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 ISC² 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)

http://www.springer.com/978-90-481-8881-9

IT Security Management
IT Securiteers - Setting up an IT Security Function
Partida, A.; Andina, D.
2010, XXXV, 247 p., Hardcover
ISBN: 978-90-481-8881-9