages of their site.

Together with white papers and frameworks, ISACA offers three IT governance-related certifications. They require continuing professional training credits to maintain them:

- Certified Information Systems Auditor (CISA).
- Certified Information Systems Manager (CISM).
- Certified in the Governance of Entreprise IT (CGEIT).
- Certified in Risk and Information Systems Control (CRISC).

[27] Unless they are seriously thinking to extend their field of expertise into hands-on security testing.

[28] This list is not exhaustive. It only provides some initial leads to the reader.

[29] ISACA web site available at http://isaca.org. Last accessed 15-10-2009.

[30] According to http://www.isaca.org/Content/NavigationMenu/About_ISACA/Overview_and_History/Overview_and_History.htm. Last accessed 15-10-2009.

9.7.1.2 ISC2[31]

The International Information Systems Security Certification Consortium (ISC2), apart from offering the Certified Information Systems Security Professional certification, held by over 45,000 professionals in more than 120 countries,[32] provides an interesting resource guide and a blog in their public pages. Certified professionals also require earning professional education credits to maintain their credentials.

9.7.1.3 ISF[33]

The Information Security Forum (ISF) is an organisation whose members include more than 50% of Fortune 100 companies.[34] Some of the briefing papers of the ISF, and their standard of good practice, are available to the public in their web site.

With a relatively high annual fee per company membership, they offer participation in various work group meetings and workshops throughout the year. The input provided in those meetings by IT security colleagues working in member companies is a core element for ISF policies and other new security papers. The ISF regularly release those documents among their members.

9.7.2 Technical IT Security Related Networking Possibilities

9.7.2.1 OWASP[35]

The Open Web Application Security Project is an open-source application security project.[36] OWASP members include corporations, educational organisations, and individuals from all over the world. This community works to create freely-available articles, methodologies, documentation, tools and technologies.[37]

OWASP offer technical and non-technical security-related videos, presentations and publications featured in their conferences. They also organise inexpensive local

[31] ISC2 web site available at http://isc2.org. Last accessed 15-10-2009.

[32] According to http://www.isc2.org/PressReleaseDetails.aspx?id=2706. Last accessed 12-10-2009.

[33] ISF web site available at http://www.securityforum.org. Last accessed 12-10-2009.

[34] According to https://www.securityforum.org. Last accessed 12-10-2009.

[35] OWASP web site available at http://owasp.org. Last accessed 12-10-2009.

[36] See Sections 4.4 and 4.9.

[37] Information extracted from http://en.wikipedia.org/wiki/OWASP. Last accessed 12-10-2009.

events with attractive topics. They benefit from a smart collaboration with local IT security communities.

9.7.2.2 SANS[38]

They are well-known security training providers. They offer the GIAC[39] certification program and they also make useful security resources available to the entire IT security community via their web site, among others:

- Security incident information at the Internet Storm Center.
- Valuable security papers available from the SANS Reading room.
- Security policy samples from the resources section.
- Several newsletters to which readers can subscribe (about security news, vulnerabilities, security tips for executives and awareness, among others).
- Security mentoring events for GIAC certifications through local communities. They are an excellent opportunity to network and to learn technical IT security topics.

9.7.2.3 Pauldotcom[40]

They provide free valuable IT security podcasts, presentations and articles in a very entertaining fashion since 2005. Their mailing list and the "full show notes" of every podcast are worth mentioning.[41] They offer not only valuable (and free) security contents but also the opportunity to network online with an active IT security community via their IRC channel and their mailing list.

9.7.3 Worldwide Known IT Security Conferences

The examples of fora that we have provided, both governance and technical hands-on related, organise or are related to IT security conferences that take place around the globe throughout the entire calendar year. They are reputable and well-known IT security events that are usually frequented by big players in IT security. We encourage security team members to send papers to those conferences.

---

[38] SANS web site available at http://www.sans.org. Last accessed 15-10-2009.

[39] GIAC is offered by the SANS Institute and it stands for Global Information Assurance Certification.

[40] Pauldotcom site is available at http://www.pauldotcom.com. Last accessed 15-10-2009.

[41] See Annex 3. IT security starter kit.

The professional and networking value that they could gain is certainly worth the research and the process to elaborate the paper:

9.7.3.1 Governance Conferences

RSA[42] Security Conference

Every year there is a RSA security conference[43] in the US and another one in Europe. The company RSA, security division of the company EMC, started this conference in 1991 for IT security governance and executive security officers.

ISACA[44] International Conference

ISACA organises a yearly conference dealing with IT governance, IT audit, information security and IT risk management topics, mostly at executive level.

ISF World Congress

ISF member companies have the possibility to attend an annual congress where they share the latest ISF reports and experiences.

9.7.3.2 Technical Conferences

Defcon[45] Hacking Conference

It is one of the most popular hacking conferences for technical security people. It was founded by Jeff Moss in 1993. In 2009, it gathered more than 10,000 attendees. It takes place in Las Vegas (USA) in hot Summer and, usually, the vulnerabilities unveiled during the conference make worth the visit. For those professionals who cannot attend, part of the material presented in the conference is released either in the conference website or in other IT security related sites.

---

[42] RSA stands for Ronald Rivest, Adi Shamir, and Leonard Adleman, inventors of the RSA encryption algorithm.

[43] See their Internet site at http://www.rsaconference.org. Last accessed 21-10-2009.

[44] ISACA is the Information Systems Audit and Control Association.

[45] See site available at http://www.defcon.org. Last accessed 12-10-2009.

Black Hat

It consists of a series of conferences (BH USA, BH DC, BH Europe) that take place every year in several locations.[46] Jeff Moss also founded this initiative in 1997, and he sold it in 2005. These conferences deal with similar technical security topics but in a more formal context. The entrance fee for Black Hat is considerably more expensive than the one for Defcon. Consequently, the number of attendees is lower.

OWASP Conferences

Most active OWASP local chapters organise, at least, half-a-day or a full-day conference every year. Apart from the local events, they also organise global application security conferences[47] in the US, Europe and Asia. OWASP provide links to most of the presentations from their site.

CanSecWest

This is a yearly conference, organised in Vancouver (Canada), that offers technical security presentations.[48] Some of them can be retrieved from the conference site.[49]

ShmooCon

Hacking convention[50] organised in the East Coast of the USA with an informal and amusing format,[51] including the weird process they follow to sell their hard-fought tickets.

Brucon

This is a new player in the technical IT security conference arena. Brucon[52] started in 2009 in Brussels. It is a European attempt to interweave security trainings with a technical conference.

---

[46] See archives at http://www.blackhat.com/html/bh-media-archives/bh-multimedia-archives-index.html. Last accessed 12-10-2009.

[47] More information on http://www.owasp.org/index.php/Category:OWASP_AppSec_Conference. Last accessed 12-10-2009.

[48] See site available at http://cansecwest.com. Last accessed 12-10-2009.

[49] See examples at http://cansecwest.com/pastevents.html. Last accessed 12-10-2009.

[50] See site available at http://www.shmoocon.org. Last accessed 21-10-2009.

[51] Attendees are armed with "shmooballs" so that they can assess the quality of the speakers real-time.

[52] See site available at http://www.brucon.org. Last accessed 2-11-2009.

Adjacent to those big names, there is an increasing number of smaller IT security related conferences and events. They adopt different formats and some of them are organised by local IT security communities. Our suggestion to IT professionals is to establish links with those IT security colleagues who work in the same geographical area and to keep track of local IT security events. In most occasions, the value of the event is up to the motivation, drive and professional acumen of the participants.

IT security team leaders should encourage their team members not only to attend local and worldwide known conferences, as excellent ways to network within the community, but also to actively contribute by preparing and presenting innovative security papers[53] on these events.

9.8 How to Network with Academia: Schools and Universities

Universities are an excellent source of trainees and of research for IT security teams. We identify two channels to contact academic representatives:

- A handful of IT security team members will maintain their networks from high school or college times.
- Universities offering IT, or even IT security, degrees located close to the geographical area where the IT security team work.

As a first measure to establish an effective networking with academia, IT security team leaders should offer traineeships in the team, so that pre-graduated or graduated students have the opportunity to get to know an IT security team[54] in action.

Those traineeships are usually warmly welcomed by IT and IT security professors, instructors and deans. They constitute a valuable instrument to connect students with the real business world. Together with traineeships, we advise to establish other types of collaboration programs with the educational world, such as:

- Lectures on IT security topics by senior team members, inside and adjacent to a programmed degree.
- Engaging University departments in IT security research for the team.[55]
- Security awareness sessions given by team members to students and professors.
- Introduction of secure development concepts in programming and IT architecture subjects.[56]
- Organisation of cyber games such as “capture the flag” (CTF) events.[57]

[53] See Section 3.5.

[54] See Section 2.4.

[55] ICT-Forward is an example of valuable collaboration among private sector, academia and institutions. See their site at http://ict-forward.org. Last accessed 12-10-2009.

[56] See SANS secure development initiative at http://www.sans-ssi.org. Last accessed 21-10-2009.

[57] See examples of a cyber exercise provider at http://www.whitewolfsecurity.com. Last accessed 21-10-2009.

9.9 How to Network with Law Enforcement Agencies

IT security team members need to have, at least, a contact in law enforcement, preferably ***before*** the occurrence of any ***serious IT security incident*** that would definitely require the intervention of law enforcement agents.

Those law enforcement representatives with interest in IT and IT security topics, especially agents who deal with illegal pornography, intellectual property and personal data theft and economic fraud, will undoubtedly benefit from a relationship with IT security experts.

How can the first contact with law enforcement colleagues happen? From the IT security team perspective, a usual way to interact is through the attendance or the organisation of events where law enforcement agents are also invited. This coincidence is becoming more usual due to two reasons:

- Terrorist groups start to commit merged attacks, i.e. concurrent acts, normally with a great impact, against the digital and the physical world.
- The dependency of physical security on IT systems is growing.

The sooner IT security professionals establish a network with law enforcement agents, the seamless any future interaction between them will be.

If the IT security team works for an organisation that employs also physical security professionals, our recommendation for the IT security team members is to establish, as a first measure, a strong link with them. Both teams will work close to each other and, more importantly, they will share common goals, only that they come from different angles. Second, we propose to network with law enforcement, initially through the contacts that the physical security colleagues might have.

IT security professionals need to achieve some rapport and tune in their relationship with physical security colleagues and law enforcement agents. An effective networking measure is to organise briefing sessions in which technical IT security team members provide them with a live demonstration on the latest IT security threats and possible means to mitigate them. Usually, physical security professionals show interest in these presentations, especially if they see a link with their physical protection world (Image 9.3).

Every minute that an IT security team member devotes to synchronise with physical security professionals, related either to the customer organisation or to governmental agencies, constitutes a real investment for future interactions with them.

9.10 How to Network in the Local Community

When Medicine students finalise their studies, their first patients are their closest relatives and acquaintances. Similarly, family and friends are the first customers that an IT professional will have. A computer infected with a handful of viruses,

Image 9.3 Networking is like grapes that produce good wine, they need care and attention since day 1

a laptop that simply does not boot or a web page that cannot be loaded in a browser are typical examples of cases that any IT professional is confronted with.

Unfortunately, IT professionals are only contacted when any other potential fixing party has already failed and there is no feasible solution that satisfies all the customer's requirements. IT security professionals embark themselves on a complex and time-consuming activity, sometimes with no happy end. We refer to this situation as the "eternal IT helpdesk".

Our proposal for this scenario is to frontload healing actions, transforming corrective actions into preventive measures. This way, the effectiveness of a similar effort is greater.

There are multiple activities that IT security professionals can perform for their local communities, being those their church, their neighbourhood, their local library or their social centre. For example:

- Presenting practical tips on how to protect a computer at home from Internet threats.
- Writing regular articles about IT security in a local newspaper.
- Creating a blog and publishing useful IT security tips.
- Appearing in local radio stations to advise on IT security.

All these actions are undoubtedly win-win deals for IT security professionals. While they provide value to their local community, they are also sharpening their presentation, writing or people skills. These skills are beneficial for their professional profile and will be priceless for their future development.

Networking for the Personal IT Security Brand

After the presentation of the networking possibilities that IT security professionals can explore inside and outside their customers and organisations, we introduce a new concept that is growing in importance within the IT security labour market: The ***personal brand*** of the IT security professional. The following sections focus on networking possibilities that could improve the value of the IT security professional.

9.11 Networking to Increase the Value of the IT Security Professional

The number of IT security professionals, especially those with highly specialised technical skills, who provide their services as ***freelance*** professionals or through micro-businesses that they run, is growing.[58] Prospective customers, with a specific and punctual IT security need, scan the market, contact one of the security specialists on that topic, such as forensics, virtualisation, remote access, and they acquire a customised value-added service.

The networking measures that we have proposed to IT security professionals in their local communities[59] are also valid marketing means to contact local businesses, scan their IT security demands and offer them tailor-made services.

This scenario is increasingly relevant for IT security professionals due to the following trends in the business world:

9.11.1 Small and Medium Enterprises (SMEs) Demand IT Security Services

Most organisations nowadays, regardless of their size, depend on information systems. A growing number of those organisations base their business processes on systems that are exposed to IT threats, many of those coming from the Internet. Most SMEs, including independent freelance-alike service providers in fields like Medicine, Architecture, Law or Insurance, cannot afford hiring an IT security service provider or professional on a permanent basis. However, they do occasionally require IT security expertise.

---

[58] Technology security consulting is a hot market for small businesses, according to Entrepreneur magazine, "Newest Trends & Hottest Markets", January 2005. Information retrieved from http://www.score.org/small_biz_stats.html. Last accessed 30-10-2009.

[59] See Section 9.10.

9.11.2 *Big Corporations Focus on Their Core Business and Outsource Support Functions*

One of the most compelling business mantras of this century is cost reduction and profit maximisation. Consequently, organisations focus on their core business processes and outsource what they consider accessory services. They buy support services from the market rather than maintaining costly in-house maintenance structures. Some organisations include their IT services within the set of functions to outsource. They also tend to package IT security and pass it on to a managed security service provider.

Considering our "***risk house***" model,[60] we could find strong arguments to justify why core elements of IT, and especially IT security, represent, not only "a support function", but a crucial component capable of providing a competitive advantage to the organisation.

Having these two tendencies in mind, it is time for IT security professionals, especially those with entrepreneurial skills, to create and look after their personal brand within the IT security market. Their IT security brand would be a means to maintain and increase their continuity as a professional in the IT security market for the coming decades.[61]

The suggestion to develop a personal brand in the market is remarkably more evident for those technical hands-on IT security entrepreneurial professionals.[62] They gather valuable experience on a daily basis in security testing, vulnerability identification and mitigation, computer forensics and incident management among others, while they interact with many different customers. On average, they are exposed to a greater number of different real IT security cases than internal IT security teams,[63] anchored at the same organisation for years.

Big corporations, all of them prominent IT security customers, demand punctual and highly specialised IT security services that, most of the times, cannot be efficiently rendered by their internal IT security staff. For example, a thorough computer forensic investigation in a server and a workstation used by a staff member in an alleged crime, or a penetration test with the latest Metasploit[64] modules on a critical server that will be exposed to the Internet.

---

[60] Presented in Section 8.6.

[61] Chapter 10 provides further input about future IT security market trends.

[62] Our forecast is that the next IT security profile following this trend will be IT security strategists, those with enough experience and vision to foresee and organise the IT security landscape in organisations in the coming decades.

[63] The role of internal IT security teams is evolving into brokers, resource coordinators and valid interlocutors with IT security service providers (independent consultants and providers of managed security services).

[64] The Metasploit framework is a tool for developing and executing exploit code against a remote target machine. Input from http://en.wikipedia.org/wiki/Metasploit. Last accessed 22-10-2009.

Against this background, we state that IT security professionals need to network within the IT security community and market their "personal professional brand",[65] regardless of the type of relationship they hold with the organisation they currently work for, be it as an employee or as an independent consultant or owner of a small security firm.

9.12 How to Build IT Security Reputation

How could proactive IT security professionals proceed to network to maintain and, if possible, increase their value in the market, i.e. to improve the image of their ***personal IT security brand***?

The main source of value for an IT security professional is their reputation in the market. The objective will be to build a durable and dependable reputation, first within the IT security community and, second, within the IT management community.

The value of a professional, inside the IT security community, resides on two pillars:

- The products[66] that they make available to the entire IT security community.
- The relevance of their position and their professional engagements.[67]

9.12.1 Provision of Value to the IT Security Community

Each human being feels more comfortable performing on one of these three activities[68]:

- Thinking (in our case, we add, thinking about the future).
- Writing.
- Speaking.

These three activities are part of everybody's life. However, it is exceptional to find individuals that excel in all three of them. This statement also applies to professionals in IT security.

---

[65] In 2009 marketing a personal IT security brand is an option. In the coming years it will be a hard fact-based requirement.

[66] Usually in the form of open source code, free tools, technical howtos, papers, articles, etc.

[67] For example, speaker at well known conferences, access to decision making fora or a high number of professional connections.

[68] Adapted from Nobokov (1973), p. 3. Foreword.

IT security professionals should embark on networking activities when they can make use of the activities they master. They need to assess their strengths with the valuable input of their closest social circles (friends, relatives, colleagues) and use them:

9.12.1.1 IT Security Thinkers

If the professional thinks and analyses superbly, they should make a forecast exercise and outline the defining parameters for IT security in the coming years. Their strategic input will be precious information for managers and IT security teams in organisations. With regard to networking, they should approach decision-makers using their second best skill, be it writing or speaking.

9.12.1.2 IT Security Writers

Professionals who are excellent writers should focus their efforts in contacting the community through their written products, without overlooking "face to face" communication:

- Writing articles about current topics for IT security magazines.
- Releasing useful posts in popular security blogs.[69]
- Creating their own security blog site.
- Writing books on novel security topics.

9.12.1.3 IT Security Speakers

If the professional is a convincing speaker, in terms of local networking, they should present hot security topics in their local community or at work. Almost any occasion is appropriate to raise security awareness through a persuasive presentation given by an excellent talker.

Regarding global networking possibilities, together with their expert knowledge, they need to make use of their voice and words[70]:

- Appearing in well-know IT security podcasts.[71]
- Answering IT security related questions in local radio stations.
- Creating their own voice-based IT security product (podcasts, radio programs, conferences, etc.).

[69] Most of the links provided in Annex 3 give also access to well-known IT security blogs.

[70] See Section 3.6.

[71] See Annex 3. IT security starter kit.

9.12.2 Provision of Value to the IT Management Community

Generally, IT managers hire IT security professionals based on the value they can provide to achieve their mandate. Initially, managers are not aware of the leverage that IT security experts can bring them. Through smart networking, preferably face to face, IT "securiteers" need to make IT managers grasp that they can use IT security both to protect the organisation and to contribute to their permanence in it.[72]

9.13 Recommendations to Build an IT Security Personal Brand

This chapter concludes with a collection of tips, based on experience, on how an IT security professional should network to create their own personal brand. This set of suggestions also applies to build the brand of an entire IT security team. A team can set themselves up as a distinctive professional entity, hence with their own collective brand.

9.13.1 Security by Default Does Not Mean Social Isolation

Passionate IT security people live security (IT securiteers).[73] They apply security to every aspect of their lives. However, their commitment to protect data confidentiality should not create a reluctance to communicate and socialise, especially when they aim at selling their services. They need to be able to establish and maintain a fluent conversation in a social event with someone they do not know yet and talk about their IT security activities without revealing critical data.[74]

9.13.2 Modesty and Honesty[75]

No individual knows everything. Neither do IT security professionals. No "IT securiteer" can afford to neglect the lively IT security community, where arrogance is not welcomed at all. Excellent networking players are modest and honest when they

[72] See Section 1.20 and Chapter 8.

[73] See Sections 2.6 and 2.7.

[74] See Section 9.6 about networking outside the organisation.

[75] Adaptation of the "underpromise and overdeliver" principle mentioned in Section 5.4.

interact with their peers. There is no point in trying to sell a professional image that does not reflect reality. Sooner or later, their customers, team colleagues and managers will discover their real quality.

9.13.3 Preparation for the Unknown

The professional world revolves fast and the IT security work landscape for any IT security professional can change dramatically very quickly. IT "securiteers" need to be ready to cope with unexpected changes. This requires a thorough evaluation of different situations, including worst-case scenarios, e.g. how long could an IT professional keep their living standard after an unforeseen layoff?[76]

Leaving a work engagement in a non-elegant way or with unsolved disputes can easily mean a potential closed door to an attractive professional adventure in the future. Professionals swap the roles of manager, coordinator, colleague, subordinate, competitor, sponsor, customer and coach in an increasingly quick and unforeseeable manner. This fact makes us strongly advise IT security professionals against "burning any professional bridge". It is usual to find a future manager in a current subordinate, colleague or team member.

Consequently, a networking principle in IT security is to keep relationships with all stakeholders in good terms, especially when there is a change of jobs in the horizon. This recommendation includes the need to avoid criticism, purely based on personal views, of prior employers, managers and colleagues.

The number of colleagues with whom any IT security professional will interact during their career tends to be high. However, the number of colleagues who will play a decisive role in the career development of the IT security professional is relatively small. The impossibility to distinguish beforehand among those two groups leads us to propose keeping good relations with all of them.

9.13.4 The Company of Better People

Those professionals who are willing to develop and evolve need to get surrounded and work with people they can learn from. Colleagues with better technical or soft skills are among them. Additionally, colleagues with different backgrounds, approaches and alternative ways of thinking can also be optimal candidates to work with.[77]

---

[76] In case of a layoff, the career incident response podcast series, by Lee Kushner and Mike Murray, is an interesting lead. It is available at http://www.infosecleaders.com/career-incident-response-audio-series. Last accessed 8-11-2009.

[77] See Section 6.2 about working with colleagues with alternative views.

9.13.5 A Permanent Ambassador Role

An "IT securiteer" is always an ambassador, first of their personal brand, second, of their team, and third, of the company they are representing. Every public appearance, product, service that an IT security professional makes available to their customers, or to the community, is subject to customer or public scrutiny.[78]

For example, an IT security professional who shows a lousy IT security stance related to any facet of information security could easily destroy the reputation that they earned during years of intense career.[79]

We conclude this chapter with these recommendations about how to maintain and look after the personal IT security brand, the ultimate purpose of all networking efforts (Image 9.4).

Image 9.4 The personal IT security brand is a treasure to look after

[78] Even careful scrutiny if the reputation of the professional is excellent.

[79] Would a customer trust their commercial secrets to an IT security professional that loses an unencrypted laptop with confidential customer information?

Chapter 9: Learning points

- Networking opens the door to tendencies, to understand society and to prepare for future professional changes.
- Networking requires time and interest but it creates value based on new information.
- Customers, IT security colleagues and security professionals are the networking targets of the IT security team.
- They can network in common use facilities, meetings and, basically, everywhere.
- We recommend to network face to face within the organisation.
- The IT security community is present in most industries.
- There are IT security governance and technical IT security fora.
- Traineeships, lectures and joint research are possibilities to network with schools and Universities.
- We recommend to network with physical security colleagues and law enforcement agents before any IT security incident happens.
- Networking in the local community has a lot of potential for IT security professionals, especially if they provide preventive security measures.
- Smart networking increases the value of the IT security professional.
- IT security professionals need to provide value to the IT security community by using their best skills.
- Modesty, honesty, preparing the future and learning from colleagues contribute to building a personal IT security brand.

Link to MBA Management Models

We have selected two MBA-related models that deal with the complexity of human relationships in organisations:

Four organisational cultures *(by Charles Handy, 1976, 1981, 1985 and 1993)*
Frequently a mix of four types of cultures exists in organisations:

- Power culture: A mesh of relations with a central power source.
- Role culture: A hierarchical and bureaucratic structure.
- Task culture: Mostly job or project-oriented interactions.
- Person culture: The structure exists only to serve individual members.

Organic vs. mechanistic management styles *(by T. Burns and G.M. Stalker, 1961)*
There is a shift in organisations from mechanistic to organic interaction styles:

- Mechanistic: Clear structure, procedures, formal communications and controls. Bureaucratic style.
- Organic: Soft links, flexible reporting lines, broad mandates and commitment of individuals to the organisation.

The networking approach to set into practice differ according to the predominant management style in the organisation.
See reference: Harding and Long (1998).

Chapter 10
Present, Future and Beauty of IT Security

Chapter 10: What will the reader learn?

This chapter answers the following questions:

- Why is IT security so relevant now?
- What is the state of IT security in small and medium enterprises?
- What is the attackers' industry like?
- What is the relevance of IT security related information?
- How is the emergence of complexity affecting IT security?
- Will reputation be a valid way to provide trust to network flows?
- Why is personal privacy dead?
- What relation does IT security have with critical infrastructures?
- Why does the "onion layer" paradigm change to an "onion ring"?
- How will IT security influence virtual IT and "the cloud"?
- How will IT security influence mobile IT?
- What is the future of IT security in terms of forensic and legal needs, log monitoring, risk management and decision making and compliance?
- How can creativity be reached in the social realm of IT security?
- And creativity in the technical arena of IT security?

Where does IT security head for? Using geographical terms, we provide in this book a helicopter view over the "growing City of IT security", located at the heart of the "country of information technology (IT)".

We dealt in Chapter 1 with the three ancient founders of the city, threats, vulnerabilities and risks and the "three main founding principles", confidentiality, integrity and availability. We introduced the outlook and skills of its "inhabitants", the IT "securiteers", in Chapter 2. Chapter 3 provided input on their "basic social unit", IT security teams. Chapters 4 and 5, respectively, have provided information on the activities that IT security teams should carry out and how these actions could be successfully performed.

A. Partida and D. Andina, *IT Security Management: IT Securiteers - Setting up an IT Security Function*, Lecture Notes in Electrical Engineering 61,
DOI 10.1007/978-90-481-8882-6_10, © Springer Science+Business Media B.V. 2010

In Chapter 6, we suggested measures to develop a prosperous "City of IT security", transforming IT security teams into effective human systems and looking at the characteristics of the IT security job, the interaction patterns within the team and possible development measures. We continued in Chapter 7 with marketing activities that IT security teams need to embark on and, in Chapter 8, we put forward a risk management model and a collection of proposals to obtain sponsorship from the "city hall", i.e. to achieve management support. Subsequently, in Chapter 9, we wrote about the value that IT security teams could obtain if they interact among each other, inside and outside the "City of IT security".

Chapter 10 aims at presenting three visions that will complement this helicopter view over the "City of IT security":

- The latest present lines of development in IT security.
- The future of IT security.
- The beauty of IT security. Reasons why it can be so attractive.

The Present of IT Security

10.1 The Relevance of IT Security Now

The current dependency of world trade and world development on IT networks is considerable and increasing. IT security is already a technical field that plays a central role to protect world trade and, in general, the development of modern societies. The following figures validate these statements:

- In 2007, 30% of global trade was based on digital transactions.[1]
- In 2008, e-commerce in the US accounted for US$132 billion in retail sales.[2]

The access to digital networks starts to become a human right:

- Starting July 2010, every person in Finland will have the right of access to a 1 Mb broadband connection to the Internet.[3]
- In 2009, the European Parliament has viewed Internet access as a basic human right.[4]

[1] European Network and Information Security Agency (ENISA). Press release on 27-05-2008. Presentation of their General Report 2007. Available at http://www.enisa.europa.eu/media/press-releases/2008-prs/eu-efforts-called-to-avoid-a-digital-9-11. Last accessed 4-11-2009.

[2] Remarks by the US President on securing the nation's cyber infrastructure on 29-05-2009. Available at http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure. Last accessed 30-10-2009.

[3] Piece of news from Cnet.com. Available at http://news.cnet.com/8301-17939_109-10374831-2.html. Last accessed 29-10-2009.

[4] See European Parliament article available at http://www.europarl.europa.eu/news/public/story_page/058-54891-124-05-19-909-20090504STO54873-2009-04-05-2009/default_en.htm. Last accessed 29-10-2009.

At the same time, traditional fraud schemes find easy ways into the digital world. There are an increasing number of threats that are materialising in the computer world we all depend on:

- Since 2004, cyber thieves have stolen US$40 million from US-based small and mid-sized companies.[5]
- In 2008, more than US$1 trillion in intellectual property was stolen using digital means.[6]
- In 2007, the number of US adult victims of identity fraud was 8.4 million.[7]
- In the first semester of 2007, every day on average 52,771 computers were infected by malicious software, making a total malware-infected population of 5,029,309 computers.[8]

10.1.1 First Worldwide Reactions

Developed states worldwide start realising the dependency of their social and economic structure on IT networks and, especially, on the Internet. They consider their digital infrastructure a strategic national asset. Two relevant examples are:

- The US White House has stated that "America's prosperity in the 21st century will depend on cybersecurity".[9]
- The European Union's (EU) Agency for Network and Information Security (ENISA) underlined the critical importance of IT security for the European economy and called for concentrated efforts to avoid a digital 9/11.[10]

To complete the description of the current scenario, we mention that there is a variety of initiatives that support the development of IT security as a professional field. Many states are passing bills to empower IT security functions and to build resilient IT security capabilities within their public services and within their armed

[5] Piece of news from The Washington Post. Available at http://voices.washingtonpost.com/securityfix/2009/10/fbi_cyber_gangs_stole_40mi.html. Last accessed 4-11-2009.

[6] Remarks by the US President on security the nation's cyber infrastructure on 29-5-2009. Available at http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure. Last accessed 30-10-2009.

[7] From the Javelin Strategy & Research Survey. February 2007. Summary of survey findings available at http://www.privacyrights.org/ar/idtheftsurveys.htm. Last accessed 4-11-2009.

[8] "Botnets-The silent threat". Report released by ENISA on 7-9-2007. Available at http://www.enisa.europa.eu/act/res/other-areas/botnets/botnets-2013-the-silent-threat/at_download/fullReport. Last accessed 4-11-2009.

[9] Remarks by the US President on security the nation's cyber infrastructure on 29-5-2009. Available at http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure. Last accessed 30-10-2009.

[10] European Network and Information Security Agency (ENISA). Press release on 27 May 2008. Presentation of their General Report 2007. Available at http://www.enisa.europa.eu/media/press-releases/2008-prs/eu-efforts-called-to-avoid-a-digital-9-11. Last accessed 4-11-2009.

forces, mostly adopting the form of national IT security agencies and coordinated emergency response teams (CERTs).

Two examples of those initiatives are:

- The Cybersecurity Research and Development Amendment Act of 2009 in the USA, authorising US$68.7 million in grant funding in 2010, increasing this figure up to US$90 million by 2014, for computer and network security research.[11]
- The European Union has approved a budget for 2009 of €7.93 million for the European Network and Information Security Agency (ENISA).[12]

Modern states demand IT security professionals and they still find difficulties to staff specialised IT security positions.[13] For example, there is a shortage of highly skilled vulnerability researchers working for governments and software vendors.[14]

To mitigate the current lack of skills, some states sponsor public education measures such as cyber games[15] and "capture the flag" events[16] among high schools, graduate students and young professionals.[17]

IT security professionals need to take this call as a unique window of opportunity to deliver real value to their customers, communities and, ultimately, to the society they live in. Their expertise and knowledge to protect digital assets from current threats and to mitigate their vulnerabilities was never so demanded as in this first decade of the 21st century.

This book presents leads to IT security professionals who are willing to take up this challenge. Especially in a scenario[18] with more IT security jobs and fewer budget cuts for IT security, in which:

---

[11] Piece of news from SCmagazine US, available at http://www.scmagazineus.com/House-subcommittee-passes-cybersecurity-RD-bill/article/149714. Last accessed 4-11-2009.

[12] Information available at ENISA web site, http://www.enisa.europa.eu/about-enisa/accounting-finance. Last accessed 4-11-2009.

[13] For example, the US government will recruit up to 1,000 information security experts. Piece of news extracted from The Washington Post, available at http://voices.washingtonpost.com/securityfix/2009/10/dhs_seeking_1000_cyber_securit.html. Last accessed 31-10-2009.

[14] See the Top Cyber Security Risk Report from the SANS Institute. September 2009. Available at http://www.sans.org/top-cyber-security-risks. Last accessed 4-11-2009.

[15] For example, The US Air Force Association (AFA) organises cyber defense competition among high schools in the US, South Korea and Japan. See their press release on 20-10-2009. Available at http://www.afa.org/media/press/cyberpat09.asp. Last accessed 4-11-2009.

[16] See Section 9.8.

[17] US States like Delaware, California and New York have joined the US Cyber Challenge. See reference at http://feinstein.senate.gov/public/index.cfm?FuseAction=NewsRoom.PressReleases&ContentRecord_id=16b1f25c-5056-8059-766e-dc4dd89f85dd&Region_id=&Issue_id. Last accessed 4-11-2009.

[18] Extracted from press release from the International Information Systems Security Certification Consortium, ISC2, on 4-06-2009. Available at http://www.isc2.org/InnerPage.aspx?id=4590&terms=news+2009-06-04. Last accessed 4-11-2009.

– Organisations demand IT security professionals with knowledge and expertise in operations security, information risk management, access control systems and methodology, applications and system development security and security management practices.
– 80% of surveyed hiring managers have difficulties to find right candidate (we would add, at currently offered rates) (Image 10.1).

10.2 IT Security in Small and Medium Enterprises

Around the world, small and medium enterprises (SMEs) outweigh big corporations as employers and exporters. These figures demonstrate it:

– In the US: 72.9% of employees work for companies with less than 250 staff members[19] and 96% of businesses employ less than 49 people.[20]
– In the EU, 67% of employees work for companies with less than 250 staff members and 98.7% of businesses employ less than 49 people.[21]

Alone in the US, small businesses employ more than 50% of the private sector workforce and 40% of high tech workers (scientists, engineers and computer workers) and they represent more than 97.2% of all exporters of goods.[22] While SMEs constitute a real social and economic engine, the resources they devote to IT security are traditionally very low, although their IT dependency is already an undisputed fact.

Most big organisations have a history, at least for the last decade, of adopting certain IT security measures and hiring IT security professionals with very varied degrees of success. SMEs, however, with less resources to invest in IT security, have not dealt with IT security issues until very recently. Attackers have taken good note of this fact and they are targeting small broadband users (SMEs and homes). For many SMEs, given their size and their limited resilience, a severe IT attack[23] can mean the end of their existence.

---

[19] Data from the Bureau of Labor Statistics. Business employment dynamics: Tabulations by employer size. February 2006. Monthly Labour Review. Available at http://www.bls.gov/opub/mlr/2006/02/contents.htm. PDF file available at http://www.bls.gov/opub/mlr/2006/02/art1full.pdf. Table 1 – Page 5. Last accessed 4-11-2009.

[20] Data from Bureau of Labor Statistics. Job Creation by Firms of Different Sizes, 1992–2008. Published by New York Times. Available at http://boss.blogs.nytimes.com/2009/08/05/are-medium-sized-businesses-the-job-creators. Last accessed 4-11-2009.

[21] Eurostat statistics in focus 31/2008. Enterprises by size class. Overview of SMEs in the EU. Available at http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-SF-08-031/EN/KS-SF-08-031-EN.PDF. Page 1. Author: Manfred SCHMIEMANN. Industry, trade and services. Last accessed 4-11-2009.

[22] Data from U.S. Small Business Administration Office of Advocacy. September 2009. Available at http://www.score.org/small_biz_stats.html. Last accessed 4-11-2009.

[23] Piece of news from The Washington Post. Available at http://voices.washingtonpost.com/securityfix/2009/10/fbi_cyber_gangs_stole_40mi.html. Last accessed 4-11-2009.

The main motivation of attackers is to steal sensitive data[24] such as online banking credentials or credit card numbers. There are two main threat vectors for SMEs and home users:

- Drive-by infections: Employees and home users access trusted, but unprotected, Internet web servers that serve malicious content[25]: Pieces of code that would make use of common vulnerabilities, existing in most desktop computer with a typical collection of office applications installed.[26]
- Email attachments: Employees trust emails that they receive, containing attachments with malicious content.

Attackers take advantage of the generalised inability of most small organisations to effectively patch office desktop applications. A recent survey made to 100 SMEs located in nine countries has provided the following hard facts[27]:

- 71% of the surveyed SMEs believe that a data security breach could put them out of business.
- 2/3 of the respondent companies said that they spend less than 3 hours per week on IT security.
- 20% of surveyed companies said that they had a data security breach within the past year, being the average cost of the breach US$41,000.

The provision of affordable and effective IT security services to the SMEs is both a pending subject and a promising market for the IT security industry, with still not many players in the game.

Using the industry lifecycle model we present at the end of this chapter, the provision of IT security services to SMEs is still at the introduction phase. Likewise, using Porter's 5 forces model,[28] it is also an attractive industry for IT professionals to join because:

- The number of experienced competitors is still relatively low: There are not so many reputable pen-testers with a decade of experience.
- The number of potential customers is high: All SMEs and home users.
- The power that suppliers (IT equipment industry) can exert is low: Normally security tests can be carried out with basic IT equipment.

---

[24] See the Top Cyber Security Risk Report from the SANS Institute. Executive Summary. September 2009. Available at http://www.sans.org/top-cyber-security-risks. Last accessed 4-11-2009.

[25] In most cases, the administrators of those sites are not aware of it, due to lack of knowledge or simply lack of time.

[26] Operating systems continue to have fewer remotely exploitable vulnerabilities. See the Top Cyber Security Risk Report from the SANS Institute. September 2009. Available at http://www.sans.org/top-cyber-security-risks. Last accessed 4-11-2009.

[27] Piece of news from Security Focus web site on 29-10-2009. Available at http://www.securityfocus.com/brief/1029. Last accessed 5-11-2009.

[28] See Porter's 5 forces MBA model at the end of Chapter 4.

– The barriers to entry are high: Technical IT security expertise is required.
– There is an absence of real substitutes: SMEs really need IT security to continue their business.

Against this background, we can only encourage technical IT security professionals who are willing to leave big and slow organisations, to find their space in this unexplored market, either through a small IT security company or working as a freelance professional.

Image 10.1 IT security professionals need to guide small enterprises through the digital world[29]

10.3 The Attackers' Industry

The history of fraud is as old as human society. The 21st century simply adds two new elements to commit fraud:

– A new scenario, the ***digital world***.
– A new set of means, ***programming languages*** and ***network protocols***.[30]

Digital networks and Internet applications, such as e-mail and web browsing, make up an attractive playground for crackers and fraudsters to obtain juicy and easy profit.

[29] Photo depicting the sculpture of "The Prophet" by Gargallo (1933).

[30] Together with social-engineering techniques based on the ancient art of deception.

We focus on three actors present in this illegal industry and provide what it could be a plausible description[31] of them and the value chain[32] of this industry:

10.3.1 IT Technical Experts

They are mainly developers and IT knowledgeable individuals, specialised and in contact with the latest technology and IT trends, with sufficient skills to write lines of code, to discover software vulnerabilities and to misuse unprotected Internet nodes (servers and clients). They sell their services to the brains of the fraud schemes.

Most of them have very low ethics, but some of them work in this industry as the only real way to keep their family going. A common characteristic of these developers is that they live in countries with very low salaries and hardly any technology-related industry that could hire them. Consequently, it is very easy, and inexpensive for fraudsters, to entice these IT experts with attractive offers, that actually they do not contain high money figures in comparison with rates for IT developers in more developed countries.

10.3.2 Fraud Brains

Leaders of organised groups that already perform other sorts of illegal activities and extend their scope into the digital world, given the easiness and the relative impunity[33] it offers. They engage groups of developers to implement their fraud scheme or they just buy their software and services to subsequently carry out their plans.

10.3.3 Internet Mules

Any inconspicuous individual with access to a bank account from which they could operate (receive, transfer and withdraw) money is potentially an optimal Internet mule. They normally receive a tempting email offering easy money.[34] They simply have to transfer the money that they will receive in their account to other accounts or they have to just withdraw the money and use wire services to send it to someone else.

---

[31] Adapted from banksafeonline, an initiative from the UK banking industry. Available at http://www.banksafeonline.org.uk/moneymule_explained.html. Last accessed 13-11-2009.

[32] See Porter's Value Chain MBA model at the end of Chapter 8.

[33] Digital fraud offers a high profit to risk ratio (PRR). See Section 1.16.

[34] Additional information in the fact sheet from the Australian Bankers' Association. October 2009. Available at http://www.bankers.asn.au/default.aspx?ArticleID=1403. Last accessed 5-11-2009.

10.4 IT Security Information Analysis

Organisations struggle to compose an Internet-wide overview of current threats and vulnerabilities to identify which of them pose the greatest risks and where they should focus their efforts.[35] They require reliable information providers. The IT security incident database that we propose[36] could answer the need for any Internet user, at work or at home, to be aware of the latest fraud schemes and threats.

Any player in the IT security arena needs to be informed about the latest IT security incidents and developments. A worth-mentioning IT security threat information provider is the Internet Storm Center[37] (ISC). Similarly to the way national weather services publish information about current and immediate future weather warning messages, the ISC was born in 2001 with a similar mission but a different scope: To act as an early warning and threat detection service to Internet users.

The latest IT security strategy tenet that many States are following is that the best way to protect a country's assets is to be able to understand how attackers act and how attacks are performed.[38] The implementation of this basic tenet requires reliable IT security information and a high degree of technical specialisation.

The IT security community of the 21st century experience hectic moments. There are a myriad of new projects, initiatives, movements, and proposals that touch on any aspect of IT security and information assurance. The task to select which ones should receive attention is not immediate. IT security experts find themselves with not enough time to get to know all those new techniques, new tools and new approaches appearing in the community, mostly through Internet, almost on a daily basis.

The present and the future of this industry demand professionals with excellent data search, handling and analysis skills.[39] This book provides information leads to those professionals working in IT and, specifically, in IT security.

The Future of IT Security

The following sections present an outlook on what the IT security scenario will be like in the next decade. All sections include our forecasts. Regarding the events that we mention, the closer they are to 2009 and 2010, the very near future, the more they are based on real tendencies and on our experience. The further these forecasts spread in the coming years, the more subjective and only possible they are.

---

[35] Adapted from the Top Cyber Security Risk Report from the SANS Institute. Overview. September 2009. Available at http://www.sans.org/top-cyber-security-risks. Last accessed 4-11-2009.

[36] See Section 1.15.

[37] Supported by the SANS Institute. See http://isc.sans.org/about.html. Last accessed 5-11-2009.

[38] For example, a central tenet of 2008s U.S. Comprehensive National Cybersecurity Initiative (CNCI) is that 'offense must inform defense'. See Federal Computer Week's special report. Available at http://fcw.com/microsites/2009-security-directives/sharing-security-information.aspx. Last accessed 5-11-2009.

[39] See Section 3.19.

10.5 The Emergence of Complexity

10.5.1 Code Complexity

The dependency of the current modern society on digital networks and IT systems is patent. This means that business processes, including critical ones, online retail purchases, and any other action based on IT systems connected among each other through digital networks, rely on pieces of software, lines of code, that are running on many hardware platforms.

There are lines of code running at present in client computers, servers, network and security devices, mobile terminals and, basically, in any embedded system with a microprocessor inside.

Although there is no agreed scientific formula that links the degree of complexity of a piece of software and its number of lines of code, it is commonly accepted that, regardless of the programming language used, the higher the number of lines of code, the more complex it is.

Complexity in a software application is detrimental to its reliability. There will inevitably be bugs. Some of these bugs will create security vulnerabilities. Attackers exploit these vulnerabilities.[40]

Software applications are more and more voluminous in size. The following figure (Fig. 10.1) shows the approximate number of lines of code present in different versions of Microsoft Windows products[41]:

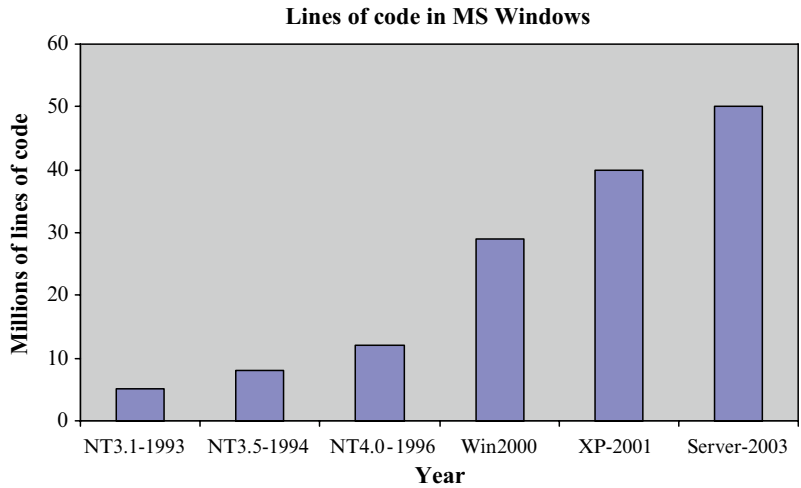

Fig. 10.1 Every new version of MS Windows has more lines of code that the previous one

[40] Attackers organise themselves in an industry. See Section 10.3.

[41] MS Windows figures adapted from http://en.wikipedia.org/wiki/Lines_of_code. Last accessed 5-11-2009.

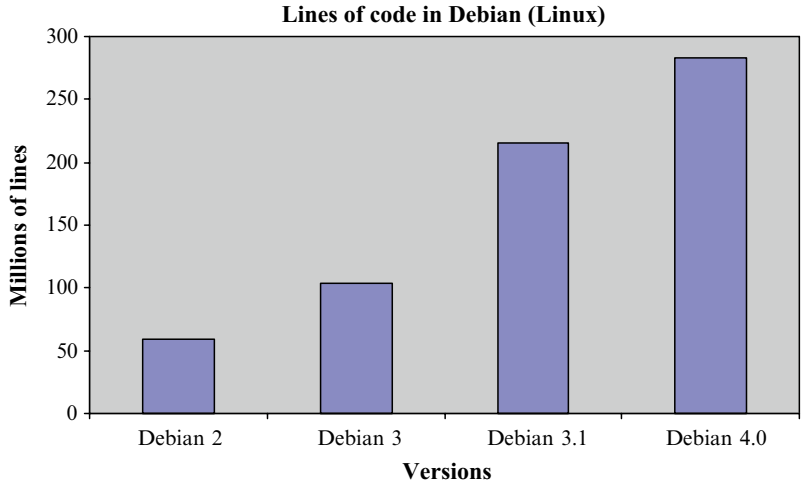

Fig. 10.2 The number of lines also increase in Debian Linux

And this figure (Fig. 10.2) displays similar information about versions of Debian Linux[42]:

Apart from the obvious appearance of new business and user requirements, we see three reasons for this increase of complexity in software:

- The unstoppable marketing trend to add more functionality, even if it is not demanded nor used by the vast majority of users.
- Functional requirements to interact with new pieces of also "longer" software.
- The generalised use of semi-automated development tools.

10.5.2 Complexity in the User Interface

How many mobile phone users get to know and use all the functionality that their devices offer them? How many Internet home users can configure a broadband router? How many people over 60 are able to use a personal digital assistant (PDA)? How many people over 70 are able to use a digital IT remote control?

The complexity of user interfaces is not only affecting the generalised acceptance of any IT device, it is also a common source of vulnerabilities. Non-IT literate users[43] find the secure configuration of the device difficult and, most of the times,

[42] Debian Linux figures adapted from http://en.wikipedia.org/wiki/Lines_of_code. Last accessed 5–11–2009.

[43] Sometimes, IT savvy users find difficulties as well.

they do not go through the painful process to harden their device, even if that could mean that they become easy targets for digital attackers.

Users of any type of digital device deserve the existence of a smart abstraction layer that would enable them to use the device in a way that they can pursue their duties and wishes without having to worry about security vulnerabilities, indecipherable warning messages, pop-up windows or any additional configuration detail.

In the future, IT will be faced with the market demand to create digital gadgets that are easier to use and secure by default.

10.6 A Possible Filtering Mechanism: Reputation Scores

The difficulty to assess whether a digital network flow is secure or, at least, whether it deserves any trust, is growing day after day. Experts foresee that, due to the impossibility to digitally confirm the trustworthiness of a network flow,[44] the future network security model will be based on the following three components:

- A secure network protocol able to protect the network flow in transit from eavesdropping and able to provide some certainty on the identity of the communicators.[45]
- A collection of distinct third parties that will act as guarantors of the reputation of the party initiating the communication.
- A local automated intelligence that will implement execution and data access control based on reputation-based input.

The way Internet entities, users and service providers, will build their reputation is still undefined. Nevertheless, there are already some application-centric initiatives that use reputation scores such as the "eBay top-rated seller" scheme.[46]

For example, a reputation granting service applied to a common tool such as email could work this way:

- Those Internet participants that invest in IT security and protect their email servers so that they are not used as relays to send spam[47] will enjoy a higher reputation level than those players with a laxer security stance.
- Email servers will accept emails coming only from those servers with a defined reputation level or higher.

[44] To provide total confidence or complete suspicion to the network flow.

[45] This means that the protocol will provide digital signing and encryption services.

[46] More information on this scheme at http://pages.ebay.com/topratedsellers/index.html. Last accessed 5-11-2009.

[47] According to a MessageLabs Intelligence Special Report, the global spam rate for September 2009 was 86.4%. Global Analysis Section. Available at http://www.messagelabs.co.uk/mlireport/MLI_2009Sep_Spam_US_FINAL.pdf. Last accessed 5-11-2009.

Reputation guarantors and Internet participants will require a secure configuration and maintenance service for their IT systems. These specialised services will be rendered by IT security professionals. We can think of two ways to implement reputation scores in entities connected to Internet:

– Formally, by respected service providers that will regularly check the trustworthiness of their customers.
– Informally, by social and professional communities acting as guarantors for their members.

In the future, the trustworthiness of services and Internet participants could rely on reputation scores granted by third parties or online social communities.

10.7 The Death of Personal Privacy

Privacy is "the quality of being secluded from the presence or view of others"[48] or "the freedom from unauthorised intrusion".[49] The day when personally identifiable information (PII) is publicly available to prying eyes has already arrived. In the coming years, this trend can only be more worrying. There are two circumstances that contribute to the "death of digital privacy":

– Vulnerable IT systems are hosting personal information. The risk that these servers are compromised is high.
– Many Internet users have a predisposition to make their personal information available to other participants in Internet applications such as social networks and other communities. This is due partly to the complexity of the interfaces that they use and partly to the misconception that a supposedly private Internet site is impregnable and it will remain that way.

10.7.1 Internet-Based Intelligence Collection

Public Internet search engines crawl the Internet and index most accessible elements, including personal data, as long as they are, or they were, available.[50] The types of formats that search engines can index are growing.[51]

---

[48] Definition from wordreference.com. Available at http://www.wordreference.com/definition/privacy. Last accessed 5-11-2009.

[49] Second definition from Merriam-Webster dictionary. Available at http://www.merriam-webster.com/dictionary/privacy. Last accessed 5-11-2009.

[50] We recommend to regularly search one's name and family name in Internet to check what others can learn from one's life.

[51] It is already possible to make basic image and video searches.

We foresee that Internet-based intelligence gathering services that big corporations are already using will be marketed and provided to final users as a detective measure to identify personal information, referring to them, that is publicly available.

The use of strong, but user-friendly, encryption will be a preventive measure that will also be popular to avoid access to personal information. So far, encryption has not reached a bigger market due to the lack of smart user interfaces that conceal its complexity to the non-IT literate user.

In the future, Internet users need to understand and prepare themselves for a scenario where any piece of information related to their person could potentially be available on the Internet to other parties. More user-friendly encryption and intelligence gathering services will be possible answers[52] *that the IT industry will provide to users on this respect.*

10.8 Critical Infrastructure Protection

The dependence on IT is also applicable to those infrastructures that are essential for the functioning of a country, a city or any human community. The number of supervisory control and data acquisition (SCADA) systems that are computer-based will grow. These systems control some of the most critical infrastructures present in modern countries, such as utilities, air and ground vehicles traffic control and health and social care systems.

The newest SCADA systems are based on the same vulnerable software that runs the Internet. Given the central role these systems have, their patching cycles are usually longer than those of non-critical systems. This means that they require additional security measures, since they will be vulnerable for longer time than standard systems.

In the future, the role of IT security in the protection of critical infrastructures will be more prevalent.

10.9 Change of the Security Paradigm: From an Onion to an Onion Ring

The following two principles are basic in IT security[53]:

- ***Defence in depth***: The implementation of a series of unrelated security measures, based on different mechanisms, to prevent a compromise of the system, in case one of the security layers fails.
- ***Protection of the crown jewels***: Allocation of resources to protect those assets that are more valuable.

[52] The first one is a preventive measure and the second one is a detective measure.

[53] See Section 4.2.

Traditionally, these two principles were graphically represented by the layers of an onion, i.e. overlaying coats that protect the core. The future brings a change of paradigm based on two facts:

10.9.1 Multi-organisational Value Chains

Organisations are progressively outsourcing and interweaving their business processes with third parties such as providers, suppliers and service providers. Every day it is more frequent to find value chains[54] in which different organisations participate and play equally important roles.[55] In terms of IT security, this means that some security layers will only be effective if they are implemented across all organisations taking part in the value chain.

10.9.2 Labour Market Events

The progressive move in modern societies' labour market from lifetime jobs to a collection of consecutive temporary work assignments, together with some generalised layoffs due to the financial crisis, are creating a high number of disgruntled employees and ex-employees. Some of them, especially those with no professional ethics and powerful system administration privileges, pose a real threat to the information assets of their organisations. For example, they could:

– Delete valuable data, including backups.
– Sell data to third parties, including competitors.
– Modify data required in critical business processes.

In the future, the disappearance of organisations' boundaries and the existence of serious internal threats change the protection paradigm from "the layers of an onion" to "an onion ring". Organisations continue to need a set of concentric and related security layers but they also have to establish strong internal security measures to mitigate the internal threat while they enable the smooth running of core business processes, some of them partly run by third parties.

Related to this forecast, in the future, organisations need to act and devise security measures that would enable them to continue making business even if they have already being hacked.[56]

---

[54] See Porter's Value Chain MBA model at the end of Chapter 8.

[55] IT boundaries among organisations are disappearing. This constitutes a new challenge for IT security.

[56] Conclusion extracted from listening to pauldotcom podcasts. Available at http://pauldotcom.com. Last accessed 6-11-2009.

10.10 IT Security for Virtual IT and for "The Cloud"

10.10.1 Virtualisation

The software industry has successfully revamped a concept that was already used in mainframes during the 1960s and 1970s in the past century, virtualisation. Software makers like VMware,[57] Microsoft[58] and Sun[59] offer the possibility to work with several installations of operating systems running all of them on a host operating system and sharing the same hardware platform, through the use of a virtualising hypervisor.[60]

Virtualisation reduces the time and the resources required to deploy new systems, both in organisations and at home. The next step for this technology has already reached the market: Legacy applications can also be virtualised and run on top of the latest operating systems.[61]

From the IT security viewpoint, there is a new field to explore and to eventually deliver value: The provision of security features required by those hypervisors to avoid virtual machine escaping[62] and unwanted communications among different virtual machines.

In the future, the use of virtualisation technologies will grow and virtualisation security will be an even more relevant field.

10.10.2 Virtual IT Infrastructure Services: Cloud Computing

Typically, IT systems required by organisations, like email, file servers and web services, resided in pieces of hardware that were located inside a computer room within the organisations' facilities. In the last years of the 20th century, many application service providers (ASPs), using the Internet as the main communication channel with their customers,[63] decided to offer a different business model.

---

[57] See http://www.vmware.com. Last accessed 3-11-2009.

[58] See http://www.microsoft.com/virtualization/en/us/default.aspx. Last accessed 3-11-2009.

[59] See http://www.sun.com/software/products/virtualbox. Last accessed 6-11-2009.

[60] More information on hypervisors at http://en.wikipedia.org/wiki/Hypervisor. Last accessed 6-11-2009.

[61] See some references at:

http://www.microsoft.com/systemcenter/appv/default.mspx

http://www.vmware.com/products/thinapp

Last accessed 3-11-2009.

[62] Virtual machine escaping is an IT attack that consists of directly reaching the hypervisor from the virtual machine, with the objective to obtain access to the host operating system.

[63] Salesforce and Peoplesoft (the last one, now Oracle) are two examples of ASPs. See http://www.salesforce.com. Last accessed 6-11-2009.

ASPs started to run business applications themselves so that customer companies did not require setting up their own application servers and, more importantly, their own IT support teams, avoiding fixed capital expenditure on hardware and human resources. Customers just had to connect to the business application through the Internet.

In the first decade of the 21st century, the possibility to start and run a business almost fully supported by IT systems provided by another company and located outside the office, in Internet, is already a reality.[64] Those IT services receive the notorious name of "the cloud".[65]

Using "cloud computing", an organisation could deploy an e-mail service for their employees in a very short time, without the need to install, commission and maintain their own IT servers.

"The cloud" offers an attractive value proposal to organisations but it also brings new IT security concerns:

- How well protected are corporate data in "the cloud"?
- Which confidentiality, integrity and availability[66] services does "the cloud" provide?

Organisations with critical corporate data are already making use of the cloud but, ideally, only for data that, if published or compromised, the future of the organisation will not be at stake.

In the future, SMEs and big companies will increase the use of information technology (IT) services provided by "the cloud". Those organisations making security-minded "cloud-related" decisions will have a greater possibility to survive and succeed.

10.11 Mobile IT Security

Together with mobile networks that are capable of transferring data at rates that make Internet browsing possible, mobile devices have also evolved. From being mere telephony gadgets with some basic personal digital assistant (PDA) functionality, they are currently closer in functionality to a personal computer than to a basic telephone.

The evolution of mobile phones brings definitely more complexity to the devices. They run their operating systems and, on top of that, their applications. This means that they require similar security measures to the ones implemented in netbooks,[67] laptops and desktop computers, such as antivirus, anti-malware software, personal firewalls and software updates.

---

[64] For example, see http://www.microsoft.com/online/products.mspx. Last accessed 6-11-2009.

[65] More on this term at http://en.wikipedia.org/wiki/Cloud_computing. Last accessed 3-11-2009.

[66] See Section 1.6.

[67] Netbooks are small-sized laptops, still with reduced features but with networking capabilities.

In the future, mobile security will become an expert field on itself,[68] *tightly coupled with the hardware layer (microprocessors) and the base software layer provided by the device manufacturer (from stable software kernels to security products that are already common in other devices such as firewalls and antivirus).*

10.12 Additional Leads on the Future of IT Security

IT security is a professional field of expertise that heads for becoming a comprehensive set of different technical disciplines (virtualisation security, "cloud" security, mobile security, etc.). All of them are certainly based on a set of basic security principles,[69] but they require deeply specialised technical knowledge.

In the future, technical IT security professionals will need to specialise themselves even deeper in very specific technical fields. The 'Renaissance model' of an IT security professional with expertise in all technical IT security fields will definitely disappear.[70]

We summarise additional features and topics that the near future could bring to IT security. This exercise provides a solid bedrock for present and future IT security leaders to establish their middle-term strategy.

10.12.1 Expert Forensic and Legal Support

The use of digital networks and systems to commit crimes, such as fraud, harassment, distribution of illegal pornography and identity and intellectual property theft, is already a tough reality.[71] Criminals use IT tools and digital networks to perform their evil plans.

When an IT related incident is reported within an organisation or to a law enforcement agency, an investigation takes place. The examination of the digital evidences, the IT elements involved in the crime, is part of any inquiry. IT security professionals specialised in computer and network forensics are essential to perform these investigations.

Forensics findings can only be used in court if they have been collected and preserved following the legal framework in force.[72] Therefore, it is essential to count on expert legal support, preferably coming from lawyers or legal advisors that have a sufficient knowledge of IT principles and elements.

---

[68] As it already happened with wireless IT security.

[69] See Section 4.2.

[70] See Section 2.2.

[71] See Section 10.3.

[72] Including guidelines about the chain of custody.

In the future, IT security professionals with network and computer forensic expertise will be more and more demanded, together with law specialists who can provide legal advice and would understand basic IT concepts.

10.12.2 The Importance of Laziness and Logs

We already mentioned how the addition of smart, and somehow "lazy", IT experts with knowledge on how to automate routine tasks, and willingness to script them, is optimal for IT security teams.[73] Log monitoring is a security task susceptible of being automated. The objective is to identify in the logs those events that require a security-related reaction.[74]

The decisive role that logs, created by all IT systems (desktops, servers, network devices), play in IT security monitoring tasks grows day by day. Just as their number and size. They keep on increasing their number and size.

A comprehensive approach to check and monitor all logs is not feasible anymore. They are too many, too spread around and too large. Log monitoring is too resource demanding, however, it will still be key to early incident detection. A new approach will start to be dominant:

In the future, organisations will actively monitor logs but only selectively, based on the specific knowledge of real threats affecting critical business processes.[75]

10.12.3 Risk Management and Decision Making

Organisations, advised by IT security professionals, will continue to manage IT risks. They will nonetheless require complementary traditional risk management methodologies[76] with more agile and fact-based techniques, based on the "micro-analysis of risks"[77] rather than on macro risk scenarios, which tend to be more useful for long-term strategies.

In the future, IT risk management will facilitate business decision making processes. To achieve this, current risk management methodologies will be balanced with "micro risk analysis". They will consider real, local and specific threat vectors, vulnerabilities and their possible impact to the business processes that organisations need to run to continue their existence.

---

[73] See Section 2.5.

[74] This reaction could be in the form of an alert, a warning or a simple message.

[75] Adapted from an interview in Spanish security magazine SIC to Santiago Moral, available at http://www.revistasic.com/revista62/entrevista00_62.htm. Last accessed 31-10-2009.

[76] See Section 1.7.

[77] Adapted from an interview in Spanish security magazine SIC to Santiago Moral, available at http://www.revistasic.com/revista62/entrevista00_62.htm. Last accessed 31-10-2009.

10.12.4 IT Security and the Threat of Compliance

Regulatory compliance requirements are a popular driver for organisations to create IT security teams.[78] Unfortunately, the threat of the creation of IT security teams, only to tick more boxes in a compliance sheet, and not to provide real value to the organisation, exists and it will grow.

In the future, dependable and successful IT security teams will utilise compliance as a useful argument to justify their actions but not as their ultimate purpose of being.

The Beauty of IT Security. An Attractive Field to Work In

IT security can hardly become a mere 9 to 5 job for years. Although possible, we discourage this approach and suggest to their followers, after a deep reflection, to find their passion and to work on what moves their emotions.[79]

The previous sections have introduced a future for IT security with more opportunities, but also greater challenges, in a more competitive context. We conclude with a collection of thoughts that could help those professionals who think that IT security can be a rewarding lifetime experience.

10.13 Creativity in the Social Realm of IT Security

Civilisations consist of human networks and social relationships. They are subject to wise and unwise decisions and they decline when their leaders stop responding creatively.[80] Our proposal for IT security professionals is to become creative within the field of expertise of IT security before it is too late for them and they might find themselves outside the labour market. This way, they will keep themselves fit for the coming challenges.

We identify the possibility to look for creative decisions in two dimensions, the social/human realm and the technical arena.

Within the social aspect of IT security, we distinguish two distinct targets of creative IT security measures: Human groups in general and the community of IT security professionals.

10.13.1 IT Security Creativity for Human Groups

Organisations are usually the ultimate recipient of the work done by IT security. And organisations consist of groups of human beings. The optimal way to deliver

[78] See, for example, Section 4.7.

[79] The intersection between passion, skills and the market is the right place to be.

[80] Toynbee (1987), pp. 366–370. See summarized information at http://en.wikipedia.org/wiki/Arnold_J._Toynbee. Last accessed 8-11-2009.

value from preventive, detective and mitigating IT security measures is to anchor those measures in features of the human nature. The following points are useful when IT security professionals design security awareness campaigns and try out social engineering[81] approaches to obtain information in the context of their security assessments.[82]

Scientists in the 21st century are studying the way human beings behave when they are confronted with varied stimuli. Thanks to the breakthroughs in functional magnetic resonance imaging, neuroscientists are able to see which areas of the human brain become active when individuals experience a variety of situations.[83]

We believe that the conclusions drawn by these neuroscience studies can also help improving the design of IT security measures that need to be accepted and actioned by human beings.[84]

Human beings can feel identically to another human being by simply observing or reading their satisfaction gestures.[85]

Human beings employ mimicry as an adaptive communication tool and, as such, it is influenced by the social context.[86]

Applying of these two learning points to IT security, we suggest social leaders to include attractive examples in mass media of sensible IT security measures that provide satisfaction to those individuals applying them. For example, a main character in a popular TV show displays signs of happiness and satisfaction after they realised that, although their laptop has died, all their data are available thanks to the daily backups they make. This scenario can bring more people to perform backups of their digital files than a dull paragraph in a thick IT security user manual.

Human beings possess a limited capacity to remember.[87]

The IT security steps that home users need to perform in their broadband routers and in their computers have to be simple, understandable and easily repeatable. In general, any IT security steps designed to be performed by non-IT users, at home or in any organisation, need to be clear and trouble-free.

As long as the software and the IT security industries deliver complex products and user procedures, there will be a high percentage of insecurely configured IT systems in homes and organisations. This is the reason why we postulate that, in all devices, their default configuration should already be secure (Image 10.2).

---

[81] Social engineering is the act of manipulating people into performing actions or divulging confidential information. Definition available at http://en.wikipedia.org/wiki/Social_engineering_(security). Last accessed 8-11-2009.

[82] See also Section 7.8.

[83] Lindstrom (2008), p. 8.

[84] For example, security awareness campaigns.

[85] Lindstrom (2008), p. 54.

[86] Adapted from Parkinson et al. (2008), Chapter 1.

[87] Adapted from Lindstrom (2008), p. 2.

Image 10.2 IT security should not be complex for the user

Human beings feel addiction and reward impulses much more intensely when they are triggered by indirect references.[88]

As an example, an explicit mentioning of a brand in a TV series triggers less purchase actions than a subtle use of the colours of their well-known logo in decisive moments of the plot. The application of this point to IT security is certainly subjective, but, maybe, worldwide recognised organisations, such as United Nations or the Organisation for Economic Co-operation and Development (OECD), could sponsor or launch basic security awareness campaigns considering this demonstrated fact.

These organisations would be in a position to create a simple colour-based logo, for example, a "basic security seal", that could be licensed to security processes and products that are easy to use and provide certain IT security leverage to their users. This way, consumers from all over the world would be able to identify the relevance of the "security seal" and they will eventually feel attracted to use products, or to follow procedures, that display the seal. Could we imagine a worldwide initiative to suggest the use of strong passwords to Internet users?

Cigarette warning labels fail to deter smoking. On the contrary, they raise the need to take one.[89]

A smart application of this learning point to basic IT security would require a deeper scientific study. Nevertheless, we would pose a question about the following scenario:

Most of the user-focused IT security policies highlight actions that can harm or create danger to the information of the user, and remind users not to perform those actions.

[88] Lindstrom (2008), p. 84.

[89] Lindstrom (2008), p. 15.

Similarly to the warning labels in cigarette packs, could these traditional policies maybe trigger a reaction in users that is opposite to the initial purpose of the policy?

10.13.2 Creativity for IT Security Professionals

Boring situations are common in any industry.[90] Fortunately, boredom in IT security is less common, due to the high number of activities to perform and the need to continuously learn new techniques[91] and contents. However, there are occasions, especially in big corporations, when IT security professionals can drown in bureaucracy, far away from the exciting IT security activities for which they were hired.

In cases of tedium, IT security professionals need to re-invent the position they hold. They need to increase the variety of work[92] and progressively add activities that could mean a win-win situation: They provide real value to their organisation while they improve their professional profile.

10.14 Creativity in the Technical Arena of IT Security

Those IT security professionals who feel more comfortable adding creativity to their technical sphere will also find windows of opportunity in the coming times. We mention two examples of technical creativity with very different purposes. The only limit to technical IT security creativity is actually the minds of the IT security professionals.

10.14.1 Cyberwar Weapons

Military research centres and military industry players in several powerful countries around the world are running a race against the clock to design, implement, test and deploy defensive and offensive IT-based tools for scenarios of cyberwar. These tools will be, if they are not already so, key in the information warfare arena.

The digital world is already an important front in current wars and its relevance in the future will increase.[93] IT security professionals will be required to staff future cyberwar related projects.

---

[90] Kroemer and Grandjean (1997), p. 219.

[91] See Section 6.9.

[92] Kroemer and Grandjean (1997), p. 233.

[93] As an example, the North Atlantic Treaty Organisation (NATO) has opened a centre of excellence on cyber defense in Estonia. News available at http://www.nato.int/docu/update/2008/05-may/e0514a.html. Last accessed 8-11-2009.

10.14.2 Digital Security Ants

Dealing with risks at a micro level is not only applicable to risk management methodologies, but also to technical scenarios such as malware detection, one of the greatest challenges for IT security in the coming years.

Several Universities[94] are researching on the possibility to create armies of digital processes, what they call "digital ants". They aim to replicate the social links that real ants[95] have between different types of basic digital processes. Each "digital ant" would focus on a specific task and, collectively, the joint work of these entities would facilitate the detection of abnormal activities in computers, caused by the infection with pieces of malware.

Innovative technical security initiatives, like the two ones presented in this section, will give shape to future technical IT security services.

This section concludes Chapter 10 and it also closes this book, where we have provided a multi-dimensional view on IT security management for the 21st century. We keep the hope that the input present in this book can help current and future IT security professionals becoming real IT "securiteers" and IT managers reducing the complexity that IT security brings to decision making boards (Image 10.3).

Image 10.3 The gate for IT "securiteers" to the 21st century IT security

[94] See news in Discovery Channel site, available at http://dsc.discovery.com/news/2009/10/28/digital-ants-computer.html. Last accessed 8-11-2009.

[95] Ants are social insects. They are highly organised and work collectively for their colony. See more information at http://en.wikipedia.org/wiki/Ant. Last accessed 8-11-2009.

Chapter 10: Learning points

- IT security is relevant because digital infrastructures such as the Internet are strategic assets for world trade and social prosperity.
- Small and medium enterprises (SMEs) require IT security services urgently.
- Fraudsters expand into the digital world because there is a high profit to risk ratio (PRR).
- IT security professionals need to analyse the latest IT security incidents and developments.
- The emergence of complexity in digital devices increases risks for all IT users.
- Reputation could be a way to provide trust to network flows and Internet entities.
- Insecure servers and security misconceptions of Internet users make privacy an almost impossible target.
- IT security will be essential to protect systems running critical infrastructures.
- The "onion layer" paradigm changes to an "onion ring" to cope also with the internal threat and the externalisation of core processes.
- Users of virtual IT and "the cloud" who are IT security aware will have a bigger chance to succeed.
- The possibility to be permanently online from complex mobile devices will give way to a specialised IT security field for mobile IT.
- IT security will need professionals with forensic expertise and legal experts with IT foundations.
- Monitoring and micro risk management will facilitate decision making processes in organisations.
- Compliance should be a trigger for an IT security team but not its main reason of being.
- The latest neurology studies can help increasing the acceptance of IT security measures targeted to human beings.
- The limit for creativity in the technical arena of IT security is only set by IT security professionals themselves.

Link to MBA Management Models

We have selected two MBA-related models. The first one is a tool to identify the stage of an industry lifecycle and the second one describes different types of change:

Industry lifecycle *(adapted from the product lifecycle model by P. Kotler, 1988)*
Placing time in the x axis and value in the y axis, the curve that represents the value of an specific industry usually adopts a Gaussian-alike function. The main stages of the industry lifecycle are:

- Introduction: Slow sales growth and very few companies.
- Growth: Increase in the number of companies and overall industry value.
- Maturity: Stable scenario with no more new players.
- Shake-out: Some companies die and some others grow. Time for the industry players to merge and consolidate.
- Decline: The value of the industry decreases. Probably a new industry starts its new introductory stage.

Different lifecycle stages require different strategies. Although there are many specific industries within IT security, most of them are still growing.

Patterns of strategic change *(by G. Johnson and K. Scholes, 1989)*
Strategic changes and changes in general in organisations tend to be one of these four types:

- Continuity: Tiny changes following the existing strategy
- Incremental: Small changes towards a different strategy
- Flux: Changes without a clear direction
- Global: Overall coordinated change throughout the organisation, typically as a response to a crisis

See reference: Harding and Long (1998).

Annex 1. Example of an Information Security Test

The following is an example test to assess knowledge of Chapter 1 of this book.

Duration: 25 min
Information Security. Vulnerabilities, threats and risks in IT.
Consider the following picture (Image A1):

Image A1 On the top of a waterfall

Imagine that a team of explorers navigate along a river and they reach a waterfall like the one depicted in Image A1. They could not know about the existence of the waterfall because their competitors modified the explorers' maps the night before, deleting all signs of waterfalls.

Please answer each question selecting only the option that you consider it is the best answer.

1 A threat for the explorers is that:

A The river stream leads their boat to the waterfall.
B The boat is made of wood.
C The boat is fully loaded.
D The river is really noisy.

2 A vulnerability of the explorers is:

A The river stream leading their boat to the waterfall.
B The fall of their boat from the upper side of the waterfall.
C Their lack of experience with waterfalls.
D The excessive load of the boat.

3 A risk for the explorers is that:

A The strength of the river stream.
B The excessive weight of the boat.
C The river stream brings their boat to the waterfall and they fall off the cliff.
D The height of the waterfall.

4 The explorers could not learn more about waterfalls before their trip because:

A Maps are usually not available to prepare a trip.
B Maps are confidential and explorers cannot consult them.
C Maps' integrity was not kept during the night prior to the trip.
D Maps usually contain no indication of waterfalls.

5 Who would ultimately set the 'appetite for risk' of the explorers?

A The sponsors of the explorers will eventually decide the risk that the explorers will run.
B The explorers themselves will eventually decide whether they jump off the boat or remain in it.
C The sponsors and the explorers will decide as a collective body.
D Neither the explorers nor their sponsors decide which risks they will run.

6 Someone deleted all signs of waterfalls printed in the explorers' map:

A This was a direct attack towards the explorers.
B This was an attack against the availability of the map.
C This was an attack against the confidentiality of the map.
D This was an attack against the integrity of the map.

Please answer also the following generic questions:

7 The information property that provides guarantee on the originator of the information is called:

A Non-authorisation.
B Non-mediation.
C Non-repudiation.
D Non-spoofing.

8 The organisation's risk appetite

A Is the combination of information confidentiality, integrity and availability.
B Is the combination of information risks, threats and vulnerabilities.
C Is the valid information management will provide on which risks are accepted and which ones are not.
D Is the valid information management will provide on which threats are accepted and which ones are not.

9 Any specific risk can be described in

A A probability-impact graph.
B A threat-impact graph.
C A threat-vulnerability graph.
D A probability-vulnerability graph.

10 Information risk management

A Is a business process that depends on the confidentiality of the documents on the organisation.
B Is a business process that depends on the integrity and availability risk the organisation is willing to take.
C Is a business process that depends on the functionality of the system.
D Is a business process that depends on the risk that the organisation is willing to take.

End of test

Solutions:
1 A
2 C
3 C
4 C
5 B
6 D
7 C
8 C
9 A
10 D

Annex 2. Security Incident News Example

We present a "partially anonymised" example of IT security incidents that reached media in the last months.[1] Distributing similar news within the organisation will show that real incidents are currently happening throughout the world. This is a fact-based instrument to raise security awareness among colleagues in the organisation:

- A public report from a reputable scientist postulates that an attack on a small power subnetwork could trigger a cascading effect and affect an entire population area. (SANS Newsbites citing a computerworld news).
- Country X issues a draft e-security code to help Internet Service Providers protecting their users.
- New scam adds live chat to phishing attack. Online scammers have created a phishing site masquerading as a US-based bank that launches a live chat window where victims are tricked into revealing more information (from news.cnet.com).

And more headlines:

- Man charged in data theft trojan and botnet case.
- Prison sentence for obtaining personal data through peer-to-peer software.
- Country X faces cyber threats from country Y and Z.
- Unencrypted laptops containing confidential information lost by governmental institution.
- Infected USB flash drives break havoc at hospital X.
- Ads available at a newspaper website serve scareware.
- Servers stolen from company X's computer centre.
- Impersonation in a social network the cause of a teenager suicide.
- Tenths of millions of credit card stolen through an insecure wireless corporate network.
- Two convicted for refusing to decrypt data.

[1] Adapted from Sans Newsbites (available at http://www.sans.org/newsletters/newsbites. Last accessed 20-09-2009), Computerworld and Cnet news.

- Executive resigns after disclosing inadvertently State secrets.
- Employee accused of hacking their company's servers.
- Internet scammers take advantage of great singer's death.
- Building company sues online bank for insufficient preventive security measures after losing some thousands of dollars.

Annex 3. IT Security Starter Kit

The following references are a good starting point for IT graduates who intent to devote their efforts to the field of IT security. The content behind these links could help them reaching their first trainee or junior position within a professional IT security team.[2]
Master the command-line in operating systems such as:

- MS Windows flavours
- Linux (scan http://distrowatch.com for different distributions)
- Discover http://blog.commandlinekungfu.com

Script your own code using languages such as Linux shell script, perl, python, etc.
Scrutinise IT security related sites websites such as:

- http://paultdotcom.com
- http://sans.org
- http://www.securityfocus.com
- http://www.milw0rm.com for vulnerabilities and exploits

Follow IT security podcasts such as:

- http://pauldotcom.com/security-weekly
- http://www.securabit.com
- http://cyberspeak.libsyn.com

Visit IT security companies sites such as:

- http://inguardians.com
- http://www.mitnicksecurity.com
- http://www.s21sec.com (partly in Spanish)

Read IT security papers from:

- http://www.sans.org/reading_room/
- http://www.owasp.org/

[2] The last time these references were accessed was on 11-11-2009.

Enjoy videos and slides from:

- http://www.blackhat.com
- http://defcon.org
- http://irongeek.com

Download and learn how to use tools like:

- http://nmap.org (also available at http://insecure.org)
- http://www.metasploit.com
- http://www.snort.org
- http://www.nessus.org/nessus
- http://technet.microsoft.com/en-us/sysinternals/default.aspx

About certifications, have a look at:

- http://www.giac.org (start with GSEC)
- http://www.eccouncil.org/ceh.htm

Other suggested blogs are:

- http://taosecurity.blogspot.com
- http://www.liquidmatrix.org/blog
- http://elladodelmal.blogspot.com (this one, in Spanish)
- http://laramies.blogspot.com
- http://www.social-engineer.org
- http://securityandrisk.blogspot.com

And finally, a high-tech thriller novel: “Deamon” by Daniel Suarez (2009). Published by Penguin.

Index of MBA Models Referenced at the End of Every Chapter

Chapter 1

- PESTLIED.
- The 7 'S' framework.
- SWOT analysis.

Chapter 2

- Belbin's team roles.
- Group development.

Chapter 3

- Herzberg's hygienic and motivational factors.
- Maslow's hierarchy of needs.

Chapter 4

- VMOST.
- Porter's generic strategies.
- Porter's 5 forces.
- Ansoff matrix.

Chapter 5

- Demand and supply.
- Economies of scale.
- Stakeholder analysis.

Chapter 6

- Action-centered leadership.
- Managerial grid.

Chapter 7

- Customer bonding: the seven key stages.
- Marketing promotion instruments.
- Customer lifetime value.

Chapter 8

- Value chain.
- Strategic triangle.

Chapter 9

- Four organisational cultures.
- Organic vs. mechanistic management styles.

Chapter 10

- Industry lifecycle.
- Patterns of strategic change.

References

Aabo, T., Fraser, J.R.S., Simkins, B.J.: The rise and transformation of the chief risk officer: a success story on enterprise risk management, version of December 10, 2004. Revised version available in J. Appl. Corporate Finance, Winter 2005, pp. 1–34. http://www.gloriamundi.org/detailpopup.asp?ID=453057237 (2009). Accessed 15 Sept 2009

Albrechtsen, E., Hovden, J.: The information security digital divide between information security managers and users. Comput. Secur. **28**, 476–490. Published by Elsevier (2009)

Appel, W.: Redefining IT governance readiness. Meta Group, Meta Practice 2369, pp. 1–8 (2005)

Ariely, D.: Predictably Irrational. Harper Collins, New York (2008)

Atkinson, M.: Lend Me Your Ears: All You Need to Know About Making Speeches and Presentations (Chapter 11). Oxford University Press, New York (2005)

Basel Committee on Banking Supervision: Sound practices for the management and supervision of operational risk. Risk Management Group, Cole, R., et al. (chairman), Bank for International Settlements (BIS), pp. 2–5 and 8 (2003)

Birchall, D., Ezingeard, J.-N., McFadzean, E.: Information Security. Setting the Boardroom Agenda. Grist and Henley Management College sponsored by Qinetiq, pp. 1–51 (2003)

Birchall, D., Ezingeard, J.-N., McFadzean, E.: Information Assurance. Strategic Alignment and Competitive Advantage. Grist and Henley Management College sponsored by Qinetiq, pp. 1–73 (2004)

Bird, D.: Commonsense Direct Marketing, 4th edn. Kogan Page, London (2000)

Blythe, J.: Principles & Practice of Marketing. TL EMEA Higher Education, p. 204. London (2006)

Bolton, N., Berkey, J.: Aligning Basel II operational risk and Sarbanes-Oxley 404 projects. In: Davis, E. (ed.) Operational Risk: Practical Approaches to Implementation, Chapter 12, pp. 237–246. Risk Books, London (2005)

Carey, A.: 2005 Global Information Security Workforce Study. IDC Whitepaper, sponsored by ISC2, pp. 1–28 (2005)

CAS Casualty Actuarial Society: Overview of Enterprise Risk Management, p. 6 and 8. Enterprise Risk Management Committee, CAS, Arlington (2003)

Coles, R.S., Moulton, R.: Operationalizing IT risk management. Comput. Secur. **22**, 487–492 (2003). 0167-4048/03

COSO: Enterprise risk management framework – Executive summary – Exposure draft for public comment, pp. 1–103. Downloadable after purchase from http://www.coso.org/-ERM.htm, draft retrieved 2006 (2004)

Damasio, A.R.: Descartes' Error: Emotion, Reason, and the Human Brain (Introduction). Putnam, New York (1994)

DeLotto, R., McKibben, D., Leskela, L.: Risk Management in the New Regulatory Environment, pp. 1–4. Gartner, Research note 19 March 2003', COM-19-4409 (2003)

Dillon, R.L., Paté-Cornell, M.E.: Including technical and security risks in the management of information systems: a programmatic risk management model. In: Systems Engineering, 8.1, Regular paper, p. 15, 17, 18 and 24. Published by Wiley Periodicals (Malden, MA, USA) (2005)

ENISA European Network and Information Security Agency: A Users' Guide: How to Raise Information Security Awareness, p. 52. ENISA (2006)
ERMC: Enterprise Risk Management Committee, Overview of enterprise risk management, Casualty Actuarial Society. Downloadable at http://www.casact.org/research/erm/overview.pdf, retrieved 2009-09-15, p. 10 (2003)
Ezingeard, J.N., McFadzean, E., Birchall, D.: Mastering the art of corroboration: a conceptual analysis of information assurance and corporate strategy alignment. J. Enterprise Inform. Manage. **20**(1), 96–118 (2007)
Frost & Sullivan: The 2008 ISC^2 Global Information Security Workforce Study, p. 6. Available at http://www.isc2.org/uploadedFiles/Industry_Resources/2008_Global_WF_Study.pdf, retrieved 23-4-2009 (2009)
Gargallo, P.: Spanish sculptor and painter (1881–1934). His sculpture "The Prophet" is displayed, among other locations, in the Reina Sofia Museum in Madrid (Spain)
Giuliani, R.: Leadership (Contents). Little Brown, London (2002)
Gladwell, M.: The Tipping Point: How Little Things Can Make a Big Difference, p. 132. Little Brown, Boston (2000)
Glen, P.: Leading Geeks: How to Manage and Lead People Who Deliver Technology, p. 16. Wiley, New York (2003)
Griffin, J.: Customer Loyalty: How to Earn It, How to Keep It, 2nd edn. (published in 2002), pp. 202–215. Wiley, New York (1995)
Gronroos, C.: Relationship marketing: strategic and tactical implications. Manage. Decis. J. **34**(3), 5–14. Published by MCB UP (1996)
Hamel, G.: The why, what and how of management innovation. Harv. Bus. Rev. pp. 1–12 (February 2006)
Harding, S., Long, T.: MBA Management Models. Gover, England, pp. 84, 181 and 187 for Chapter 1, pp. 105–108 and 109–112 for Chapter 2, pp. 161–163, 197–199, 59–63 and 73–76 for Chapter 4, pp. 17–20 and 21–24 for Chapter 5, pp. 101–103 and 121–124 for Chapter 6, pp. and 191–194 and 95–98 for Chapter 8, pp. 149–153 and 169–172 for Chapter 9 and pp. 211–214 and 173–176 for Chapter 10 (1998)
Herzberg, F.: One more time: how do you motivate employees? Harv. Bus. Rev. **46**, 53–62 (1968)
ISO: ISO Guide 73 – Risk management – Vocabulary – Guidelines for use in standards, Reference: ISO/IEC GUIDE 73:2002(E/F), pp. 1–16 (2002)
ISO: ISO/IEC 13335-1 Information technology – Security techniques – Management of information and communications technology security. Part 1: Concepts and models for information and communications technology security management, Reference: ISO/IEC 13335-1:2004(E), pp. 1–28 (2004)
ISO: ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements, First edition, Reference: ISO/IEC 27001:2005(E), pp. 1–115 (2005)
Kahneman, D., Tversky, A.: Choices, Values and Frames. Cambridge University Press, New York (2000)
Kotler, P.: Marketing Management, International edition, 11th edn, pp. 443–452. Prentice Hall, New Delhi/Upper Saddle River (2003)
Kotler, P., Kartajaya, H., Young, S.D.: Attracting Investors: A Marketing Approach to Finding Funds for Your Business, pp. 181–183. Wiley, Hoboken (2004)
Kroemer, K.H.E., Grandjean, E.: Fitting the Task to the Human: A Textbook of Occupational Ergonomics. Taylor & Francis, London (1997)
Leavitt, H.J., Pondy, L.R., Boje, D.M.: Readings in Managerial Psychology, 4th edn, pp. 669–671. University of Chicago Press, Chicago (1989)
Lee, S., Hattemer, R.: Marketing lectures prepared for the Henley Management College MBA (2006) and Frankfurt School of Business and Finance (2006). Set of slides 1 to 5
Lindstrom, M.: Buyology: Truth and Lies About Why We Buy, Foreword by Underhill P. Broadway Books. Crown Publishing Group (New York, USA) (2008)

Long, J., et al.: Penetration Tester's Open Source Toolkit, pp. 2, 3 and 96. Syngress, Canada (2006)
Lupien, S.J.: Stress, memory and aging, Conference at the Douglas Mental Health University Institute, Ph.D. Montreal University, Canada. Video available at http://www.smartplanet.es/redesblog/?p=452, retrieved 20-08-2009 (2007)
Mallol, E.: Las lecciones de los lideres, Lessons of leaders, published in Spanish by Editorial Planeta Empresa, Escuela de empresarios fundacion de la Comunidad Valenciana (EDEM), p. 72 (for Section 3.1), p. 129 (for Section 3.2) and p. 202 (for Section 3.6 and Section 3.12) (2008)
Maslow, A.: Motivation and Personality, 3rd edn. Harper & Row, New York (1954/1987)
May, C.: Risk management – practising what we preach. Comput. Fraud Secur. **8**, 10–13 (2002)
McClure, J.: In: McClure, S. (ed.) How to Find Your Dream Job and Make It a Reality: Solutions for a Meaningful and Rewarding Career, p. 154. Trafford Publishing, British Columbia (2003)
McCorkell, G.: Direct and Database Marketing, p. 68. Kogan Page, London (1997)
McFadzean, E., Ezingeard, J.-N., Birchall, D.: Boards of Directors' engagement with information security. Henley Management College, Working Paper Series, HWP 0309, pp. 1–25 (2003)
NIST: Risk management guide for information technology systems. National Institute of Standards and Technology NIST (Technology Administration, U.S. Department of Commerce), Recommendations, Special publication 800-30 by Stoneburner, G., Goguen, A., Feringa, A., pp. 1–F1 (2002a)
NIST: Security guide for interconnecting information technology systems. National Institute of Standards and Technology NIST (Technology Administration, US Department of Commerce), Recommendations, Special publication 800-47 by Grance, T., Hash, J., Peck, S., Smith, J., Korow-Diks, K., p. 3–3 and 5–2 (2002b)
NIST: Guideline on network security testing. National Institute of Standards and Technology (NIST), Recommendations, Special publication 800-42 by Wack, J., Tracy, M., Souppaya, M., p. 3–13 and 3–14 (2003)
Nobokov, V.: Strong Opinions (Foreword), p. 3. McGraw-Hill, New York (1973)
OECD, Organisation for Economic Co-operation and Development: Implementation plan for the OECD guidelines for the security of information systems and networks: towards a culture of security. Working Party on Information Security and Privacy, 2 July 2003, pp. 1–6 (2003)
Öst, L.G., Breitholtz, E.: Applied relaxation vs. cognitive therapy in the treatment of generalized anxiety disorder. Behav. Res. Ther. **38**, 777–790 (2000)
Parkinson, B., Marinetti, C., Moore, P., dos Anjos, P.L.: Chapter 1: Emotions in social interactions: unfolding emotional experience. Emotions in Social Interactions: Construction of Emotion Experience. Available at http://cfpm.org/~pablo/anjos,humaine_chapter.pdf (2008)
Poor, M.: SANS training in 2007 – 503: Intrusion detection in-depth (GCIA), see http://www.sans.org/training/description.php?mid=43, retrieved 23-4-2009 (2007)
Punset, E.: The Happiness Trip. Chelsea Green, White River Junction (2007)
Rinnooy Kan, A.H.G.: IT governance and corporate governance at ING. Inform. Syst. Control J. **2**, 26–31 (2004)
SANS: SANS 2008 Salary & Certification Survey, Rob Kolstad of Delos Enterprises on behalf of the SANS Institute, p. 0. Available at http://www.sans.org/resources/salary_survey_2008.pdf, Retrieved 23-4-2009 (2009a)
SANS: The top cyber security risks. Data from Tipping Point and Qualys and input from Ed Skoudis and Rob Lee. Available at http://www.sans.org/top-cyber-security-risks/, Retrieved 20-09-2009 (2009b)
Scholtz, T.: Articulating the business value of information security. Security & risk strategies, security infusion, global networking strategies. Meta Group, Meta Delta **2774**, 1–4 (2004)
Sheffi, Y., Rice Jr., J.B.: A supply chain view of the resilient enterprise. MIT Sloan Manage. Rev. **47**(1), 45–47 (Fall 2005)
Thompson, J., Martin, F.: Strategic Management (Military strategy revisited) 5th edn, pp. 399 and 400. Thomson, London (2005)

Torrington, D., Hall, L., Taylor, S.: Human Resource Management, 5th edn. Pearson Education, London (2002)

Toynbee, A.J.: A Study of History, vol. 1: Abridgement of Volumes I–VI, pp. 366–370. Oxford University Press, New York (1987)

Van Vugt, M., Hogan, R., Kaiser, R.: Leadership, followership, and evolution: some lessons from the past. Am. Psychol. **63**, 182–196. Interview by Eduard Punset, video available at http://www.eduardpunset.es/index.php?vim=48, Retrieved 15-09-2009 (2008)

von Solms, B.: Information security governance: compliance management vs operational management. Comput. Secur. **24**, 443–447 (2005)

West, R., Turner, L.H.: Understanding Interpersonal Communication: Making Choices in Changing Times, p. 274. Cengage Learning, Boston (2008)