Summary of National Reports on IS

Document Details:	
Reference	**INSEMOT SME**
WP/Activity	WP 2 - Reports on IS
Author(s)	Handwerkskammer Münster
Character	National Reports & Summary
Date	09.01.2012

Education and Culture DG
Lifelong Learning Programme

Table of Content

PART I - Summary of all National Reports

PART II - the National Reports

PART I - Summary of all National Reports

0) Aim of the Report

Information and eventually knowledge are vital capital for each company and most important for the capacity to compete. Therefore especially the security of information and knowledge should be of general concern to each company. Further more, as companies and organisations store not only company related but also personal related information the legislator shares interests in questions of information security and data protection. Due to structure and organisation, bigger companies are generally better organised in managing necessary processes. Smaller companies on the contrary quite often show a lack of necessary competences.

Against this background the aim of this report is to provide an overview of the demands and needs small and medium sized enterprises (SME) are facing while implementing Information Security Management (ISM).

In this regard, an overview of national rules and regulations concerning Information Security (IS) relevant for SME will be given. Next qualification offers covering this topic will be identified and their suitability for SME will be estimated. Further more the current situation of SME e. g. regarding their general structure, implementation of Information Security Management, qualification needs of responsible persons will be described. Against this background a possible profile of an "Information Security Officer in SME" will be drafted.

Definition of Terms

As the terms Information Security, Computer Security and Information Assurance are frequently incorrectly used interchangeably the definition of the terms Information Security and Information Security Management used within this report will be clarified here. Furthermore the term Small and Medium Sized Enterprises will be used in accordance to the EU definition:

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Information Security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms. (Reference: http://en.wikipedia.org/wiki/Information_security, 04.11.2011)

An information security management system (ISMS) is a set of policies concerned with Information Security Management or IT related risks. The idioms arose primarily out of ISO 27001.

The governing principle behind an ISMS is that an organization should design, implement and maintain a coherent set of policies, processes and systems to manage risks to its information assets, thus ensuring acceptable levels of information security risk. (Reference: http://en.wikipedia.org/wiki/Information_security_management_system, 04.11.2011)

Small and Medium Sized Enterprises

Enterprises qualify as micro, small and medium-sized enterprises (SMEs) if they fulfil the criteria laid down in Recommendation 2003/361/EC which are summarized in the table below. In addition to the staff headcount ceiling, an enterprise qualifies as an SME if it meets either the turnover ceiling or the balance sheet ceiling, but not necessarily both.

Enterprise category	Headcount	Turnover	Balance sheet total
medium-sized	< 250	≤ € 50 million	≤ € 43 million
small	< 50	≤ € 10 million	≤ € 10 million
micro	< 10	≤ € 2 million	≤ € 2 million

(Reference: http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/sme-definition/index_en.htm, 08.11.2011)

1) Resume of the National Reports

An international comparison shows that the vast majority of enterprises are SMEs in all member states of the EU. With a total of 20.7 million small and medium-sized companies represent 99.8% of all businesses. Almost 92% of all enterprises were micro businesses with fewer than 10 employees.

The main common characteristics of SME and their attitude to Information Security Issues are:

- SME usually do not have full-time IS staff respectively staff skilled in data processing (DP);
- SME suffer of a lack of time, money and know-how in regard of IS and data protection in combination with a lack of transparency of cost-benefits;
- SME usually do not have in place appropriate protocols for safeguarding confidential data and organize IS most likely on ad-hoc basis, often in response to security breach that has already occurred;
- Most SME are family owned.

Exceptions are SME operating in a sector were IS is a priority or if the owner / managing director has prior experience of information security.

Considering these characteristics, partners believe the training should be directed at the owner respectively manager or managing director of the business. The prerequisites of this target group can be summaries as follows:

- Unlikely to possess any formal qualification in the area of IS and DP
- IS procedures are unlikely to be in place
- A general awareness of the relevance of IS issues is not to be assumed.

Regarding the specific national situation, partners came to the following conclusions:

Austria

According to a study on IS in small and medium sized enterprises a main reason for the insufficient implementation of safety measures is a lack of safety awareness. Other problematic factors are costs, time and a lack of transparency of cost-benefit. The lack of decision-making support and the indicated complexity of IS systems make it clear that there is a need for a comprehensive information platform and specific training in SMEs.

Czech Republic

The sphere of general security awareness is something on which organizations should concentrate over the next few years. Since 1999 the proportion of companies which perceive this issue as one of the key obstacles to the future development of IS in the Czech Republic has increased steadily. At the same time very few companies have introduced a functional program aimed at increasing security awareness.

Germany

A lack of resources, especially time, money and professionally trained staff, as well as a lack of information are the reasons that ISM has yet to be implemented in SMEs. The focus of the companies lies on the economically most relevant business processes. Many

companies still do not seem to be sufficiently aware of the importance of internal data processing for these business processes.

Therefore, the objective of the INSEMOT SME project should be to assist companies in establishing inwardly and outwardly directed processes and practices in order to protect trusted assets and information against security incidents. Crucial for an effective and efficient ISM is knowledge of most critical business processes and their relevant contact points with data processing.

Spain

The main objective of INSEMOT SME should be raising awareness of both, SMEs and public organisations. The main target group are senior managers. Awareness and understanding are essential for good business practices and are referred to as prerequisites in various international standards such as ISO 27001.

Ireland

Concluding the findings of the report, the creation of a short online questionnaire which acts as summary risk assessment audit for the training participants is recommended. Further more it should be considered that many business with the target group will not have IS procedures in place and may demonstrate limited understanding of their obligations under relevant IS and data protection legislation. It is likely that many companies have little or no interest in implementing IS procedures, occupied as they are with what they consider to be more pressing business concerns. It is also likely that the owner/manager will be time-poor and will not have the resources to research and address IS findings. It may also be possible that the owner/manager will not have the financial resources to act upon the findings of and IS audit.

Italy

The analysis conducted shows that a profound change is underway. New opportunities, unfortunately, are seen only by a very small part of the Italian economy and businesses. The result is that actors of the production system resorting to IS are still patchy and mainly undertaken by large companies and an objectively modest number as regards SMEs.

There is also a need to bridge the mismatch between supply and demand for training programmes, tailored to organizational, size and cultural characteristics of small businesses, filling an "open" space with the development and provision of training products/programmes that provide adequate depth and systemic vision of information security, and at the same time, provide the key elements of knowledge to guide the small business owner to introduce and manage proper data and business information security policies.

2) National Rules & Regulations Concerning Information Security in SME

The partners were asked to give an overview of relevant national rules and regulations concerning Information Security in small and medium sized enterprises (SME). In addition to national rules and regulations the European Standard Family ISO 2700x is to be considered within the context of all National Reports.

The comparison of results show Information Security and Data Protection requirements are reflected in different national rules and regulations.

Austria

In Austria basically the Data Protection Act (Datenschutzgesetz) is to be considered regarding Information Security Management within enterprises. Amongst others the Data Protection Act regulates the confidentiality of personal data, duties of companies storing data as well as requested data security measures.

Czech Republic

The National Information Security Strategy is approved by Government Resolution CZ No. 1340/2005 and developed based on the task of the State Information and Communications Policy eČesko 2006 in accordance with the laws of the Czech Republic and EU and for the field of information security.Methodology of the provision, implementation and operation, monitoring and maintenance of information security management system (hereinafter referred to as ISMS - Information Security Management System) in the organization. Simply said, the ISMS is only one and one that is described in ISO / IEC 27001.

Germany

In Germany a number of rules and regulations covering Information Security Management in enterprises are to be divided in 3 application areas: due diligence of companies, consumer protection and data privacy protection. Due diligence refers to the fact that deficiencies in information security can cause serious damage. Consumer protection is aimed to regulate consumer's duties and rights while using Information and Communication Technologies (ICT). Data privacy protection refers to the protection of individual before the abuse of personal data.

Spain

In Spain the legal framework concerning Information Security is based on four laws, the Ley Orgánica 15/1999, Real Decreto 1720/2007, Directive de la Unión European 95/46/CE and Ley 34/2002. The requirements derived from this rules and regulations allow companies to identify potential threats, their impact and efficient responses.

Ireland

The main Irish law dealing with data protection in SMEs is the Data Protection Act 1988. The Act was amended by the Data Protection (Amendment) Act 2003 which brought Irish law into line with the EU Data Protection Directive 95/46/EC. In order to comply with the terms of the Act a data controller, carrying the main responsibility for the creation of a safe environment for the processing of personal data, or data processor, responsible to

keep personal data secure from unauthorised access, disclosure, destruction or accidental loss, can be required.

Italy

The Italian ICT sector regulatory framework is in constant and rapid evolution. Among the most significant legal issues is the Law of 18th March 2008, No. 48, with which Italy ratified the Council of Europe Convention. Further more the Privacy Code (Decree Law No. 196/03) imposes strict security measures to control anyone who comes into contact with personal or sensitive data. Additionally Decree Law of 29th November 2008, No. 185 regulates the use of certified e-mail addresses. The Copyright Law 248/2000, the Industrial and Intellectual Property Decree Law 30/2005 and the Administrative transparency Decree Law No. 231/2001 are to be considered within this context.

3) Vocational and Continuing Education and Training

Two of the objectives of the INSEMOT SME project are the establishing of a web based information service directed at SME as well as a qualification offer meeting the current needs of SMEs in the field of data protection. Before this background partners were asked to identify and describe services and qualifications available on the national market and to estimate their suitability for SMEs.

3.1) Overview of Existing Training Offers in the Field of Information Security

The partners were asked to identify and describe qualifications covering Information Security. A short description of the content covered, required prerequisites and testimonials to be achieved was asked for.

A detailed description of the available offers will be found in the complete National Reports. Summing up can be noted that the majority of trainings addresses IS and or IT professionals.

Austria

The Data Protection Act in Austria does not require a data protection officer. However 3 comprehensive and a serious of 1-day seminars covering the topics "Information Security Management", "Information Auditor", "Data Protection Officer" and "Information Security basics" could be identified.

Czech Republic

For Czech Republic two comprehensive qualifications could be identified, the "Information Security Manager", providing key elements on ISO 27001, and the "Internal Information Security Auditor" preparing the company for external audits.

Germany

In Germany a variety of qualifications and trainings is available covering the topics data privacy protection, information security, IT security, Implementation of ISO 207001, rules and regulations on data protection, etc. Nevertheless, one important finding of the research is that employees of SME, who in addition to their regular jobs also are responsible for IT and Information Security, are addressed by these offers only in rare cases.

Spain

For Spain also a variety of qualifications could be identified, covering for example ICT Management, Information Security Management, Data Protection, IT-security. Some courses explicitly address professionals, some courses address SME but require a general understanding of the covered concepts and ideas.

Ireland

For Ireland three courses on academic level could be identified. 2 courses address undergraduate degree holders and lead to a Master in Computing in IS & Digital Forensics respectively to a Master of Engineering in Information and Network Security. The third qualification addresses IS professionals leading to a postgraduate certificate and diploma in Information Security.

Italy

The qualifications identified for Italy cover basically professional trainings on academic level and address IS and IT professionals. Two training providers, the ISACA – Information Systems Audit and Control Association as well as the University "La Sapienza di Roma" are named as most important actors. Basic references for the trainings are the EUCIP – European Certification of Informatics Professionals and the European e-Competence Framework (e-CF).

3.2) Overview of Existing Services Regarding Information Security

The picture of existing IS information services is somewhat more inconsistent. Information services addressing a wider audience to solely addressing IT and IS professionals are available within partnering countries. General information usually offered for free via Internet. More sophisticated services might be a subject to fees.

Austria

Besides a number of freely accessible websites providing information specifically for SMEs also fee-based services are available. Experts in information security provide consulting and analysis of the existing security system and assist companies in planning and implementing security measures.

Czech Republic

The Czech Institute of Information Security Management offers a fee-based service. In addition to exclusive conferences and networking information directly from practice are provided.

Germany

In Germany, as in Austria, a number of freely accessible websites provide information as well as fee-based services are available. As already mentioned above, not all of the available offers and services meet the needs and consider the prerequisites of SMEs but basically address professionals or persons with considerably previous knowledge.

Spain

In Spain S21SEC is one of the relevant service providers regarding Information Security. Services are categorized with regard to company size. Some are especially directed at companies with less than 50 employees. Topics covered are compliance, technical auditing, e-crime-incident management, outsourcing etc. In addition a web portal offers an overview of companies offering security services.

Ireland

For Ireland 4 main providers could be identified, two of them offering free web services and two charging membership fee.

Italy

Basically three providers offer information services regarding Information Security especially designed for SME. A variety of topics and services is covered, e. g. technical guides, practical tips, IT security, certifications, networking up to the provision of IT resources.

4) Description of Target Group

The partners were asked for statistical data regarding SME as well as to give an overview of the implementation of Information Security Management in SME. Of most interest are the general organisational structure of SME and the status quo of Information Security Management in particular. Further more the question regarding responsibility for Information Security in SMEs, should be discussed.

4.1) SME (in general)

Austria

99.6 % of Austrian companies are small and medium sized in accordance with EU definition. These businesses employed approximately two-third of all workers (62 %) and achieved approximately 60 % of all revenues and 57 % of the gross value added of market-oriented economy.

On closer inspection the majority of these companies is to be considered micro enterprises with only one employee (ca. 33 %) or 2-9 employees (> 50 %). 11 % are small enterprises with 10-49 employees and only 2 % are medium sized.

The Austrian economy is dominated by family-businesses. 80 % of Austrian companies are family owned. Characteristic of these companies is the close relationship between the family and the business sector.

SME in Austria come off badly in terms of information security. The main reason for this is an insufficient awareness of the management. The majority of SMEs therefore works without any protective measures. They have minimal or nonexistent IT budgets and no security strategies.

Czech Republic

The majority of Czech enterprises (99.85 %) are SME in accordance with EU definition, employing approximately 60 % of all workers.

The greatest obstacle to the faster implementation of information security is low awareness of the issue as such. Only 21 % have introduced a program for increasing awareness. Furthermore only one fifths of companies have a dedicated information security budget. Expenses are most often 1-5 % of the total IS/IT budget.

Germany

Contrary to the EU definition the German Federal Ministry of Economics and Technology defines small and medium sized businesses in qualitative and quantitative terms. In quantitative terms businesses with an annual turnover of less than 50 million Euros and fewer than 500 employees are classified as SME. Qualitative criteria include the unity of ownership and management rights within the person of the entrepreneur.

According to this definition 99.7 % of all German businesses are SME, providing roughly 60 % of all jobs requiring social insurance contributions. Furthermore 80 % of these companies are micro businesses with less than 10 employees.

Awareness on Information Security is increasing in SME but implementation on average is poor. Companies rather decide on easy manageability than complex security measures.

Spain

In Spain 99 % of all companies are SME in accordance with the EU definition, employing 90 % of all workers. The majority of these are micro enterprises (94 %). Only 5 % classify as small and 0.7 % as medium sized enterprises.

According to a study most SME invest in firewalls, antivirus, antispam and backup. These measures leave aside other aspects such as physical safety or continuity of services provided by suppliers.

Ireland

82.6 % of Irish companies are classified as micro-enterprises, 14.2 % are classified as small businesses and 2.6 % are classified as medium enterprises.

Issues surrounding Information Security and data protection do not feature as a priority for many small business owners, particularly those that are in the early stage of development.

Smaller businesses are frequently exposed to IS risks because the may not benefit from the oversight provided ban an experienced Board of Directors and may not have full-time information security staff. Without in-house IS expertise, such businesses are unable to track developments in the security landscape. As a consequence, it is more typically the responsibility of the Managing Director to draft and implement the IS policy. IS systems are organised on an ad-hoc basis, often in response to a security breach that has already occurred.

Italy

Micro enterprises constitute 94.7 % of the overall Italian entrepreneurial network. One of the critical issues for Italian micro-enterprises is the close relationship between the business and family dimension and thus a model of a "family business". This plays an important role as it pivots on informality in processes, flexibility, transmission of know-how, that represent the strengths of the business formula that characterizes the family business.

The main factors that impede the use of ICT solutions and thus Information Security are a lack of appropriate skills in human resources and technological costs. Moreover, the majority of micro enterprises do not have a real IT management, and therefore, ICT Security, and often a person does this but not exclusively.

4.2) Persons to be Trained (in particular)

In order to develop a suitable Information Security Officer Profile partners were asked to describe persons within SMEs who should be trained and qualified. What kind of previous knowledge could be expected? What job assignments will these persons most likely have?

Austria

Decisions regarding IT security and data protection are in 80 % of the companies made by the management or at least they are made by their inclusion. Especially in small companies the director is directly responsible for all matters.

The target group is focused on people across a variety of jobs, having basic IT skills.

Czech Republic

Managers respectively owners of SMEs and company's IT experts having general knowledge in IT issues are identified as target group.

Germany

SME owners and family co-workers are in the focus of this project. It should be the aim of provided information and training to promote this target group in the implementation and processing of Information Security Measures including outsourcing of tasks requiring special qualifications.

Spain

In Spain the target group consists of SME owners, personnel responsible for Information Technologies, sales management and employees as IT users in general.

Ireland

In Irish SMEs the training should be directed at the owner or managing director of the business. It can be assumed that the vast majority of this target group is unlikely to possess any formal qualifications in the area of IS. Further it is not to be assumed that any IS procedures will be in place in the target market.

The achievement of the training should be a working understanding of data protection law and the creation of best practice IS procedures.

Italy

Given the organizational model prevalent in SMEs, where it is usually the entrepreneur who is responsible, governs and strategically and operationally develops the business, it is difficult to imagine the development of technical vocational profiles responsible for Information Security in SMEs. Instead, there seems to be the need to increase the entrepreneur's knowledge, skills and managerial qualities to oversee planning processes, direction and control of IS systems, according to the ISMS logic.

5) Conclusions about Common Training Needs

Based on the results of the national reports common training needs of SME regarding Information Security in general and Information Security Management in particular can be summarised as follows:

Prerequisites of Target Group

- Basic IT knowledge
- No formal qualification in the area of IS or data protection
- None to basic awareness about the relevance and coverage of IS and data protection
- Clear priority towards central business activities

To be considered Surrounding Conditions

- IS procedures will most likely not be in place
- relevant contact points of economically most critical business processes with data processing will most likely be unknown
- lack of time, money and know-how

Central Training Topics

- overview and understanding of relevant rules and regulations
- identification of most relevant business processes and their contact points with data processing
- identification of trusted assets and most confidential data
- introduction / overview of main IS measures, distinguishing between technical and human/social factors
- principles of Information Security Management
- overview of specific risk potential of different applications
- understanding the correlation between lack of security and loss of reputation

PART II - the National Reports

6) Complete National Report Austria

6.1) National Rules & Regulations Concerning Information Security in SME

As a major part of today's business many of the business processes run electronically - or at least supported electronically – which meas that a large amount of information is also processed electronically. Much of this information is confidential and worthy of protection. According to a KPMG study, 80% of Austrian companies run important processes with IT support. 63% speak of "highly confidential information," which will be stored in their computer systems. 56% of the companies are talking about a significant business interruption, if corporate data is no longer accessible.

A failure of computer systems calls a company to a halt, no bills, no contracts, no customers are available. But not only availability is essential, even by viruses modified data can mean chaos and ruin the organization.

(Reference: http://bibliothek.fh-burgenland.at/fileadmin/Download/bibliothek/diplomarbeiten/AC05370279.pdf, 14.12.2011)

The Austrian Data Protection Act provides- in contrast to the German data protection law- no obligation to nominate a Data Protection Commissioner. At the same time, however, the creation of enterprise data protection structures is explicitly welcomed in the Data Protection Act (§ 6 Data Protection Act 2000).

Apart from the companies themselves, others need to know about the relevant company data stored to be safe. These are: customers, suppliers, partner companies and any other, whos data are used by those companies. Everyone has the right to have his personal data kept confidential. This right is also enshrined in Data Protection Act 2000): "Everyone shall have the right of confidentiality of personal data concerning him, as far as he has legitimate concern, particularly with regard to respect for his private and family life."

Furthermore, the company will also be prompted by law to provide for security of stored information. So it says in the law for data confidentiality (§ 15 Data Protection Act 2000) "It is the duty of the client, the service provider, or its employees to hold data secret, that they have only become accessible because of their professional employment, unless there is a legally permissible reason for a transfer."

In addition, data security measures (§ 14 Data Protection Act 2000) must be taken, which means to protect data "from accidental destruction, unlawful destruction, loss, improper use and access by unauthorized persons."

If data is not adequately protected in a company, the owner may be prosecuted. This law also speaks against the argument of many small-and medium-sized enterprises, which

are of the opinion that they are too insignificant to qualify as a goal of safety-critical attacks. But they also have the responsibility for the information handled within their company. Because small companies often have a weak security infrastructure, they are potential targets.

(Reference: http://www.dsk.gv.at/DocView.axd?CobId=41935, 15.12.2011)

In the quality thinking of SMEs an internationally recognized standard, the ISO 9001, has been established a long time ago. Similarly, in recent years a standard for information security management, the ISO 27001, has been established. Within a short time this standard was a guide on which companies oriented themselves. The question of "if" this standard is introduced in the company has often been changed to "when" this standard is introduced. Especially large companies now require their suppliers to comply with and ultimately to certify according to ISO 27,001. The risk for these companies is just too high, if a company does not worry about information security.

The ISO standard is seen by many as the "bible" in the IT security field. It includes a short, concise guide, which provides guidance to the implementation of security measures.

The **advantage** for smaller companies, that do not have a security team, is to get tips on how to get a grip on information security. Especially organizational measures increase the overall security dramatically and are strongly demanded in the standard.

The **disadvantage** is undoubtedly the fact that on a few pages the world of security is set out in note form. An "over look" without the assistance of a security expert is not possible. Even the IT employees of most companies will thereby be overburdened. And misunderstood measures are usually more expensive.

6.2) Vocational and Continuing Education and Training

In a previous study of TechConsult (2004) there were only a third of the companies which had already formulated and implemented fixed guidelines for IT-Security, whereas nowadays up to three quarters of the Austrian companies formulated fixed IT-guidelines and up to 16% are planning on implementing them in the future.

The three main themes in the future according to the study:

- Mobile Security - an increasing proportion of data loss is associated with the loss of mobile devices
- E-mail security to protect against malicious code and phishing and
- Identity Management to implement a targeted and responsible use of identities within the enterprise as well as units and access rights.

The range of the share of IT budget spent on IT security and IT training courses extends from less than 1% to about 15%. The average is 12%. The edition includes both spending on data protection as for data security. 60% of the companies spend about 10% of IT budget for IT security. 31% even over 15%.

(Reference: own translation of http://www.security-forum.at/?id=52, 14.12.2011)

6.2.1) Overview of Existing Training Offers in the Field of Information Security

Since the corresponding job description of a data protection officer does not exist in Austria there are, however, mainly three courses in information security available with

certification. This is on the one hand the Information Security Manager, the Information Auditor and a formation to be a Data Protection Officer. Furthermore there is the Information Security Refresher, which focuses on a continuing education and updating of the Information Security Manager and Information Auditor. In addition, also 1-day seminars can be claimed, which communicate the Information Security basics.

Name	Main Content /Objective	Target Groups	Terms of Use	Kind of Testimonial
Information Security Manager	The Information Security Manager will oversee the company taking responsibility for designing, implementing and continuous improving of information security management system (ISMS) and acts as an interface between the top management level and the operational divisions. The CIS curriculum provides the core elements of the international standard for Information Security ISO / IEC 27001 compact and user-oriented and shows its correct interpretation and implementation. (Reference: http://at.cis-cert.com/Ausbildungen/Informationssicherheit/IS-Manager/Information-Security-Manager-ISO-27001.aspx, 14.12.2011)	Entrepreneurs, managers, decision makers, computer scientists, computer officers, IT experts and whoever is interested	None	Nationally and internationally recognized certificate "Information Security Manager in accordance with ISO / IEC 27001". As a certified IS managers the requirements for participation in the secondary IS auditor training of the CIS are met.
Information Auditor	The series of courses to the IS auditor is the ideal complement for trained IS managers. As an auditor, all internal audits can be carried out by themselves and the company prepared itself for external audits with the help of the course-mediated methods. The IS auditor in the company is the "supreme authority" for ISM systems. It assesses the information security to their conformity to standards and identifies potential improvements before a company will be certified with the CIS certificate for the best possible standard of safety according to ISO / IEC 27001 or given an extension. (Reference: http://at.cis-cert.com/Ausbildungen/Informationssicherheit/IS-Auditor/Information-Security-Auditor-ISO-27001.aspx, 14.12.2011)	Information Security Manager	To participate, a valid certificate as an IS manager is needed. In this way a high level of qualification of the auditors is ensured.	Nationally and internationally recognized certificate "Information Security Auditor for ISO / IEC 27001"
Training as a data protection officer	With this seminar the skills necessary to master the future role as Data Protection Officer are obtained. All relevant legal and technical knowledge is provided and the goal of the seminar-workshop is to be "practical proof" in data protection. After the seminar one will have the ability to sense the data protection issues and to control them within the company. One has the communicative ability of the data protection rules to mediate in the company and one feels grown to the entire tasks of a Data Protection Officer. (Reference: http://www.kmu-plattform.eu/betrdaten.html, 14.12.2011)	Future data protection officers, engineers, lawyers, managers and interested parties who wish to obtain a thorough overview on the issue of data protection officer.	None	Certificate of attendance

Name	Main Content /Objective	Target Groups	Terms of Use	Kind of Testimonial
Information Security basics	The seminar provides an insight into the topic of information security. It explains terms such as "data" and "information security", and gives an overview of the current standard series ISO 27000. After the seminar, the contents of an information security management (ISMS) are understood. One is capable of the potential security needs of the company and can identify solutions for the protection of corporate information.	Entrepreneurs, managers, decision makers, QM and prospective DS Officer, interested parties	None	Certificate of attendance

6.2.2) Overview of Existing Services Regarding Information Security

Provider	Kind of Service	Target group	Terms of use	URL / Contact
IT-Safe WKO	IT security initiative for SMEs with the WKO Information Security Manual for download, news, events and current articles	SME	Freely accessible	http://www.it-safe.at/DE/Homepage.aspx
Austrian Information-Security-Manual	Revised information security manual with references to current developments, compact presentation of risks and countermeasures. Implementation assistance to national and international standards.	Companies and public administration	Freely accessible	https://www.sicherheitshandbuch.gv.at/
Information on Information-Security of the Chancellors-office	Basic information on information security, to protect the enterprise and information security commissions.	Community and companies in particular	Freely accessible	https://www.usp.gv.at/Portal.Node/usp/public/content/foerderungen_und_ausschreibungen/industrial_security/44661.html
Austrian Community for Data Protection	Information about data protection laws, certifications, events, seminars and the latest developments in information security.	Companies	Freely accessible	www.argedaten.at
Community of Interest Information-Security	The aim is to build a platform of information and awareness-raising among decision-makers. Information on seminars, events, networks and contacts with experts.	Companies and public facilities	Freely accessible	http://www.igis.or.at/index.php
Austrian Data Protection Commission	Information about the basic concepts of data protection law as well as Austrian and European data protection rules	Whoever is interested	Freely accessible	http://www.bka.gv.at/site/3462/default.aspx
Association Initiative Information-Security Austria	Construction of an electronic information network, press releases and publications on information security	SME	Freely accessible	http://www.iisa.at/

(Reference: own research, 14.12.2011)

Besides the above mentioned freely accessible Internet sites that provide information specifically for SMEs on information security, there are also fee-based services. Experts in information security provide consulting and analysis of the existing security system and assist companies in planning and implementing security measures.

Also, there are numerous foreign sources in German that deal with the issues of information security. A selection of these is given below:

Name	Kind of Service	Terms of Use	URL/Contact
Federal Office for Security in Information Technology	Information platform	Freely accessible, German source	https://www.bsi.bund.de/DE/Home/home_node.html
Federal Data Protection Commission	Information platform	Freely accessible, Swiss source	http://www.edoeb.admin.ch/
CIS-CERT	Certification in Information Security	Fee-based certificates	http://at.cis-cert.com/Unternehmen/Zertifizierungsorganisation-CIS.aspx
R+	Advice, analysis, implementation of management systems, in-house training, preparation for certification	Fee-based consulting and preparation of solutions	http://www.r-plus.eu/web/
E-Sec	Interactive training and training software	Fee-based software and trainings	http://www.e-sec.at/Software.aspx

(Reference: own research, 14.12.2011)

6.3) Description of Target Group

The Austrian Security Forum (ASF), an association of leading IT security service provider in Austria 2008, presented a study on IT security and information security by the consulting firm TechConsult.

The key messages of the study demonstrate that data protection and data security in Austria are one of the important functions of the internal IT departments. If there is no dedicated security team in the company, the IT department is in charge of performing duties. Every year it take up about 30% of their time (at a reference of 200 man days per year) on the tasks for IT security. But increasingly the management is more and more the initiator of the new security projects.

In businesses with more than 250 employees a growing awareness of information security manifest itself, whereas in small companies it is rather disastrous. A lack of basic measures, both organizational and technical nature, is often the case.

(Reference: own translation of http://www.security-forum.at/?id=52, 14.12.2011)

6.3.1) SME (in general)

In 2009 were about 299,000 small and medium enterprises (SMEs) in the market-oriented economy in Austria. Compared to the previous year the number has decreased by 0.2%. In these companies worked about 1.8 million employees (of which around 1.5 million workers) in 2008. The SMEs were able to generate net revenues totaling

approximately EUR 405 billion and a gross value of around EUR 99 billion. 99.6% of Austrian companies were therefore SMEs. These businesses employed approximately two-thirds of all employed workers, or about 62% of all workers. They achieved approximately 60% of all revenues and approximately 57% of the gross value added of market-oriented economy.

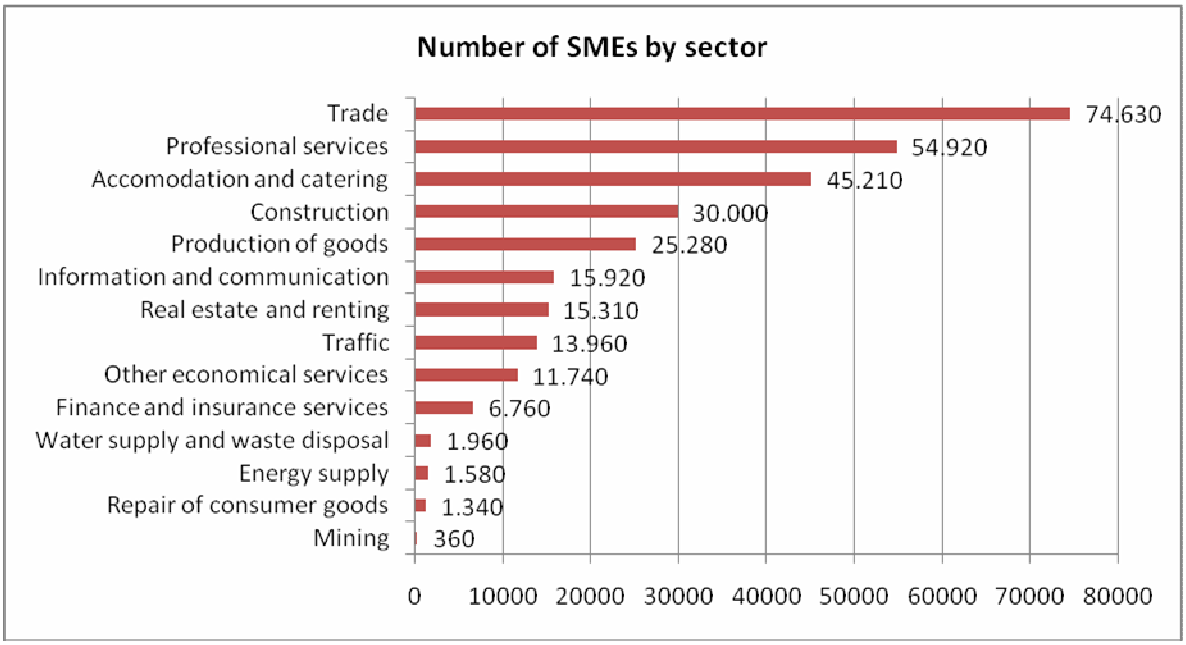
On closer inspection of the SMEs by size class it's obvious that more than one third of all businesses involve companies with only one employee, so-called one-person businesses (EPU). More than half of the companies were small businesses with 2-9 employees. Almost 11% of the businesses were employers for 10-49 persons. In approximately 2% of the companies 50 to 249 employees were working.

	2008		2009	
	Total	**Share of all companies in %**	**Total**	**Share of all companies in %**
1 employee	**106.174**	**35,3**		
2 to 9 employees	**155.892**	**51,8**	**263.140**	**87,7**
10 to 49 employees	**32.368**	**10,8**	**31.070**	**10,4**
50 to 249 employees	5.192	1,7	4.760	1,6
SME total	**299.626**	**99,6**	**289.970**	**99,6**
250 and more employees	300.745	100	300.050	100

(Reference: adaptation of: http://www.bmwfj.gv.at/Unternehmen/UnternehmensUndKMU-Politik/Documents/Mittelstandsbericht%202010%20final.pdf, 14.12.2011)

In 2009, nearly 75,000 SMEs worked in trade. This sector was almost one quarter of all small and medium enterprises in the market-oriented economy in Austria and thus represents the largest economic sector. This was followed by the professional services (almost 55,000 SMEs) and the accommodation and catering establishments (more than 45,000 SMEs).

In the majority of industries were mainly small businesses with 2-9 employees. In the sectors of information and communication, professional services and repair of consumer goods, most companies were, however EPU. The percentage of companies with 10 to 249 employees was at its highest in mining and in the production of goods.



(Reference: http://www.bmwfj.gv.at/Unternehmen/UnternehmensUndKMU-Politik/Documents/Mittelstandsbericht%202010%20final.pdf)

An international comparison shows that the vast majority of enterprises are SMEs in all Member States of the EU. With a total of 20.7 million small and medium-sized companies they represent 99.8% of all businesses. Almost 92% of all enterprises were micro businesses with fewer than 10 employees.

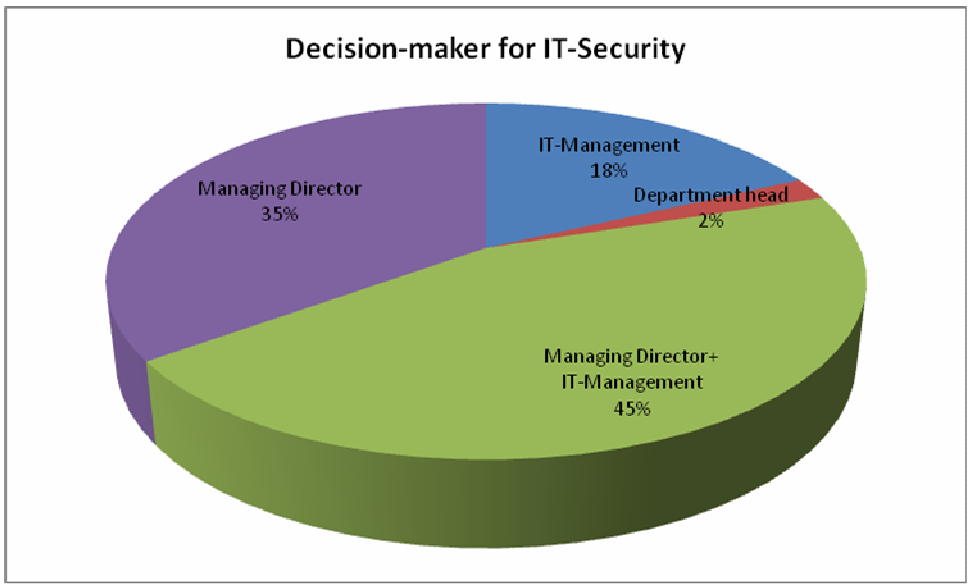
Family-businesses dominate the Austrian economy. 80% of Austrian companies are family owned and employers are responsible for 70% of the workforce. Characteristic of these companies is the close relationship between the family and the business sector and their mutual influence. These family-businesses have a strong advantage towards non-family-businesses in terms of strong personal commitment, strong identification and pursuit of sustainability.

The SMEs in Austria come off badly in terms of information security according to a study in 2008. The main reason for this is hardly the cost of products and implementation, but in reality an insufficient awareness of the management. The majority of SMEs therefore works without any protective measures. They have minimal or nonexistent IT budgets and no security strategies.

(Reference: own translation of http://www.bmwfj.gv.at/Unternehmen/UnternehmensUndKMU-Politik/Documents/Mittelstandsbericht%202010%20final.pdf, 14.12.2011)

6.3.2) Persons to be Trained (in particular)

The traditional job description of a security officer or a data protection officer, as it exists in Germany does not exist in Austria. Decisions regarding IT security are in 80% of the company made by the management or at least they are made by their inclusion.



(Reference: http://www.kpmg.at/uploads/media/Report_IT_Umfrage_2004.pdf, 14.12.2011)

Especially in small companies the directors are directly responsible for all matters. The security issue is constantly increasing in complexity and now requires the know-how of experts. The company lacks on the one hand on the conscious use of the risk in IT, on the other hand, increases the liability for the manager by ever stricter laws and regulations. An SME has little free resources and must focus more on its core business - therefore the security area is often too short. IT agendas are often alongside co-supervised, as there is no IT officer or security officer.

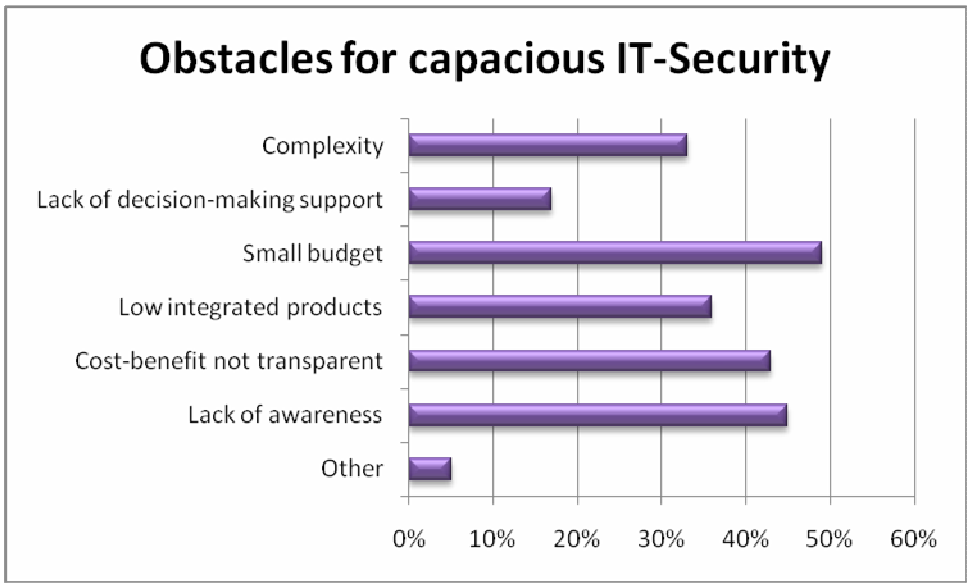
Despite the lack of implementation of information security, 97.3% of all small businesses work with Internet access. Although they are often less affected by the threats to information security than larger companies, the basic protection is paramount. Small businesses work in the field of information security with a relatively high level of independence, though they are often unaware of the hazards. Practical recommendations and trainings, as are provided by INSEMOT, are likely to be of crucial importance for this type of company, because in very few companies IT-staff is employed.

The target group is not intended to focus on IT professionals whos main job is to deal with information security, but to people across a variety of jobs, who have basic IT skills. E.g.: secretaries, personnel managers, accountants, sales reps, etc. The industry can be as varied as the job title. Information security-related industries, both the hotel industry, trade, etc. as well as private sector companies.

6.4) Resume

According to a study on information security in small and medium-sized enterprises a big problem factor for the lack of implementation of safety measures was the lack of safety awareness. It was discussed a "lack of risk awareness," a "lack of awareness of the risk manager" and a "lack of security awareness of bosses". Other problems that were mentioned were "costs", "time" and "lack of transparency of cost-benefit" because the security measures are implemented mainly by the managers.

The lack of decision-making support and the indicated complexity of information security systems make it clear that there is a need for a comprehensive information platform and specific training in SMEs.



(Reference: http://www.kpmg.at/uploads/media/Report_IT_Umfrage_2004.pdf, 14.12.2011)

The study participants also clearly want more objective information and possibilities the security system can be compared internationally.

Surveys on information security in small enterprises show that a request for comprehensive information on information security is desired and would certainly be welcomed by small businesses. Thus, in the course of the survey it became clear that small companies are on the one hand interested in an information platform, and on the other hand would approve of the development of a package or a standard explicitly for very small businesses. Doing this, emphasis should be placed on comprehension, scope and feasibility, which must correspond to the size of the company in this case.

6.5) List of References

Austrian.security.forum (2011). TechConsult Multiclient-Studie „IT-Security in Österreich 2008". http://www.security-forum.at/?id=52

Bundesministerium für Wirtschaft, Familie und Jugend (2011). Mittelstandbericht 2010. Bericht über die Situation der kleinen und mittleren Unternehmungen der gewerblichen Wirtschaft. http://www.bmwfj.gv.at/Unternehmen/ UnternehmensUndKMU-Politik/ Documents/Mittelstandsbericht%202010%20final.pdf (14.12.2011)

CIS - Certification & Information Security Services GmbH (2011). CIS-Lehrgangsreihe: Information Security Manager nach ISO 27001. http://at.cis-cert.com/ Ausbildungen/Informationssicherheit/IS-Manager/Information-Security-Manager-ISO-27001.aspx (14.12.2011)

European Commission (2011). Enterprise and Industry. Small and medium-sized enterprises (SMEs): SME Definition. http://ec.europa.eu/ enterprise/policies/sme/facts-figures-analysis/sme-definition/index_en.htm (14.12.2011)

KPMG Austria GmbH Wirtschaftsprüfungs- und Steuerberatungsgesellschaft (2011). IT Umfrage 2004. http://www.kpmg.at/uploads/media/Report_IT_Umfrage_2004.pdf

Wikipedia (2011). Informationssicherheit. http://de.wikipedia.org/wiki/Informationssicherheit (14.12.2011)

Wikipedia (2011). Infomation Security Management System. http://de.wikipedia.org/wiki/Information_Security_Management_System (14.12.2011)

6.5.1) Sources of Law

Datenschutzgesetz 2000 (DSG 2000) in inoffizieller englischer Übersetzung. http://www.dsk.gv.at/DocView.axd?CobId=41935 (15.12.2011)

7) Complete National Report Czech Republic

7.1) National Rules & Regulations Concerning Information Security in SME

The National Information Security Strategy is approved by Government Resolution CZ No. 1340/2005 and developed based on the task of the State Information and Communications Policy eČesko 2006 in accordance with the laws of the Czech Republic and EU and for the field of information Security Methodology of the provision, implementation and operation, monitoring and maintenance of information security management system (hereinafter referred to as ISMS - Information Security Management System) in the organization. Simply said, the ISMS is only one and one that is described in ISO / IEC 27001.

7.2) Vocational and Continuing Education and Training

7.2.1) Overview of Existing Training Offers in the Field of Information Security

There are these possibilities of education in the IS field in the Czech Republic:

Information Security Manager

Participants of "IS Manager" (Information Security Manager) program will familiarize with complex issues of ISMS (Information Security Management System), learn new skills and information necessary for assessing actual conditions, implementation, communication with auditor, management, and permanent ISMS improvement, where he or she would act as an interface between organization's top management and executive departments. The manager shall be capable of successful promotion of company's objectives with minimal friction area at the level of relationships of the company, organization, or corporation. The manager learns to create project teams, to manage them and to motivate them. He or she also receives basic knowledge of legislative framework related to ISMS issues and problems.

Internal Information Security Auditor

This course for Internal Auditors of IS (Information Security) is ideal supplement for qualified Information Security Managers. As because the Internal IS Auditor may himself or herself perform internal audits within the organization and thus prepare it optimally for challenges of a global organization or for assessments performed by external auditors, he or she represents the "highest instance" for system of information security management within the organizations. The auditor assesses the system from the view of its compliance with standards and legislative requirements, detects imperfections and defines potential improvements. His or her activity directly impacts the system capabilities before the certification or during certificate renewal.

Internal Training or Effective Solution to Individual Needs of Your Company

The most effective way to receive qualification is training directly within your company – in the team of your colleagues and superiors, based on examples from within your own work area. Internal trainings are cost effective and efficient mainly for larger organizations. It is also guaranteed that company's know-how would not get beyond the company's borders.

Name	Main Content / Objective	Target Groups	Preconditions / Requirements	Kind of Testimonial
IS manager by ISO 27001	Course provides the key elements of an international standard for Information Security ISO / IEC 27001	Possible IS managers form the companies	To have 1000EUR per 4days lasting course (without VAT)	Internationally accepted certificate: Information Security Manager by ISO/IEC 27001
Internal IS auditor	Internal IS auditor can provide internal audits and prepare the company for the external audits	Supplement for qualified IS managers	To have 1000EUR per 4days lasting course (without VAT)	Internationally accepted certificate: Information Security Auditor by ISO/IEC 27001

7.2.2) Overview of Existing Information Services Regarding Information Security

Further services, training opportunities and getting news in the field of IS is membership in the Czech Institute of Information Security Managers. The annual membership fee is 1000 CZK and allows members to participate in conferences and communicate between managers and get information directly from practice.

www.cimib.cz

Provider	Kind of Service	Target Groups	Terms of Use	URL / Contact
Czech Institute of Information Security managers	Membership (for fee 40EUR per year)	IS managers	Conferences, dialogues	www.cimib.cz

7.3) Description of Target Group

7.3.1) SME (in general)

The persentage of the SMEs in the amount of all enterprises in Czech republic is 99,85 percent (taking into account all SMEs from0 to 249 employees). On the other hand, when we take a look at number of staff employed in SMEs it is 61,38 percent from the whole amount of emploees in all enterprises in Czech Republic.

When we are talking about Micro-enterprises they are more flexible and able to response to customers needs. They have addopted "client approach" using gaps in the market,

where big companies are not able to reach them.Their market place is mainly fixed thanks to no interest of big companies in these positions.

Many small and medium enterprises came from the original trades, or a small team of people who knew each other very well. Gradually, as the company developed and expanded, began to grow business management problems and it turned out that the original way of managing the current conditions are already poor.

Barriers to development

The following is a selection of problems that significantly hinder or prevent the development of small and medium-sized enterprises:

- production priority over other activities
- lack of a strategic plan (vision of business development)
- lack of marketing and information systems (including Information Security)
- inadequate definition of roles (competencies) managers - entrepreneur, manager, engineer - master organization of the company is built on personalities rather than on the features
- model management companies - often the acceptance of "pointed" organization along the lines of big companies
- lack of control documentation - plans, manuals, standards, coherent management system, Information Security system
- minimize the qualification level of employees (small firms can not pay highly qualified professionals)
- lack of quantification of all activities that take place in the company and their evaluation (what do not measure, not control)
- ignorance of the work of staff, non-use consumption standards of work, demotivating pay systems

Model solutions

Generalization of the findings from the rationalization of the centers activities of small businesses, there is concluded that the problems of small and medium-sized firms are similar. For their solution there is prepared the following model:

- A – defining the roles of management (entrepreneur, manager, technician)
- B – a vision of development - the company's future definition (marking of products, company logo, employee clothing, corporate color segmentation - fragmentation of products and services)
- C – company management system

The area of information systems

- management tools (plan, standards, operating manuals for the implementation of sub-activities)
- Quantification of key business processes (management of flows of information, presentation and interpretation of data, information security and safety when handling information)
- system of evaluation of company activities

The number of companies is declining in which no single employee has clearly defined responsibility for information security.

In the vast majority of companies information security is incorporated into IS/IT divisions.

Generally speaking the greatest obstacle to the faster implementation of information security is low awareness of the issue as such. The proportion of companies which put this obstacle in top place above financial demands is on the increase. At the same time only 21% of organizations have introduced a functional program for increasing awareness in this sphere.

Increasing security awareness is also the most frequently cited activity with the potential for cost savings over the medium term.

Four fifths of companies do not have a dedicated information security budget. Expenses in this sphere are most often 1-5% of the total IS/IT budget.

7.3.2) Persons to be trained (in particular)

In particular our target groups, within SMEs/MEs, are mostly the Micro enterprises and mainly their managers (currently owners) and IT experts in the companies.

It is not reguired, that the IS manager is currently an IT expert, but the IS manager would have general knowledge in IT issues.

Further training is a key component for a successful implementation of IS measures in SMEs/MEs. Responsible for matters in this field are mainly the owners themselves, who are therefore defined as the main target group for the training measures. The further training can also be relevant for their employees in the fields of HR, IT, back office or other staff in administration who will need additional skills in order to support the implementation of an IS strategy.

7.4) Resume

As far as the level of information security in the Czech Republic is concerned, confidence rose over the course of the year, backed up by the large qualitative steps which the Czech Republic has taken in this sphere since 1999. Almost 70% of enterprises believe that we are on the same level as Western Europe. In 1999 only 24% of those questioned believed this, and 16% believed that the situation was considerably worse. Twenty-five percent of respondents still rate the situation as worse.

The sphere of general security awareness is something on which organizations should definitely concentrate over the next few years. Since 1999 the proportion of companies which perceive this issue as one of the key obstacles to the future development of information security in the Czech Republic has increased steadily. At the same time very few companies have introduced a functional program aimed at increasing security awareness. Moreover, an increase in security awareness is one of two leading spheres which can offer cost savings in terms of information security.

8) Complete National Report Germany

8.1) National Rules & Regulations Concerning Information Security in SME

Within the *Leitfaden für Informationssicherheit. IT-Grundschutz kompakt* the Federal Office for Security in Information Technology divides rules and laws relate to Information Security in companies and administrations in three application areas: a) due diligence of companies, b) consumer protection, and c) data privacy protection.

Due Diligence

Deficiencies in information security can, in extreme cases, endanger the existence of a company, but at least cause serious damage. As part of the legal regulation of due diligence of an entrepreneur or manager a concrete commitment to ensuring appropriate security levels within the company can be derived from several laws.

Thus, for example, the **Aktiengesetz** stipulates that a director is personally liable if he not monitores trends that may pose a future risk to the company by a risk management and prevents demage with appropriate measures. (1 BSI) (AktG § 91 Abs. 2 http://www.gesetze-im-internet.de/aktg/__91.html and § 93 Ab. 2 http://www.gesetze-im-internet.de/aktg/__93.html , accessed: 19/12/2011)

The **Gesetz betreffend die Gesellschaft mit beschränkter Haftung** imposes a corresponding duty of care on directors of limited companies. (GmbH-Gesetz § 43 Abs. 1 http://www.gesetze-im-internet.de/gmbhg/__43.htm , accessed: 19/12/2011).

The **Handelsgesetz** oblige auditors to consider, whether the risks of future developments are appropriately depicted (§ 317 para 2 and 4 http://www.gesetze-im-internet.de/hgb/__317.html, accessed: 19.12., 2011).

The **Strafgesetzbuch** contains special rules for certain professions (eg. doctors, lawyers) including regulations on handling confidential information and data as well as sanctions for violations (StGB § 203 http://www.gesetze-im-internet.de/stgb/__203 .html, accessed: 19/12/2011).

Consumer Protection

The consumer protection is also regulated by different laws. With regard to the use of information technology, Internet or telecommunications services, in particular the following laws are to be considered:

- **Telekommunikationsgesetz** (TKG) http://www.gesetze-im-internet.de/tkg_2004/ (19/12/2011)
- **Gesetz über Urheberrechte und verwandte Schutzrechte** http://www.gesetze-im-internet.de/urhg/ (12/19/2011)
- **Gesetz über die Nutzung von Telediensten** (TDG) http://www.online-recht.de/vorges.html?TDG (12/21/2011)
- **Mediendienste-Staatsvertrag**

Data Privacy Protection

Data privacy protection refers to the protection of individuals before the abuse of personal data and is governed by the following laws:

- **Bundesdatenschutzgesetz** (BDSG) http://www.gesetze-im-internet.de /bdsg_1990/ (19/12/2011) and **Datenschutzgesetze der Länder** (LDSG)
- **Gesetz über den Datenschutz bei Telediensten** (TDDSG) http://www.online-recht.de/vorges.html?TDDSG (12/21/2011)
- **Telemediengesetz** (TMG) http://www.gesetze-im-internet.de/tmg/(19/12/2011)
- **Telekommunikationsgesetz** (TKG) http://www.gesetze-im-internet.de/tkg_2004/ (19/12/2011)

8.2) Qualification and Information regarding Information Security

The study *Netz- und Informationssicherheit in Unternehmen 2011* of the *Netzwerk Elektronischer Geschäftsverkehr*, published by the E-Commerce-Center Handel shows that the topic of IT and information security is becoming increasingly important for small businesses. Small businesses, however, due to lack of resources are facing at the same time the challenge of ensuring a high level of security and a simple and understandable manageability in everyday life. Crucial factors in this context are the comprehensive information and regular training of employees. When asked: "Do you inform / educate your employees about IT- and Information Security?", however, around 40% of the 324 companies surveyed answered "No". Reasons given are insufficient examination of the topic and a lack of information.

It should be noted that the study *Netz- und Informationssicherheit in Unternehmen 2011* is not representative because of the number of respondents and the composition of the sample. It is assumed that first and formost companies participated in the voluntary survey being already aware of the subject Information Security. This assumption is based on the fact that 20% of companies surveyed state that they had been vicitim of data los and had suffered significant financial demage. The study clarifies, however that the issue Information Security is still fare from beein implemented in everyday life of small and medium enterprises, as even in open-minded companies significant gaps and deficiencies in Information Security Management could be detected.

As companies state a lack of information as reason for not training and informing employees an overview of already available training and information services in the field of IT and Information Security is given in the following. The list does not claim to be complete.

While searching for further and continuing education and trainings and information services, another problem became apparent. The variety of available offers addresses a group of persons with relevant previous knowledge and practical experience in Information and IT Security. The employee of a small company, who in addition to his regular job also is responsible for IT and Information Security, is addressed only in rarer cases.

8.3.1) Overview of Existing Training Offers in the Field of Information Security

Name	Inhalt / Ziele	Zielgruppe	Voraussetzungen	Zertifizierung
Data Protection Assistant	• Basic rules and regulations regarding data privaciy protection • Tasks of the Data Protection Commissioner and the Data Protection Assistant • Construction and maintenance of data protection documentation in practice • Knowledge base to assist in planning, implementation and evaluation of data protection audit • possible problems and solutions	People who support and represent the data protection commissioner	Job assignment in the IT, human resources, controlling, marketing or workers council	Certificate of educational institution
Data Protection Commissioner	• Data protection law • Organization of data protection and data security in the enterprise • Operational tasks of the Data Protection Commissioner • Selection, establishment and integration of technical security concepts • Individual operating procedure for preparation of basic safety in the company • Criminal abuse of modern IT • The project "data security and transfer" in company practice	Established and future data protection commissioner, staff from Internal Audit, Legal Department, Organization	Exclusion of the following persons: IT management, human resources, management	Certificate Data Protection Commissioner
Data Protection Manager	• Training for Data Protection Commissioner • Planning, implementation, monitoring, control and maintenance of data protection management system in the company • Methods of project management	Data Protection Commissioner, officers, management officer, project manager	Certificate Data Protection Commissioner or comparably	Partial contribution to the proof of expertise and further education
Data Protection Auditor	• Preparation, planning, implementation and documentation of data protection audits • Audit procedures • Documentation, evaluation of the results of a data protection audit • Implementation of corrective and improvement measures	Data Protection Commissioner, officers, management officer, project manager	Certificate Data Protection Commissioner or comparably	Certificate
External Data Protection Commissioner	• Analyse bestehender Strukturen beim Kunden • Analysis of existing structures at the customer • Successful implementation of data privacy protection • Building up mutual trust with customers • Know and recognize the pitfalls and possibilities of legal safeguarding • practical Tips	Established and future external data protection officer	Certificate Data Protection Commissioner or comparably	Certificate „External Data Protection Commissioner"

Name	Inhalt / Ziele	Zielgruppe	Voraussetzungen	Zertifizierung
IT Basics for Data Protection Commissioners	• IT basic knowledge • Function and operation of PC, laptop and Co • Networks • operating system • Internet • Protocols	future and established data protection commissioners		
Up-date on data protection	• Changes in laws and regulations • Practical experiences in implementing the new guidelines • Data Privacy Policy • exchange of experiences • Instruments and tools • Work / tasks of the supervisory authorities	Data Protection Commissioner, officers, management officer, project manager	Certificate Data Protection Commissioner or comparably	Certificate of attandance
Compiling and Maintaining a Catalog of Procedures	• Efficient and comprehensive method of creating the Catalog of Procedures • identifying interfaces to other documentation and linking meaningfully • testing legitimacy of procedures and effective monitoring of compliance	data protection commissioner, management officer, staff responsible for IT	Data Protection Commissioner	
professionally Handeling data mishap	• Obligations • Scheduling and tactical considerations • Content and design of a message • Risks of injury to the reporting requirement • Risks despite their registration • Current compliance measures	Privacy officers, IT security officer, compliance officer, data protection and IT consultants, lawyers, corporate lawyers		Certificate of attandance
Rules and Regulations on Data Protection relevant for HRM	• Current basic knowledge of data protection laws relevant for HRM • dealing with critical questions regarding behavior and performance monitoring	Officers, employees from the personnel department, works, IT department, internal and external data protection officer		
ISO/IEC 27001 Basics	• Benefits of using standard-based management systems • Policies and objectives • Responsibilities and resources • process models • documentation • Risks and their analysis • Improvement, evaluation and assessment • Auditing • compliance	Professionals and executives responsible for information security		

Name	Inhalt / Ziele	Zielgruppe	Voraussetzungen	Zertifizierung
Information Security Management practically + Transfer Workshop	• ISO 2700x family of standards and others • Principles and practices in risk management • Requirements of ISO 27001 to the management / implementation • Application of measures • case study	Professionals and managers who are responsible for information security, quality managers, IT specialists, data protection commissioners, councils, directors, project/product manager, customer consultant, facility management, human resources	profound knowledge of standard-based management application systems	
Certification as Information Security Management Officer			Participation in: Introduction to the ISO / IEC 27001, Information security management in practice + Transfer Workshop	Certificate
IT-Security Basics (BSI)	• Information and Information Security • BSI standard 100x series • Auditing and certification to ISO 27001 based on IT Security Basics	Experts		Certificate
IT-Sicherheits-beauftragter (TÜV) – Teil 1 IT-Security Officer – Part 1	Introduction to information security (IS) - Spectrum and strategic importance - Threats and weak points - Requirement and Risk Management - Position and tasks of the IT Security Officer ISO 27001/27002 and BSI IT-Security Basics - Structure, content, applications, tools - Auditing and Certification Comprehensive Security Concepts - Virus protection, data backup, archiving - HW/SW- and Security Incident Management - Contingency Planning, Cryptography, Authentication Infrastructure Security - Blocks and measures Internet safety - Protocols, services, vulnerabilities, and measures	People from industry, services and administration working in the field of information technology being responsible for the implementation of risk analysis, preparation of IT Security Policies and their implementation and control		Certificate

Name	Inhalt / Ziele	Zielgruppe	Voraussetzungen	Zertifizierung
IT-Security Officer – Part 2	IS management with proven standards - ISO 2700x, BSI-100-x, ISO 13335, ITIL, CobiT etc Concepts and measures for network security - Local area networks, voice over IP - Mobile / wireless communication systems and devices Security of IT systems and applications - Client-server and host systems - User and authorization management - Web applications, databases, SAP - IT Security Services personnel IT security - Content and necessity - Target groups and their behavior - Concepts, measures, practices - Project implementation Legal aspects of IT security - Legal basis of the IT security - Legal requirements for IT security - rules and regulations regarding IT Security Officers	People from industry, services and administration working in the field of information technology being responsible for the implementation of risk analysis, preparation of IT Security Policies and their implementation and control		Examination

8.3.2) Overview of Existing Information Services Regarding Information Security

Provider	Kind of Service	Target Group	Conditions	URL / contact
Deutschland sicher im Netz e. V.	Informationen, Web Services, Downloads	consumer, SME, adolescent, parents	Free of charge	https://www.sicher-im-netz.de/
BürgerCert	Information and warning about mal ware and security vulnerability in computer applications	SME, consumer	Free of charge but registration required	https://www.buerger-cert.de/
Bundesamt für Sicherheit in der Informationstechnik (BSI)	The BSI investigates security risks associated with the use of IT and develops preventive security measures. It provides information on risks and threats relating to the use of information technology and seeks out appropriate solutions.	Government, Companies, Administration, Consumer	Free of charge	https://www.bsi.bund.de/DE/Home/home_node.html
BSI für Bürger	Intelligible to all information on the topic of IT security. Main categories are: • What risks come across on the net? • How can I secure my PC? • How to surfe safely in the net? • How to safely use mobile networks?	Consumer	Free of charge	https://www.bsi-fuer-buerger.de/BSIFB/DE/Home/home_node.html
Rechtsanwalt Dr. Sebastian Kraska	Selected articles about data privacy and data security, awareness raising and of data security and data privacy	SME, free lancer, Consumer	Free of charge	http://www.datenschutz beauftragter-online.de/
BMWi/NEG-Verbundprojekt Sichere E-Geschäftsprozesse in KMU und Handwerk	Information Material: Best Practice, Manuals, Practical Advice, Studies Seminars Regulars' table IT-Sicherheit	SME	Free of charge	http://www.kmu-sicherheit.de/
Fachhochschule Gelsenkirchen, Institut für IT Sicherheit	Consultation, Live-Hacking, Studies, Concept development and Specification, Prototyping, Benchmarking, Surveys, Penetration Test, IT-Security Advice	Consumer, administration, companies	Some services are free of charge, some are with costs	https://www.internet-sicherheit.de/
Landeszentrale für Medien und Kommunikation (LMK) Rheinland-Pfalz, Landesanstalt für Medien Nordrhein Westfalen (LfM)	Information and materials for teaching a competent and critical Internet use and create awareness of problematic areas	Parentd, teachers	Downloads are free of charge, print material is purchased	https://www.klicksafe.de/

Provider	Kind of Service	Target Group	Conditions	URL / contact
TÜV Rheinland AG	Consulting, IT-security in the production, online safety and quality, data security, security of mobile devices, network security, strategic information security	Companies and consumer	With costs,	http://www.tuv.com/de/deutschland/gk/consulting_informationssicherheit/consulting_informationssicherheit.jsp
Bundesministerium für Wirtschaft und Technologie Referat Öffentlichkeitsarbeit	Information, Web Services, Downloads	SME	Free of charge	http://www.ec-net.de/sicherheit
Netzwerk Elektronischer Geschäftsverkehr	Web service, interactive questionnaire to determine the state of IT security / information security within the company, including evaluation, optimization tips and information material	SME	Free of charge	http://ris.ecc-ratgeber.de
Gesellschaft für Datenschutz und Datensicherheit e. V.	The GDD helps data controllers and particularly their data protection officers / corporate privacy officers (DPOs / CPOs) to solve the many different legal, technical and organizational problems in order to achieve a proper balance between the interests of data subjects who merit protection and the equally justified need for information on the part of controllers and individual persons. • Date Protection Quick Check • Regional experience exchange groups • technical information • Membership and exclucive services • Training • Events • Forum • Benchmarks and best practice on data protection	Companies and Data Protection Commissioners	Membership with costs Webservices free of charge	https://www.gdd.de/index_html_v

8.4) Description of Target Group
8.4.1) SME (in general)

Definition of SME in Germany

The Federal Ministry of Economics and Technology (BMWi) defines on its website the term *small and medium sized businesses* (SME) as follows:

> In quantitative terms, businesses with an annual turnover of less than 50 million Euros and with fewer than 500 employees are classified as SMEs in Germany. Qualitative criteria include the unity of ownership and management rights within the person of the entrepreneur (or his or her family).
>
> In accordance with this definition 99.7% of all businesses in Germany are SMEs and provide roughly 60% of all jobs requiring social insurance contributions.

According to the Federal Statistical Office in 2007 approximately 80% of this cohorte were so-called micro businesses. Therefore the clear majority of all German companies are part of the potential target group of the INSMOT SME project.

For further target group consideration next to the company size the qualitative criterion "unity of ownership and management rights" should be considered. Due to the close bond of the company to the person or the family of the owner small and micro enterprises often show individual and distinct organizational structures. Family businesses are often characterized by a certain degree of informal processes, flat hierarchies, flexibility and readyness to share knowledge, which on the one hand are reasons for their particular strength, but at the same time reasons for their specific problems.

Information Security in German SMEs

With regard to the integration of Information Security in these companies indistinct structures clearly are a weakness. The study *Netz- und Informationssicherheit in Unternehmen 2011* clarified alsothat above all a lack of resources – especially time, money and qualified personnel – is becoming a problem. Although the surveyed SMEs from the industrial, commercial, service and trade sectors increasingly examine the topic of IT and Information Security, rather decide on easy manageability in everyday life.

For example, only 50% of companies surveyed have a security policy and 25% say they do not have a computer emergency response plan. At the same time, however, around 20% of companies surveyed experienced a permanently loss of significant data due to a crash or a disk or device loss. 7.6% of companies surveyed between January and May 2011 became the victim of successful digital attacks. Of these companies 9.1% suffered a loss of 20,000 € and more.

65% of surveyed companies are aware of being able to run the business without the company file server for less than 4 hours. Second and third on the list of the greatest potential threats are the loss of phone respectively the companies own ERP-/WWS-System.

8.4.2) Persons to be Trained (in particular)

Considering the BMWI SME definition the SME owners and family co-workers are in the focus of the INSEMOT SME project. Especially in the crafts sector in a multitude of companies family members work in responsible positions next to the owner. In crafts

companies the "traditional" role sharing predominates with the owner and Master Crafts Man taking over leadership in technical matters, and the wife taking leadership in business and organizational matters. Accordingly, besides the company owners also the group of co-working family members should be considered as potential target group for training within the INSEMOT SME project.

Considering the results of the NEG-survey 2011 and the statutory requirements for Information Security in companies the following "Information Security Officer" requirements can be outlined.

Profile Information Security Officer in SMEs

- Being able to raise employees awareness on Information Security
- Organizing trainings for employees on regular bases; being able to recognize individual training needs
- Being able to assess at what point the support of IT services are needed and what tasks can be done internally
- Inducing and coordinating the development of a security policy
- Adherence to the security policy / ensuring quality management
- Being able to identify necessary amendments of the security policy and encouraging adaptation
- Coordinating the development and update of an IT contingency plan
- Understanding the specific risk potential of different applications such as PC, networks, online shops, mobile applications and devices, social media; being able to arrange for adequate protective measures
- Understanding the link between lack of security and loss of reputation
- Knowing relevant certificates and seals, for example for online shops and understanding the underlying certification criteria
- Aranging for regular backups and inspection of backups
- Being able to assess potential danger by external persons and taking appropriate protective measures, such as employee training, no access for unauthorized persons to sensitive areas
- Knowledge / understanding of economically important or critical business processes and their relevant points of contact with data processing

8.5) Resume

A number of SMEs in Germany is already aware of the importance of IT and Information Security. Nevertheless, a lack of resources, especially time, money and professionally trained staff, as well as a lack of information are the reasons that Information Security Management has yet to be implemented in SMEs. The focus of the companies lies on the economically most relevant business processes. Many companies still do not seem to be sufficiently aware of the importance of internal data processing for these business processes.

The objective of the INSEMOT SME project should therefore be to assist the companies in establishing inwardly and outwardly directed processes and practices in order to protect trust assets and information against security incidents. Crucial for an effective and efficient Information Security Management is knowledge of most critical business processes and their relevant contact points with data processing.

8.6) References

Bundesamt für Sicherheit in der Informationstechnik (Hg.): Leitfaden Informationssicherheit. IT-Grundschutz kompakt. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfaden_pdf.pdf?__blob=publicationFile (01.12.2011)

Bundesministerium für Wirtschaft und Technologie. Mittelstandspolitik. http://www.bmwi.de/BMWi/Navigation/Mittelstand/mittelstandspolitik.html (01.12.2011)

Englische Version: http://www.bmwi.de/English/Navigation/Economic-policy/small-business-policy,did=76812.html (01.12.2011)

Deutsche Gesellschaft für Qualität DGQ (Hg.) Informationsmanagement-Beauftragter. http://dgq.de/weiterbildung/informationssicherheitsmanagement-beauftragter.htm

E-Commerce-Center Handel (Hg.): Netz- und Informationssicherheit in Unternehmen 2011. Management Summary. http://www.kmu-sicherheit.de/fileadmin/kmu-sicherheit/publikationen/studien/Management_Summary_Netz-_und_Informationssicherheit_WEB.pdf (01.12.2011)

Duscha, Andreas, Maria Klees, Reinhard Weisser: Netz- und Informationssicherheit in Unternehmen 2011. Ergebnisse einer Befragung von kleinen und mittelständischen Unternehmen in Deutschland. http://www.kmu-sicherheit.de/fileadmin/kmu-sicherheit/publikationen/studien/Studie_Netz-_und_Informationssicherheit_2011.pdf (01.12.2011)

Spindler, Prof. Dr. Gerald: Verantwortlichkeit von IT-Herstellern, Nutzern und Intermediären. Studie im Auftrag des BSI durchgeführt von Prof. Dr. Gerald Spindler, Universität Göttingen. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Recht/Gutachten_pdf.pdf;jsessionid=FD960883131DDA6B6B2F5EE820CE83A1.2_cid251?__blob=publicationFile (02.12.2011)

Statistisches Bundesamt (Hg.): Kleine und mittlere Unternehmen, Mittelstand. http://www.destatis.de/jetspeed/portal/cms/Sites/destatis/Internet/DE/Content/Statistiken/UnternehmenGewerbeInsolvenzen/KMUMittelstand/Aktuell,templateId=renderPrint.psml (01.12.2011)

TÜV Rheinland (Hg.): Datenschutzassistent. / Datenschutzbeauftragter. / Datenschutzmanager. / Datenschutzauditor. / Externer Datenschutzbeauftragter. / IT-Grundlagen für Datenschutzbeauftrage. / Datenschutz Update – Fortbildung für Datenschutzbeauftragte. / Erstellen und Pflege des Verfahrensverzeichnisses. / Professioneller Umgang mit Datenpannen. / Datenschutzrecht in der Personalabteilung. http://www.tuv.com (11.10.2011)

9) Complete National Report Spain

9.1) National Rules & Regulations Concerning Information Security in SME

As main regulations of the Information Security in business, we analyzed first the legislation, which affects the development of entrepreneurial activities involving SMEs and explicitly implementing security measures systems information. The legal framework concerning Information security is established by the following legislation:

- Ley Orgánica 15/1999, on Personal Data Protection.
- BOE de 14 de dismember (in advanced LOPD).
- Real Decreto 1720/2007 by approving the regulation implementing of the Organic Law 15/1999, of December 13, the Personal Data Protection
- Directive de la Unión European 95/46/CE, on protection of people regard to treatment personal data and freedom of movement (DOCE 24-VII-1995).
- Ley 34/2002, on society services information and electronic commerce (LSSICE).

To complement the existing legislation on personal data protection, currently exists the international standard UNE ISO/IEC 27001 which is configurated as a standad about auditing aspects of Information Security in organizations.

And the standard UNE 71599 / Management BS 25999 Business Continuity, which will establish a management system for effective business continuity in a company, based on a code of best practices for implementation and continuous improvement. The requirements developed on both sides will allow you to identify potential threats to the organization, its impact if it occurs and an efficient response to protect the interests of your organization. The Management of Business Continuity is a complementary element of risk management, to combine risk analysis with the ability of the organization to continue functioning without interruption.

9.2) Vocational and Continuing Education and Training

9.2.1) Overview of Existing Training Offers in the Field of Information Security

Name	Main Content / Objective	Target Groups	Preconditions / Requirements	Kind of Testimonial
Fundamental of service life cycle IT + ITIL Foundation V3 official certification	This course introduces the concepts of IT Service Management (ITSM) based on Version 3 IT Infrastructure Library (ITIL)	Aimed at professionals who are familiar with the environment of Information Technology, to all staff that is related to IT Service Management, as well as other professionals who want to gain insight into the processes and procedures of best management practices IT Services	none	
Course Strategy and Innovation expert in ICT.	ICT Portfolio, meet legal and regulatory framework.	The course is for professionals interested in the new crimes committed by computer or information technology and telematics.	None	
ICT Quality Training Pack	This course is designed to provide knowledge of what a management system for IT services, the minimum requirements that must aspire providers of service within the context of ISO / IEC 20000.	To all staff of any INFORMATION ORGANIZATION handled and who wants to acquire knowledge in information security. In a variety of professionals such as IT operations staff, supervisors, senior consultants, managers, executives and auditors.	None	
Course management systems information security UNE ISO IEC 27001	Introductory Course Management Systems Information Security (ISMS) according to UNE-ISO/IEC 27001 Information Security in an Organization, based on ISO / IEC 27001	To all staff of any organization that handles information and want to acquire knowledge in information security. In a variety of professionals such as IT operations staff, supervisors, senior consultants, managers, executives and auditors.	None	
Course of Data Protection: Compliance and Enforcement	Introductory course to the various aspects and facets of the Data Protection from the point of view of the adequacy and compliance.	Focus on SMEs, but given the generality of the concepts and ideas discussed, may also be aimed at all types of organizations	none	

Course of Introduction to Information Security	Introductory course to the various aspects and facets of Information Security.	Focused on SMEs, but given the generality of the concepts and ideas covered, also can be targeted at all types of organizations.	None	
Introductory course on the protection on the Internet	Introduction to protection on the Internet, through the various threats, risks and solutions.	Focused on SMEs, but given the generality of the concepts and ideas covered, also can be targeted at all types of organizations.	None	
Introductory course to the work protection	Introductory course on the protection of work, organizations and business-oriented.	Focused on SMEs, but given the generality of the concepts and ideas covered, also can be targeted at all types of organizations.	None	
BS25999 business continuity training	The continuity of the business	Business continuity managers. Responsible for risks. Head of quality. It managers. Information security professionals. Auditors who shall be responsible for audit business continuity operations	none	

9.2.2) Overview of Existing Information Services Regarding Information Security

Provider	Kind of Service	Target Groups	Terms of Use	URL / Contact
S21SEC	Compliance. Compliance with legislation	Medium-sized enterprises (50-249 employees) Big-sized enterprise (>250 employees)	Services designed to ensure compliance with legislation, regulations and safety standards that apply to organizations based on their activity. The objective is to align the security management with the achievement of the objectives of business as well as assist those responsible for security in their work as managers of the technological risk. Advice for the implementation of systems of management of information security (ISMS), based on the ISO/IEC 27001 and ISO/IEC 27002	www.s21sec.com
S21SEC	Assessment. Technical auditoria	Small-sized enterprise (10-49 employees) Medium-sized enterprises (50-249 employees) Big-sized enterprise (>250 employees)	Security auditing services increase the integrity of information systems, eliminate illegal accesses and prevent information theft, loss of productivity or fraud in organizations.	www.s21sec.com

S21SEC	E-Crime.Incidents management.	Medium-sized enterprises (50-249 employees) Big-sized enterprise (>250 employees)	Services for the detection and resolution of incidents affecting organizations, mainly due to the proliferation of criminal activities on the Internet, cybercrime and fraud online, 24 hours 365 days a year.	www.s21sec.com
S21SEC	Intelligence. Outsourcing of security services	Medium-sized enterprises (50-249 employees) Big-sized enterprise (>250 employees)	Aimed at a better understanding of the opportunities and threats of the business, technology and services facilitate the optimization of the processes of decision-making and help to achieve greater competitiveness through knowledge and capacity to adapt to sudden changes	www.s21sec.com
S21SEC	Cert.Incidents management	Medium-sized enterprises (50-249 employees) Big-sized enterprise (>250 employees)	Services offered 24 x 7 x 365 from the CERT for proactive management of security risks, monitoring compliance with standards and regulations and identification, analysis, and mitigation of security threats.	www.s21sec.com

Website where you can find companies related with security services:

http://cert.inteco.es/searchSuppliers/Catalogo_STIC/Catalogo/Busqueda_de_Empresas/?postAction=searchSupplierFromSearchEngine

9.3) Description of Target Group

9.3.1) SME (in general)

SMEs: entrepreneurs and employees of micro, small and medium enterprises.

Microenterprise is a company that has fewer than 10 employees and a turnover or annual balance less than 2 million Euros. Generally, these companies do not have computer experts or internal security. Their number varies from one Member State to another, for example in Spain tends to be formed by less than five people.

Small business: a company that has fewer than 50 employees and a turnover or a balance of less than 10 million Euros. The definition of small business also varies from one Member State to another. A small business may or may not have a computer expert and is unlikely to have an expert in information security

Medium enterprise: a company that has fewer than 250 employees, whose annual turnover not exceeding EUR 50 million and / or annual balance sheet is less than or equal to 43 million Euros. The definition of medium enterprises varies from Member State to another. Generally, midsize companies have a computer expert and can have someone who is knowledgeable about information security.

How are SME of this kind generally organised?

SMEs in Spain are often family businesses. These SMEs tend to have more traditional features, including an attachment to the hierarchy within the organization. The hierarchy in Spanish SMEs is seen as a positive and a lack of respect to any existing hierarchy can be viewed negatively.

The majority of SMEs are operating in the services sector, followed by commerce.

By economic sectors, the size of SMEs varies significantly. The higher proportion of large firms is concentrated in the sector "other services" followed by the industry, while the smaller cluster in the field of commerce and services.

Regarding the legal form, the individual is the predominant form in the creation of an SME, limited companies is the second most take legal Spanish SMEs, and community property is the third. Fourth place is the public limited companies that are losing weight with respect to the above.

Other data about Spanish SME are:

- SMEs in Spain, accounting for 99% of the business, generating 90% of jobs.
- In Spain there is a higher rate of creation of SMEs in Europe, as well as a higher rate of destruction. The net creation of companies is lower in Spain than in Europe.
- In Spain there are about 7 SMEs per hundred inhabitants.
- The business with zero employees constitutes 52% of companies.
- Very small enterprises between 0 and 10 employees account for 94% of all enterprises.
- Small enterprises between 10 and 49 employees are 5%.
- Medium-sized enterprises between 50 and 249 are 0.70%.
- Just over 60% are individuals.
- About 27.5% are limited companies.
- Between 4 and 5% are public limited companies
- Communities of property, cooperative societies and other legal forms about 8%.
- The importance of SMEs in the social network in Spain is very high. Just as the significance of the contribution of microenterprises.

The majority of SMEs are operating in the services sector, followed by commerce. Therefore, that is why in these two activities, which should be directed our target.

What are the main interests of SME of this kind (in general and regarding Information Security in particular)?

Regarding the use of technology and information systems, their use has positioned itself as a catalyst for economic growth based on increasing the competitiveness and productivity, with numerous initiatives in the public sector aimed to facilitate access to ICT as part of the main actors in the Information Society.

Ultimately, the threats and contingencies can affect all types of businesses regardless of size or condition. The wide range of these makes that their source can be motivated by their business risks, disasters (e.g., terrorist attacks, tornadoes, earthquakes, floods, etc.), Or even due to everyday situations that have their source in components installation (power outages), computer equipment (malware, problems with hardware or software) or in those with a human component (intentional sabotage, phishing, dissatisfied employees and partners, distraction and / or errors).

All these constraints mean that at present the companies and thus SMEs are facing multiple challenges that can be seen as a challenge in management of information security and in the operations or activities that are carried out continuously and without apparent interruption. One of them is to design and/or develop plans associated with technologies and processes necessary to recover as soon as possible, critical operations to ensuring business continuity in case of a disaster.

There are multiple reasons that lead companies to consider the management of Information Security, regulatory requirements or the partners themselves and/or customers, strategies to increase competitiveness and profitability, the dependence of business activities in the ICT, and so on.

What are potential risks regarding Information Security?

As indicated in the report (1) published by INTECO entitled "Study on e-security and confidence of small and micro Spanish companies", 34.3% of Spanish SMEs are interested in following plans or strategies in information security. And even it may seem at first glance that there is a good level of protection. However, most SMEs recognize not to know the risks inherent to their activity.

Spanish SMEs in relationship with the risks and the implementation of Security Plans for Information, in such cases choose for solutions that cover only part of the problem.

According to the SMEs themselves, most of their investments are designed to provide firewall, antivirus, antispam and backup. These measures only mitigate a small part of the risks, leaving aside other aspects such as, for example, physical safety or continuity of services provided by suppliers.

Other factors seen in the study and that again denote the degree of immaturity in terms of continuity of the organizations are:

- Low level of implementation of actions related to the adoption of risk management processes after an incident (35.4 per cent of institutions have adopted this kind of process).
- Absence of business continuity requirements to suppliers who provide critical services for your business (18.7% of institutions require their suppliers such measures).
- Ignorance about the economic losses suffered security incidents.
- Lack of uniform criteria for the correct assessment of the impact and the probability of occurrence of each of the threats that may affect the continuity of the business.

The situation of SMEs is special, because it should focus on the production of every day, and simply the task of maintaining its business activity and survive in the business world, becomes his main target. This priority objectives leads to other important aspects such as the information security management to be forgotten, or at least, in the background.

INTECO: Study on safety and e-confidence of small and micro-Spanish. Available in: http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Estudios_e_Informes_1/Estudio_seguridad_microempresas)

9.3.2) Persons to be Trained (in particular)

Target group, qualification and prerequisites

As a general rule will be defined the responsibilities mentioned in the following sections. It must be taking into account that these responsibilities will be a reference model that will serve as guidance in the development of the structure of any organization's security.

Director/owner: the person who takes the main decisions on investments in security.

Head of the information technologies – these users have technical training but they may not be security experts, but they must understand and implement information security protocols.

Sales management - this group of users, which often has no technical training, need to be trained to understand the importance of information security, in order to implement the policies and the relevant security checks in their operating areas.

Employees: this group is a greater number of users in the target group and is certainly the most important. The majority of violations of information security are caused by human error and/or lack of training.

What work assignment / job will this person have most likely?

Direction: a figure by integrating the following functions:

- Entity responsible for the files (if there is personal data)
- Responsible of the information
- Responsible of the company service

Supervision: a figure, reporting to Direction

- The Information Security Officer (IS Officer)

Operational: a figure, reporting to management, and integrating the following functions:

- Responsible of operating with the data

Profile of an IS Officer

The head of the information system is usually a person who occupies a high position in the direction of the organization.

Responsibilities:

1. Maintain the security of managed information and services provided by information systems in its area of responsibility, as established in the security policy of the organization.
2. Promote training and awareness in the field of security of the information within his scope of responsibility.

3. Develop, operate and maintain the information system throughout their cycle of life, their specifications, installation and verification of proper operation.
4. Define the topology and the system of information management system by establishing criteria of use and the services available therein.
5. Make sure that the specific security measures are properly integrated within the overall framework of security.
6. The implementation, management and maintenance of the security measures applicable to the information system.
7. Management, configuration and update, if any, of the hardware and software underlying mechanisms and security services of the information system.
8. Management of authorizations granted to users of the system, in particular the privileges granted, including the monitoring that the activities carried out in the system conforms to authorize.

9.4) Resume

In conclusion

- Organizations, whether public or private, are storing and disseminating an increasingly vast amount of information by electronic media. Nowadays we have a strong dependence on Information Technology.
- In addition, companies have experienced an extraordinary increase in the use of Internet services. So, these tasks are becoming important part of business. Not to be present on the Internet can backfire for the business objectives.
- The increasing use of systems for storing and processing the information becomes more important fact to keep it safe.
- One of the main duties for any organization is to ensure that staff acts correctly.

What could be a good starting point to address our target group?

The main objective of INSEMOT should be awareness of the information security both SMEs and the public institutions of the EU. And it is therefore necessary that our main objective is the awareness of senior management regardless of the sector in which to operate. Awareness and understood is an essential part of good business practices in the field of security. She refers as a prerequisite in various international standards such as ISO 27001.

Where will the INSEMOT SME products fit in to?

Standards of good practice emphasize much on the need to implement a security policy that covers the entire organization. Thus, ISO 27001 recommends that organizations take training and awareness programmes. Managers must meet the requirement of ensuring that staff under their command applies security pursuant to a pre-existing guidelines. To meet this objective, they must provide adequate awareness training, and regularly update policies and procedures of the organization. It is in this section, where the development of INSEMOT products have greater meaning and usefulness.

What do we have to keep in mind while developing our products?

Business needs change as evolving use of technology.

The priority that regulatory bodies of EU Member States attach to security is growing.

Every day emphasizes high levels of criminal activity on the net, registering an increase of fraud based on the usurpation of identity, spam, robot networks, Trojan attacks,...

Customers have become now more receptive to the problems of security and this affects the possibilities of business in the SMEs

The usurpation of identity constitutes an increasingly widespread security risk. Organizations that store and manage personal identification data must take precautions to ensure your confidentiality and integrity.

9.5) List of References

http://cert.inteco.es/searchSuppliers/Catalogo_STIC/Catalogo/Busqueda_de_Empresas/?postAction=searchSupplierFromSearchEngine

INTECO: Study on safety and e-confidence of small and micro-Spanish. Available in: http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Estudios_e_Informes_1/Estudio_seguridad_microempresas

10) Complete National Report Ireland

10.1) National Rules & Regulations Concerning Information Security in SME

The main Irish law dealing with data protection in SMEs is the Data Protection Act 1988. The 1988 Act was amended by the Data Protection (Amendment) Act 2003 which brought Irish law into line with the EU Data Protection Directive 95/46/EC.

The office of the Data Protection Commissioner in Ireland (dataprotection.ie) is responsible for ensuring that people's rights are respected, and that the persons who keep personal information meet their responsibilities. Under section 10 of the Data Protection Acts, 1988 and 2003, the Data Protection Commissioner may require a data controller or data processor to take whatever steps the Commissioner considers appropriate to comply with the terms of the Acts.

Data controllers are those individuals or organisations (companies, government departments and voluntary bodies) entrusted with personal data by members of the public and they carry the main responsibility for the creation of a safe environment for the processing of personal data.

Data processors hold or process personal data, but do not exercise responsibility for or control over the personal data. Unlike data controllers, data processors have a very limited set of responsibilities under the Data Protection Act. These responsibilities concern the necessity to keep personal data secure from unauthorised access, disclosure, destruction or accidental loss.

Certain categories of data controllers and data processors are required to register with the Data Protection Commissioner. Registration must be renewed on an annual basis.

10.2) Vocational and Continuing Education and Training

10.2.1) Overview of Existing Training Offers in the Field of Information Security

Name	Main Content/ Objective	Target Groups	Preconditions/ Requirements	Kind of Testimonial
Griffith College Dublin, in assoc. with QCC IS (qccis.com) & Royal Holloway University of London	Postgraduate Certificate & Diploma in IS. (Part-Time Modular training). Topics include: Systems Security/Risk Assesment/ Cyber Crime/ Incident Response & Investigations	People seeking employment as IS experts (Professional career foundation courses)	There are no academic pre-conditions for these courses. Fee: Up to £2,000 for Diploma course	Not Available
The Institute of Technology in Blanchardstown (ITB), Dublin	MSc in Computing in IS & Digital Forensics (1 Yr Full-Time)	Undergraduate degree holders seeking to develop knowledge and skills	Applicants must have an primary degree (a minimum 2nd class honours), in a relevant	Not Available

	Topics include: Network Security/ Business Continuity & Disaster Recovery/Biometrics/ Secure Communication & Cryptography/ Cyber Crime Investigation	appropriate for careers in IS & Digital Forensics	discipline. Fee: €4,000	
University of Limerick (UL)	Masters of Engineering (MEng) in Information & Network Security. Topics Include: Communication & Security Protocols/ Data Forensics/ Biometrics	Undergraduate degree holders seeking to become technical leaders & researchers in IS systems management	Applicants must have an primary degree (a minimum 2nd class honours), in a relevant discipline. Fee: Unknown	Not Available

10.2.2) Overview of Existing Information Services Regarding Information Security

Provider	Kind of Service	Target Groups	Terms of Use	URL / Contact
The office of the Data Protection Commissioner	Web portal Offering advice on how to comply with national Data Protection legislation	Irish Businesses & Consumers	Free-to-use Web portal, with telephone helpdesk, email support	dataprotection.ie Canal House Station Road Portarlington Co. Laois, Ireland +353 57868 4800
Irish Reporting & Information Security Service (IRISS)	Independent, not-for-profit company formed in 2008 to provide IS services to Irish businesses & consumers	Irish Businesses & Consumers	The service is provided free of charge by volunteers / IRISS is funded by a combination of donations and corporate sponsorship	iriss.ie info@iriss.ie @irisscert Suite B011 The LINC Centre Blanchardstown Road Nth, Blanchardstown Dublin 15, Ireland +353 1 440 4065
Information Security Ireland (ISI)	In 2009, six Irish IS companies established ISI as a networking body for their industry	Irish & multinational companies providing IS technology, research institutes developing IS technology, third level colleges providing IS education & industry associations	Annual Membership [€500-€2,500]	Infosecurityireland.org @InfoSecurityIre Enterprise Ireland East Point Business Park, Dublin 3, Ireland T: +353 1 727 2000 F: +353 1 727 2020
Information Systems Security Association (ISSA) - Irish Chapter of Global Organisation	Since 2003, ISSA Ireland has organised seminars for Irish IS professionals	IS Industry professionals, managers & executives	Annual Membership costs c. €180	issaireland.org info@issaireland.org @ISSAIreland

10.3) Description of Target Group

10.3.1) SME (in general)

An overview of business (by size) in Ireland

As reported by the European Commission's Small Business Act (SBA) Factsheet for Ireland (2010/11), of the 87,231 enterprises recorded in Ireland, 82.6% are classified as micro-enterprises; 14.2% are classified as small businesses and 2.6% are classified as medium enterprises. The report notes that "Ireland's economy has relatively higher concentrations of small, medium-sized and large businesses that the European Union average, where micro firms are comparatively more prevalent."

A profile of the Irish businesses that the INSEMOT SME project will seek to support

Dun Laoghaire-Rathdown County Enterprise Board (DLR CEB) will use its participation in the INSEMOT SME project to enhance the IS management capabilities of micro-enterprises operating across a range of business sectors. As a state enterprise development agency, DLR CEB has a statutory mandate to assist new and expanding businesses which employ no more than 10 employees. Our organisation's catchment area is Dun Laoghaire-Rathdown County, a local government region with c.200,000 citizens.

Our organisation has experience of working with promoters of each of the most common business structures (sole trader, partnership and limited liability companies). Sole traders will typically take responsibility for the majority of business management activities. It is in the case of partnerships (where work functions are split between two or more partners) and limited liability companies (where functional units are more likely), that we begin to observe the emergence of strict work assignment.

Attitudes of SMEs and Microenterprises to IS Issues

It is our organisation's experience that issues surrounding IS and data protection do not feature as a priority for many small businesses owners, particularly those that are in the early stages of development. Ventures in start-up mode are typically pre-occupied with raising finance, forging partner relationships, securing sales and, in some cases, building a team of professionals. As a consequence, issues relating to IS systems and procedures tend to get overlooked. The principal challenge facing the partners in the INSEMOT SME project is to challenge this mindset.

The role played by ISO 27011 Certification in Ireland

Our designated IS expert advises that government-issued tenders do not typically require respondents to possess ISO 27001, the highest internationally recognised IT security standard. It is important to note, however, that the authors of these tenders will take into account the IS capabilities of the respondent company in their scoring criteria. If the respondent business is clearly acting as a Data Processor then issues of IS will become a feature of the sales process. In those industries characterised by the processing of large quantities of personal data, such as healthcare and financial services, these issues are likely to be more prelevant.

There is no shortage of private companies offering training and consultancy services in ISO 27011 certification. There are also resources available on social media platforms which may be of interest to the SME sector. One such example is a LinkedIn Group 'ISO 27001 Ireland & UK', which provides information from experienced ISO 27001 certification auditors to first-time and experienced users alike.

Responsibility for IS within SMEs and Microenterprises

In well-resourced large companies, it is the board of directors, management (of both business lines and staff), and internal audit functions that must share the responsibility for ensuing that robust IS policies are in place.

The situation with SMEs and Microenterprises is often strikingly different. Smaller businesses are frequently exposed to IS risks because they may not benefit from the oversight provided by an experienced Board of Directors and may not have full-time information security staff. Without in-house IS expertise, such businesses are unable to track developments in the security landscape. As a consequence, it is more typically the responsibility of the Managing Director to draft and implement the IS policy.

The Organisation of IS systems within SMEs and Microenterprises

It our observation that IS systems, where they are found to be present in our micro-enterprise client businesses, are organised on an ad-hoc basis, often in response to a security breach that has already occurred. It is often only in the case where the Managing Director has prior experience of IS or where the business is operating in a sector where IS is a priority, that you will find a structured approach to the protection of confidential data.

Overview of IS Risks

Small businesses typically don't have in place appropriate protocols for safeguarding their confidential data. Within entrepreneurial businesses at start-up stage, information is frequently transferred verbally, or through email, and formal policies and procedures are not implemented until the organisation starts to grow.

Examples of Best practice

- Systems and networks protected from loss/misuse of data by viruses, spyware etc.
- Secured internet connection / firewall on all business systems
- Important business data/information backed-up daily
- Physical access to the IT network components controlled
- Individual user accounts for each employee on network
- Written policy documents regarding the handling of data
- Proper vendor management

Examples of worst practice

- Confidential information left unsecured e.g. laptops, memory sticks, CDs, printed material in filing cabinets, website content
- The absence of a regular risk assessment audit and/or any written procedures
- Failure to control staff and/or visitor access within business premises

It is well documented that cloud computing represents one of the most significant shifts in the short history of information technology. It is equally clear that cloud computing is fraught with security risks. Businesses must be alive to the risks which flow from the loss of direct control over data for which they are ultimately accountable. It is our view that the INSEMOT SME project needs to make this issue a headline message.

10.3.2) Persons to be Trained

The staff members that will be targeted by the INSEMOT project

We believe the training should be directed at the Owner/Manager or Managing Director of each business, particularly so in the case of microenterprises. The training must be offered to this individual in the first instance; they can then choose to send a delegate, such as an IT Director/Manager or Marketing Director/Manager, in their place.

The IS qualifications & infrastructure that can be expected in the target group

We make the following observations:

- It is a fair assumption to make that the vast majority of our target group is unlikely to possess any formal qualifications in the area of IS
- It is our view that the training recipient will be either be a General Manager or perhaps have responsibilities in the area of IT or Marketing
- We cannot assume that any IS procedures will be in place in our target market
- It is too early in the project to comment with any confidence on the kind of IS qualification a training recipient is likely to need. It may be the case that the achievement by the trainee of 1) a working understanding of data protection law and 2) the creation of best practice IS procedures will deliver on the primary objectives of the INSEMOT SME project.

First Draft of profile for an "IS Officer/Manager"

An IS officer is responsible for creating and maintaining the systems needed to ensure information assets are securely protected. This member of staff is responsible for information-related compliance and works to reduce information risks, establish standards and controls, and implement policies and procedures.

10.4) Resume

Report Conclusions

- There is clear legislation in place governing the management of data in Irish SMEs
- Over the past 10 years, a range of state, private and voluntary bodies has emerged to provide information on IS, specific to the needs of Irish consumers & businesses
- There are some postgraduate qualifications on offer in Ireland to people who wish to establish careers as IS experts
- Our organisation, DLR CEB will use its participation in the INSEMOT SME project to enhance the IS management capabilities of micro-enterprises
- Microenterprises in Ireland, in our organisation's experience, tend not to prioritize IS issues. This is particularly true for those businesses in early stages of development.
- An opportunity exists for our target group to pursue ISO 27011 Certification, where the business case is merited. Further research is needed in this regard.
- The security risks created by the growth in cloud computing need to be highlighted
- We cannot assume that either IS procedures or IS qualifications will exist within the operations of our target group of microenterprises

How INSEMOT SME products fits will fit into this landscape

To be effective, the INSEMOT SME products must encourage the trainees to address the following questions:-

- Do you have a IS risk assessment program in place in your business?
- Are you adequately prepared to respond to an IS incident / breach of data?
- Does your business have a business continuity/incident recovery plan?
- Is your business in compliance with data protection legislation / is it obliged to register with the Office of the Data Protection Commissioner (or equivalent body)?
- How robust are your IS policies and procedures?
- What types of tools are you currently using to monitor IS risks?
- Do you know whether your partners and vendors have IS policies in place?
- Do you have IS awareness training in place for your employees?
- Do you see the value in having a designated 'IS Officer/Manager'?
- Could your business survive the financial and/or reputation loss which may result from an IS breach?

A recommended starting point to address our target group

We recommend, as a starting point, the creation of a short online questionnaire which acts an summary risk assessment audit for the training participants. The questionnaire may pose some of the questions listed in the above section.

The issues that must be considered when developing the INSEMOT SME products

- The reality that many businesses with the target group will not have IS procedures in place and may demonstrate limited understanding of their obligations under relevant IS and data protection legislation, hence the need for an 'entry level' approach
- The likelihood that many businesses with the target group will not have IS procedures in place and may have little or no interest in implementing such procedures, occupied as they are with what they consider to be more pressing business concerns
- The likelihood that the owner/manager will be time-poor and will not have the resources to research and address IS failings
- The possibility that the owner/manager will not have the financial resources to act upon the findings of any IS audit

11) Complete National Report Italy

11.1) National Rules and Regulations concerning Information Security in SMES

The National ICT sector regulatory framework is in constant and rapid evolution due to the increasing importance of "information" in all fields and its appropriate protection and security in compliance with current regulations.

Among the most significant legal issues in the ICT sector, there is the Law of 18th March 2008 number. 48, with which Italy ratified the Council of Europe Convention on Cybercrime, signed in Budapest on 23rd November 2001. This international agreement concerns crime through the Internet or other computer networks.

The before mentioned law introduces important changes to the Code of Criminal Procedure to Decree Law 231/2001 on the administrative liability of legal persons and to the Decree Law 196/2003 on the processing of personal data, the Privacy Code.

(please see the text of Decree Law 30th June 2003, n. 196 "Code on protection of personal data", published in the Gazzetta Ufficiale No. 174 of 29th July, 2003 – Ordinary Supplement No. 123 and available on the website of the "Chamber of Deputies" in the special section on laws/proxies at the following internet address: http://www.camera.it/parlam/leggi/deleghe/testi/03196dl.htm)

In Italy, the protection of confidential data is not optional; in businesses, the Legal Representative is obliged to take all necessary measures to ensure a suitable level of security in line with the value of the data even in the case of companies that are not subject to notifying the privacy guarantor (art. 37 D. Law 196/03).

The Privacy Code (Decree Law no. 196/03) imposes strict security measures to control anyone who comes into contact with 'personal' or 'sensitive' data on natural or legal persons, to ensure that data is not used improperly or unduly disclosed.

Decree Law no. 196/2003 states that the Document on Security Planning (DPS) of companies, that is compulsory, be attached to the annual budget, and is subject to periodic review (at least every six months) and possibly prepared before 31st March of each year.

According to current Italian law every company should:

- provide, prepare and implement (periodically checking validity and appropriacy) what is necessary as regards information security in line with latest regulations;
- check that what they have is sufficiently technologically advanced to tackle any critical issues that may arise;
- ensure that staff use these technologies on a daily basis;
- demonstrate use by analysing periodical reports;
- monitor responsibility in the case of critical system issues;
- have business continuity management;
- ensure compliance.

(for further information on the Document on Security Planning – DPS – please see what is published at the following internet address http://www.tecnologieinformatiche.com/dps.html)

A very recent legal obligation (30th November 2011) regards Certified E-mail. (PEC – Posta Elettronica Certificata).

Decree Law of 29th November 2008, n. 185, states that companies have to inform the Companies Register of their certified e-mail address.

Certified e-mail (also known as "certified mail" or "PEC") is a communication system similar to ordinary e-mail, but that, as well as having security and transmission certification, also has legal effects.

In fact the PEC is recognized as having full legal value and receipts can be used as proof of sending, delivery and even the contents of the message sent.

The main information concerning transmission and delivery is retained by the organisation for 30 months and it, too, is valid for third parties.

Pleae note that transmission is considered certified e-mail only if both parties have PEC boxes, even if they belong to different managers.

Not communicating your PEC address leads to suspension of the registration procedure at the Companies Register and if you do not communicate it your registration can be refused.

(*to see the integral text of Decree Law 29th November 2008, n. 185, please use the following internet address:* http://www.tesoro.it/documenti/open.asp?idd=20301)

The International Standardization Organization (ISO) is issuing a series of norms on Information Security that try to help organisations in Information Security Governance and to improve trust and relationships between businesses (B2B – Business to Business) or between businesses and consumers (B2C – Business to Consumer). The founder of this norm is ISO/IEC 27001:2005 – Information Technology – Security Techniques – Information management systems- Requisites, that entered into force in Italy in 2006.

The ISO/IEC 27001:2005 is a management standard used to certify the "Sistema della Sicurezza delle Informazioni" (SGSI that corresponds to the English ISMS – Information Security Management System) of bodies and companies.

Information security management systems, in fact, as well as considering technical aspects, also bear in mind those relating to human resource management, organisational processes and physical spaces.

The ISO/IEC 27001 concerns the secure management of all corporate information assets and electronic and paper media and defines information security in terms of preserving integrity, availability and confidentiality.

The ISO/IEC 27001 is an auditable and certifiable standard (via its requirements), while all the rules that constitute the ISO 27000 family are guides to support ISO/IEC 27001 and, therefore, not subject to certification, but are used to support ISMS implementation.

Currently the ISO 27000 family consists of:

ISO/IEC 27001:2005 – Information Technology – Security Techniques- Information management systems- Requisites

ISO/IEC 27002:2005 – S.G.S.I. Practical advice

ISO/IEC 27005:2008 – S.G.S.I Management risks

ISO/IEC 27006:2007 – S.G.S.I Guidelines for Accredited Certification Bodies

(for further information on information security and ISO 27000 Norms please see what is published on the following site:

http://www.mondodigitale.net/Rivista/08_numero_3/Rub.%20Piva%20%20p.%2059-65.pdf)

Here follow some other current norms in Italy that concern Information Security:

Copyright Law 248/2000 (please see the text of Law 18th August, 2000, No. 248, "New regulations on copyright protection", Published in the Gazzetta Ufficiale No. 206 of 4th September, 2000, and available on the "Chamber of Deputies" site in the special section on laws at the following internet address: http://www.camera.it/parlam/leggi/00248l.htm)

Industrial and Intellectual Property Decree Law 30/2005 (see the text of Decree Law 10th February 2005, No. 30, "Industrial Property Code, according to article 15 of Law 12th December, 2002, No. 273," published in the Gazzetta Ufficiale No. 52, 4th March, 2005 – Ordinary Supplement No 28 available on the site of the "Chamber of Deputies", in the laws/proxies section, at the following internet address: http://www.parlamento.it/parlam/leggi/deleghe/05030dl.htm)

Administrative transparency Decree Law No. 231/2001 (see the text of Decree Law 8th June, 2001, No. 231 "Regulations of the administrative responsibility of legal entities, companies and associations, including those without legal status according to Article 11 of the Law of 29th September, 2000 No. 300," published in the Gazzetta Ufficiale No. 140 of 19th June 2001 and available on the website of the "Chamber of Deputies", in the laws/proxies section, at the following internet address:http://www.camera.it/parlam/leggi/deleghe/testi/01231dl.htm)

11.2) Vocational and Continuing Education and Training

As Confindustria ("General Confederation of Italian Industry") has testimonied in the guide to "**Business and professional skills for digital innovation**" (for further information please see the attached pdf document: "Competenze e professionalità Aziendali per l'innovazione Digitale –Business and professional skills for Digital Innovation"), in Italy, ITC oriented vocational training has its foundations in the **EUCIP - European Certification of Informatics Professionals**, the European reference framework for computer skills and vocational profiles.

EUCIP was developed with support from the European Community, by European professional associations part of CEPIS (Council of European Professional Informatics Societies), including the AICA (Italian Association for Informatics and Automatic Computation)

EUCIP is a system that is independent of its suppliers that thanks to the availability of a complete set of certification of ICT skills required for each ICT trade, is already a reference system in the world of computing professions, businesses and training organisations.

In this regard, Confindustria Servizi Innovativi e Tecnologici -Innovative and Technological Services has sent a document to the Government containing proposals for the Documento di Programmazione Economica e Finanziaria 2009-2011 (Economic and Financial Planning Document 2009-2011), where it suggests adopting EUCIP as a

reference standard for training policies and development of ICT skills connected to the business world. The document can be downloaded from the Confindustria website

http://www.confindustriasi.it/index.php?cont=login

on the page containing proposals for the DPEF (Documento di Programmazione Economico Finanziaria) 2009-2013. Furthermore, for further information on the relationships between AICA/CONFINDUSTRIA and the EUCIP model – please see what is contained in the pages of the AICA site http://www.aicanet.it/certificazioni/eucip

http://www.eucip.it/proposta-di-confindustria-per-adozione-di-eucip

The EUCIP standard is divided into **21 vocational profiles** to which you should add the IT specialist Administrator profile (designed especially for small to medium sized organizations), that have "Core" EUCIP - the set of basic skills that every professional and IT manager should possess.

Two levels of certification were defined for the EUCIP standard. The first **("core")** certifies the possession of the fundamental skills that are a prerequisite for the specialist.

The second which is **"elective"** certifies the specialist skills for each of the 21 profiles and for the specialist one (IT admin), reserved for those who do or will undertake one of these professions.

In particular, the **EUCIP - European Certification of Informatics Professionals**:

- is designed as a reference framework to certify ICT skills;
- is the basis to design certified professional development and global management courses of the patrimony of personal and organizational skills;
- can identify and measure weak areas **("skills gaps");**
- provides a unique reference curriculum framework for students, workers and businesses, as well as staff working in training, so that they can better target and promote their offer;
- completes the European system of ICT skills certification, which ranges from basic skills to professional level;
- is recognized by the system of Italian Universities (*Consorzio Interuniversitario Nazionale per l'Informatica* -CINI Interuniversity Consortium for Informatics), which has signed specific agreements with the AICA to diffuse EUCIP;
- is recognized by the business system (Confindustria) and by large public organizations;
- is integrated in the "Guidelines" of DigitPA (formerly CNIPA) for ICT contracts for the Public Administration;
- is integrated in the "Thesaurus" of the Ministry of Labour, adopted by the Regions to define professional standards;
- is the subject of collaboration with leading ICT providers to link up with their respective certification systems.

Please note the important contribution of the **European e-Competence Framework (e-CF)** which is the ICT skills reference framework, used in Europe by ICT companies, ICT professionals, managers and HR departments, Public Administrations, people working in the world of education and social partners.

The framework was developed within the CEN Workshop on ICT Skills, by a large number of European experts in ICT and Human Resources (HR).

Italy was represented in the European e-Competence Framework Expert Workgroup by experts from the Bank of Italy, Cap Gemini, CPI Competenze per l'Innovazione and the Polytechnic of Milan.

The efforts made in the four years work have been recognized in the European Commission Communication on "e-Skills for the 21st Century: Fostering Competitiveness, Growth and Jobs" in September 2007 and in the conclusions of the "Competitiveness Council" of November 2007.

The European e-Competence Framework (e-CF) provides an international instrument for:

ICT professionals and managers, with clear guidelines for their professional development

HR managers, allowing the anticipation and planning of competence needs

Education and Training, allowing effective planning and design of ICT curricula

Professionals working in market research and strategy, providing a clear reference agreed at European level, to assess and anticipate skills and ICT competences required in a long-term perspective

The **European e-Competence Framework** is focussed on the competences required to:

- develop, exercise and manage ICT projects and processes
- exploit the use of ICT to the full
- take decisions, develop strategies and forecast new scenarios.

The purpose of the e-Competence Framework is to provide a general and global framework of e-competences that can be adapted and customized to different business contexts such as e-commerce, e-health, e-banking, etc.

In other words, the European e-Competence Framework 2.0 provides a clear, solid and fundamental base for companies to make decisions on staff recruitment, career paths, training, evaluation, etc..

The e-CF is also useful to obtain a better understanding of skills needs of companies.

We would finally like to point out that, even if the **5 levels** of competence of the **European e-Competence Framework** (from **e-1 to e-5**) are correlated to levels **3** to **8** of the EQF - **European Qualifications Framework**, as the **European e-competence Framework** is business-oriented, it uses descriptors for the professional competences required and applied in the workplace and not for qualifications, as is the case for the **European qualifications Framework.**

Therefore, the levels are not identical, as they have different points of view: the **European Qualifications Framework** reflects the point of view of qualifications, the **European e-Competence Framework** adopts the perspective of competence in the workplace.

11.2.1) Overview of existing Training offers in the Field of Information Security

In Italy, there are different types of training provided on Information Security. Among these, it is worth mentioning the **CEFRIEL**, which is amongst the most prestigious cuurently operating as a centre of excellence in research and innovation, as

well as in training within the IT industry (for more information, please visit its official website at the following Internet address: http://www.cefriel.it/index.php/it)

The CEFRIEL is a consortium that was formed following an agreement between three poles: scientific, public and industrial.

The scientific pole is the **Politecnico di Milano "MIP"**, the Business School of the Politecnico di Milano, one of the most prestigious Italian management training bodies accredited by **CEPIS - Council of European Professional Informatics Societies** (for more information, please visit its official website at the following Internet address: http://www.mip.polimi.it/mip/it.html).

The public pole reports to the Lombardy Region, in partnership with the industrial centre consisting of the most important companies in the ICT sector.

The CEFRIEL obtained **REP - Global Registered Education Provider** certification in 2006 from the **Project Management Institute**.

This certification endorses a supplier of specialized training on Project Management, recognizing the high quality of courses for their adherence to international standards for SMEs.

The Project Management Institute (PMI), is the most authoritative body in the field of Project Management at international level. It promotes and administers a certification programme that is of high quality, rigorous, professional and based on a series of tests (certifications).

The CEFRIEL and MIP Politecnico di Milano, offer courses in Higher Education in Information Security Management, which aim to train experts (Information Security Manager or Chief Information Security Officer) to design and manage system to protect information security and business assets.

The course is basically divided into three integrated macro-areas:

- **Technology** (techniques, intrusion, detection systems and firewalls- approaches to business continuity and disaster recovery, security auditing and testing procedures)
- **Management** (all organisational and procedural aspects, as well as economic-management –info security project management)
- **Legal** (legal themes to conform to current norms)

To complement the skills profile of the Information Security Manager, there is a section of the course dedicated to business intelligence for Risk Analysis.

The course aims to train a person to:

- use the latest technology for computer systems and telecommunications networks;
- analyze the cost/benefits of investment in security;
- implement a Risk Analysis;
- design, evaluate and implement a system that is integrated with the core business" that covers all the activities and processes related to Information Security, according to the main reference standards.

The course is for staff who deal with IS and for all those who would like to fill the role of Information Security Manager.

The course is also for managers of information services for small and medium sized enterprises (SMEs) in industry and services, government, and also all specialists in the field of consulting and outsourcing management of networks and information systems.

The registration fee is 5,800 Euros + VAT for personal registrations and 7,000 Euros + VAT for companies or freelancers (for further information please see the brochure at the following Internet address: http://www.securman.it/FLYER_ISM_2011_1a.pdf)

Another important body that provides training on Information Security is **ISACA - Information Systems Audit and Control Association** (for further information, please visit the official site at: http://isacaroma.it/html/Capitolo.html)

Today, ISACA has more than **65,000 members** and can be found in **140 different countries**.

Associates have different roles in the world of Information Technology, such as Information Security Auditor, Consultant, Educator, Security Professional, Chief Information Officer, Internal Auditor. This is a varied world, where IS auditing and control standards of IS itself are the basis.

ISACA in particular provides training for the following professional certifications:

- "**Certified *Information Systems Auditor***" *(CISA)*, that today has more than **50,000 certified professionals**,
- "***Certified Information Security Manager***"*(CISM)*, taken by more than **7,000 people** throughout the world.

ISACA and *ITGI (IT Governance Institute)* have also created the ***COBIT*** *(Control Objectives for Information and related Technology)* framework, which is a series of best practices for Information Technology commonly recognised as a standard approach in the IS sector.

ISACA organizes, at the Dipartimento di Informatica of the Università La Sapienza di Roma, courses on CISM certification. The modules cover:

- Information Risk Management
- Information Security Programme Development
- Information Security Programme Management.

Teachers of the course are professional IS Auditing and IT Security experts who have professional qualifications (CISA or CIA or CISSP) or academic certifications.

The prerequisites for certification are:

- **Qualification** (degree in technical, scientific discipline),
- **5 years proven experience**, of which three in Management in at least three skills areas, a maximum of two years can be substituted by other qualifications (e.g. CISA or CISSP qualification, and other certificates).

Furthermore, acceptance of the ethical code and rules of continuing professional development is of fundamental importance.

The overall average duration of each module is of 16-20 hours.

The course costs on average **500 Euros**.

The Università "**La Sapienza di Roma**" organizes:

- 1st Level Master's Degree courses in "**Security of Computer Systems and Networks for businesses and the Public Administration**" whose aim is to promote the professionalism of those who wish to dedicate themselves to Information Security and offers a preparatory course in all operational strategies for the protection, preservation and restoration of networks and computer systems. Some modules provide expertise in Intelligence and Information Warfare. The Master's course is open to graduates (at least first level) that already work in the computer industry for the Public Administration or for private companies, who wish, without interrupting their work, to increase their professionalism as regards issues on information security of information systems and computer networks, primarily from a technological point of view, but also as regards management, organization and regulation.
- 2nd Level Master's Degree in "**Managing Information Security for Businesses and the Public Administration**", that aims to investigate management, organizational and regulatory aspects of Information Security and provide training to those who want to take, or who have already taken on the responsibility, planning and organization of the information security division of a company or a Public Administration. The Master's course is open to second-level graduates who wish to gain a complete culture about information security, to manage and coordinate from a regulatory and organizational point of view, the security process within the organization and, thus, also deal with any threats caused by malicious use of information technology. The Master's course is both theoretical and practical in the different areas of information security which includes classroom training and project work.
- 2nd Level Master's Degree in "**Governance and Audit of Information systems**" that aims to: encourage the management of information systems, through the study of techniques and methods of governance, operations and performance monitoring systems, thanks to auditing techniques covered. The student will be trained on Cobit, ITIL v.3, PMBOK standards and methodologies and best practices provided by CISA (Certified Information System Auditor) and CGEIT (Certified in the Governance of Enterprise IT). The Master's course is open to second-level graduates already working in the computer industry in government or private companies, who wish, without interrupting their work, to enhance their professionalism regarding issues relating to the management and control of information systems and computer networks, from a management point of view, but also organizational, legal and technological. This is a part-time course, with activities concentrated in classroom training two days a week, grouped into three periods and also carrying out project work during the third period.

The overall duration of each Master's course is 1,500 hours.

For further information you can consult the University's web page at:
http://mastersicurezza.uniroma1.it/

Name	Content/ Objective	Target Groups	Preconditions/ Requirements	Kinds of Testimonials
ISACA	CISM certification course	Graduates Business staff	In-depth knowledge and skills in the IS field	Università La Sapienza di Roma
UNIVERSITA' LA SAPIENZA DI ROMA	1st Level Master's in Security of Information systems and networks for Businesses and the Public Administration	Graduates Business staff	Degree courses in Scientific-technological disciplines	Patronage of the Presidency of the Council of Ministers; CLUSIT (Associazione Italiana per la Sicurezza Informatica-Italian Association for Information Security)
UNIVERSITA' LA SAPIENZA DI ROMA	1st Level Master's in Information Security Management in Businesses and the Public Administration	Graduates Business staff	Degree courses in Scientific-technological disciplines	Patronage of the Presidency of the Council of Ministers; CLUSIT (Associazione Italiana per la Sicurezza Informatica Italian Association for Information Security)
UNIVERSITA' LA SAPIENZA DI ROMA	1st Level Master's in Governance and Audit of Information Systems	Graduates Business staff	Degree courses in Scientific-technological disciplines	Patronage of the Presidency of the Council of Ministers

11.2.2) Overview of existing information services regarding information security

The "Search Security" site is one of the sites of Il Sole 24 ORE Business Media Services, (Reference editorial product for all professionals in businesses and professions with a range of highly specialized content and coverage of all major target groups of the business world). It offers free support and advice for the world of ICT security. Contents (technical Guides, Tips, White Papers, practical tips, news and product market), are considered as reference points for security managers, consultants, security specialists, operators in the world of security. The contents of the "Security Search" site can be consulted at:http://searchsecurity.techtarget.it/

Research conducted on the site shows how several consumer products companies, designed for information security, have created special products designed for the needs of SMEs (partners/sub-providers/end users).

An example is provided by Symantec, a global leader in infrastructure software products with its own network for security and data protection (firewall, antivirus, intrusion detection, data protection), whose **Symantec** Licensing **ExSP** programme allows you to purchase software products based on a monthly subscription model to respond to their specific dimensional requirements, helping them to use their IT budgets to the full, without sacrificing quality or functionality.

This programme is based on technology trends that see the needs of SMEs increasingly going hand in hand with those of large enterprises in terms of security, back up, identity certification, encryption. For this reason, Symantec has already foreseen free courses on endpoint security, encryption, back up, in cooperation with its distributors, and courses on Symantec technologies for SMEs.

On the Symantec website, available at http://www.symantec.com/it/it there is a specific offer of services to "**small businesses**":

"Symantec offers small and medium-sized businesses with 5 to 100 employees and limited IT resources, protection of Enterprise information with speed, flexibility and affordable features that are commensurate with their needs."

Supplier	Type of service	Target Groups	Terms of use	URL/Contact
Symantec	Data security and protection	Individuals/businesses	Payment	http://www.symantec.com/it/it/

The **CLUSIT** (Italian Association for Information Security), offers information and training services on issues relating to Information Security.

Training Services include technical seminars, to which the company can send up to a maximum of 3 employees, and events aimed mainly at SMEs, in cooperation with representatives of large companies in the world of ICT security.

The Clusit offers opportunities to:

- create "video pills" on computer security, posted on the CLUSIT YouTube Channel
- participate in Working Groups
- participate in European projects in the sector
- host interns in the company who are participating in the University Master's courses on Information Security
- have close contacts with the academic world, research communities and the world that supplies ICT security in Italy.

To benefit from these services you need to undersign an annual association fee.

SME Clusit members also have the right to legal consultancy as regards legal requisites. For further information please consult the online brochure at: http://www.clusit.it/newsletter_30_06_07.pdf

11.3) Description of the Target Group

11.3.1) SMEs (in general)

When it comes to IT issues, and in particular Security issues, it is useful first of all to refer to the big difference between a medium-sized enterprise (up to 250 people and 50 million Euros turnover), a small company (up to 50 people and 10 million Euros turnover) and micro enterprise (no more than 10 people and a turnover less than 2 million Euros).

From surveys conducted by ISTAT (year 2008) on the classification of SMEs in Italy, Italian companies in the main have up to 9 members of staff.

Micro enterprises constitute 94.7% of the overall national entrepreneurial network, with 96.6% working in service activities and 82.1% in industry in the strict sense of the word.

Please consult the site "EconomiaFinanza" at the following Internet address:

http://www.economiafinanza.net/istat-in-italia-e-boom-di-micro-imprese

This information can also be found in the document "Small Business ACT –Initiatives to Support SMEs in Italy and in the 27 members states of Europe", Report of 2010, issued by the Ministry of Economic Development, Department for Enterprise Management and internationalization Directorate General for small and medium-sized firms and cooperatives. For further information please consult the attached pdf document:

Small Business ACT –Initiatives to Support SMEs in Italy and in the 27 members states of Europe

Recent studies have shown that small and micro-enterprises have organization models and different objectives and characteristics that distinguish them from other parties. A typical and absolutely predominant aspect in micro-enterprise is "subjectivity". Often the founder is the person who manages and controls the company. Thus, culture and entrepreneurial attitudes determine development and company choices.

One of the critical issues for Italian micro-enterprises is the close relationship between the business and family dimension and thus the model of a "family business".

This is a business model that is widely used in the Italian industrial system, above all for reasons of a historical, cultural and institutional nature.

Today, this plays an important role as it pivots on informality in processes, flexibility, transmission of know-how, that represent the strengths of the business formula that characterizes the *family business*. These enterprises have contributed greatly to expand the productive base of our country and to make our products appreciated abroad (*Made in Italy)*. However, this model has diverse weaknesses, primarily the lack of openness to the contribution of third parties that links to the lack of specialization in roles (multirole parties).

For further information on the "*family business model"*, please consult the "PMI Finance" site at the following address: http://www.pmifinance.it/show9cde.html?page=18380

Here follows a table that shows the distribution of Italian enterprises by number of staff and sector:

Distribution % of enterprises by number of staff and sector (year 2008)						
1-9		**10-19**	**20-49**	**50-249**	**Over 250**	**Total**
Mineral extraction	74,3	17,1	6,6	1,8	0,1	100,0
Manufacturing activities	81,3	11,0	5,3	2,1	0,3	100,0
Industry in strict sense of the word	81,1	11,0	5,3	2,2	0,3	100,0
Construction	94,6	4,0	1,2	0,3	0,0	100,0
Services	96,6	2,2	0,8	0,3	0,1	100,0
TOTAL	**94,7**	**3,4**	**1,3**	**0,5**	**0,1**	**100,0**
Source: Elaboration of ISTAT data						

If we then look at employment, the ISTAT study explains how it is located mainly in the north-west of Italy.

In fact, 32.3% of employment is in those regions, followed by 23.8% in the Northeast, by 20.5% in Central Italy and 23.5% in Southern Italy.

There are not many differences in the construction industry: the North and South are divided more or less equally in this particular sector; a big difference lies in the services sector, where there is a clearer gap: 25.2% of employees working in the South are employed in this sector, while in the North it increases to 31.1%.

In general, however, in the Report between ITC and Italian SMEs, conducted by the Department of Informatics and Communication of the University of Milan, shows that SMEs do not have the resources needed to use ICT in a strategic manner.

The SME group is not enough, however, to cover the reality of categories belonging to this family: micro and small to medium sized enterprises can have extremely different organization and operations features.

The main factors that impede the use of ICT solutions and thus Information Security are:

- the lack of appropriate skills in human resources (typically a micro-enterprise has very few staff dedicated to IT).
- technological costs

Moreover, as testimonied by members of the Steering and Scientific Committee of CLUSIT (Italian Association for Information Security) and of the AIPSI (Italian Association of Information Security Professionals), the majority of micro enterprises do not have a real IT management, and therefore, ICT Security, and often a person does this but not exclusively.

In addition, a large proportion of small businesses use external staff with limited training and no real guidelines on how IT should support the firm's activities.

The conclusion is that the Security market is strongly orientated towards large businesses.

For further information on this issue, you can consult the interview with Claudio Telmon on information security in small and micro enterprises at the following internet address:

http://www.compliancenet.it/content/sicurezza-informatica-nelle-piccole-e-micro-imprese-intervista-claudio-telmon

A recent survey conducted by the Information Security Management Observatory of the School of Management of the Polytechnic of Milan, published on the portal dedicated to Security (SearchSecurity - point 3.2), on the identikit of the Head of Security, 22% of small and medium-sized enterprises do not have a person exclusively working on ICT security in the IT department.

For more information, please refer to the article published online at the following Internet address: http://searchsecurity.techtarget.it/articoli/0,1254,18_ART_86123,00.html

Data contained in the Report of the Information Security Management Observatory of the School of Management of the Politecnico di Milano, on ICT Security in SMEs, validates the preceding claims, namely that the rate of adoption of ICT security solutions in SMEs grows from 8% to 33% with the size of the business.

Most companies are aware of the importance of information security, but the level of "maturity" of solutions used is still very heterogeneous.

The most advanced storage solutions (Network Attached Storage - NAS - and Storage Area Network - SAN) are more common in firms with more than 100 employees. These systems are, however, almost unknown in smaller firms, who prefer disk array solutions, or even tape.

The areas where these systems are most commonly used are those in which there is a higher volume of information to manage, such as, for example, Chemistry-Rubber-Plastics (for physical installations and operations data), Engineering-Electrical (for project data) and Wood-Furniture-textiles (for drawings and data relating to fabrics and clothing).

There is a clear awareness of Italian SMEs of data protection issues. A high percentage of them adopt security systems, both as regards servers and clients. As regards the former, more than half of SMEs are equipped with antivirus and firewall systems, with rates close to 90% in larger firms. Less common, especially among smaller firms, are anti-spam systems, anti-spyware and proxy servers.

As regards client-side systems, almost all SMEs have adopted anti-viruses on PCs, while almost half use personal firewalls.

The benefits and opportunities of using Voice Over IP (VoIP) communication systems both dedicated or on the PC, seem well known to Italian SMEs.

This is confirmed by diffusion data contained in research: approx. 1 in 3 businesses use dedicated VoIP systems or use VoIP on their PCs.

As regards dedicated VoIP systems, the reduction of communication and infrastructure management costs remains the most noted reason to use them, while advanced services are underused, due to business's lack of knowledge of their potential.

As regards VoIP systems on PCs- these are often adopted to reduce communication costs for offices/branches of the company located abroad (half of the firms with at least 1 location/subsidiary abroad use these systems), even if their use is then extended, also to external communications.

Infrastructural open source packages are quite common in Italian SMEs, with adoption rates ranging from 13% to 35% based on size.

The most commonly used software are the server's operating systems on which the management system is installed, followed by the mail server, firewalls and client operating systems.

For more information on the "**RAPPORTO TRA LE PICCOLE E MEDIE IMPRESE E LE TECNOLOGIE DI COMUNICAZIONE E INFORMAZIONE (ICT)-RELATIONSHIP BETWEEN SMALL AND MEDIUM SIZED ENTERPRISES AND ICT**", please consult the

document on line at the following address: http://arxiv.org/ftp/arxiv/papers/1001/1001.1232.pdf

Other information that outlines the progress of the ICT sector and the Information Security sector in Italian companies is provided by the columns of the SMAU. The SMAU is a prestigious Italian exhibition, as well as a valuable content provider in the ICT market as it organizes training workshops purely for businesses, thanks to recent collaboration with Polimi (School of Management at the Polytechnic of Milan).

Among the focus areas of the 2011 edition, great importance was given to Information Security in SMEs (data protection, identity theft through embezzlement of accounts) as regards technologies that can increase safety and security. All this in the light of added value offered to customers in terms of continuity of operation and protection in the face of new use patterns (social media, clouds, mobilization of users) that require increasingly more advanced solutions and whose threats often anticipate the market itself. For more information on technological trends in the SME Security market, you can consult the online documents at the following addresses:
http://www.smau.it/milano11/schedules/potenziare-la-sicurezza-nella-piccola-impresa/
http://www.smau.it/milano11/partners/vasco-data-security/

The collaboration of SMAU with the Polimi Observatory highlights statistics identifying emerging trends of the ICT security world, in terms of organizational structure, positioning and sizing of the organizational units involved, their dedicated budgets, as well as analyzing the strategic planning process with particular reference to risk analysis methods.

As regards SMEs, data showed that in 61% of cases ICT security is tackled by only one person. In 22% of cases there are more resources that can go from 2 to 5. One should note that, as size increases, so does the number of staff involved in ICT security: we find that in 3% of cases the number of people ranges from 6 to 10, while in 14% of companies there are more than 10 people.

For further information on the entire Italian scenario on Information Security traced in all kinds of businesses (Small-Medium-Large), you can refer to the document attached called Speciale SMAU.

Another insight into the relationship of SMEs and information security is provided by Akhela Security, ICT Company of the Saras SpA group which is a leader in services and high-quality, innovative solutions in the ICT sector and in particular in the field of IT Security. This research, conducted for an AICA (Italian Association for Informatics and Computing) workshop, reiterates once again that SMEs are the drivers of the global economy, creating jobs and generating innovation and wealth.

According to Assinform (Italian Association for Information Technology) sources which is the basis of the Akhela research, in Italy SMEs are a strategic part of the wealth and employment levels in Italy: they employ 81% of the total workforce, a percentage which is significantly higher than the United Kingdom (54.8%), Germany (60.5%) and France (61.7%).

It shows how SMEs compared to larger companies, do not have large budgets to implement data protection systems which is why data protection is often entrusted to the "conscience" of individual human resources. In relation to economic resources available for protection and safety, in relation to large companies, SMEs have proved to be the weakest category of enterprise as regards data protection. SMEs are, in fact, an easy target for computer viruses and hacking, identity theft and information.

According to this research, as SMEs cannot invest in high-cost IS technology solutions, they should focus on the education and training of staff involved in projects to diffuse the culture of "confidentiality" of processed information in the company, which is the only real investment to reduce risks.

The next step would be to construct and maintain an information security management plan that takes into account organizational aspects (people and processes) of the entire business environment, to only then, worry about technological investments which are commensurate with actual needs.

(for further information, please look at the pdf document: "Aica-Akhela-SecurityA")

1.1.1) Persons to be trained (in particular)

Given the organizational model prevalent in SMEs, where it is usually the entrepreneur who is responsible, governs and strategically and operationally develops the business, it is "difficult" to imagine the development of technical vocational profiles responsible for Information Security in SMEs.

Instead, there seems to be a significant trend regarding the need to increase the entrepreneur's knowledge, skills and managerial qualities to oversee planning processes, direction and control of IS systems, according to the ISMS (Information Security Management System) logic.

This aspect is closely related to the increasing use by SMEs of outsourcing as regards to IT security services.

Precisely due to the need to interact and interface with "external" structures that are technically, technologically advanced, it is strategic to valorise SME managers' knowledge both widely and systematically to allow him/her to manage the service structures he/she has chosen to manage data security suitably and responding to the organisational management and cultural characteristics of SMEs.

This trend involves the „active involvement" of Management and ist „awareness" as this is considered the true driving force of ICT Security for any business. This is repeatedly emphasized and confirmed by research conducted by the School of Management of Politecnico di Milano in the following articles of the „Searchsecurity" magazine-web:

- ICT SECURITY, CRESCE LA CONSAPEVOLEZZA IN AZIENDA (for online consultation please go to http://searchsecurity.techtarget.it/articoli/0,1254,18_ART_103067,00.html)
- SECURITY MANAGEMENT (for online consultation: http://searchsecurity.techtarget.it/articoli/0,1254,18_ART_104000,00.html)

The absolute novelty □ort he security technology alone is not sufficient to protect the infrastructure of an organization.

The added value is management support in security policies that need to be respected by all employees/users, the quality of software and hardware solutions, as well as the professionals working on security to be used, which in the case of SMEs are often outsourced.

Delegating non-core activities to outside specialists or outsourcing, is identified as one of the concepts of business success in SMEs: „The key factor to successful outsourcing □ort he the contractor is not managed as an external entity but as an integrated part of the company", this is what is reported in one of the academic articles „New Business Model" by Assolombarda (please see attached pdf file „Assolombarda New Business Model").

It is apparent, therefore, that the reference target group for suitable, complete training in an ideal world should be enterprise managers.

There are diverse training opportunities for business leaders to provide the tools for a systematic approach to IT security which is vital both from an automation and organisational point of view to protect company data and employees' rights.

The objectives of the „E-security for SMEs" pilot project implemented by the Lombardy Region and the Chambers of Lombardy are to support the diffusion of what is defined as a „mindset" in IT security and to support Italian SMEs to identify appropriate security solutions. For further information please consult the project site at: http://www.ictbusiness.it/cont/articolo/le-pmi-trascurano-la-sicurezza-it-arrivano-manuale-e-voucher/27751/1.html

The project includes a tender (Nov. 2011) for direct support to enterprises through the provision of vouchers that provide a specialist to perform an eight-hour check-up focused on the overall security of enterprise systems.

Companies are, therefore, being offered a series of free training courses on computer security provided directly by the Chambers of Commerce participating in the area. In addition, web-based self-assessment software is provided, which can already be downloaded, which assists the entrepreneur in the self-assessment of the existing level of safety and potential risks in his/her company. A manual has also been created „The security of information, tools and solutions for SMEs", based on a survey undertaken of 750 small and medium-sized enterprises.

The study shows how the need for protection from computer risks is now widespread in businesses and in particular 75% of the sample confirmed that they have a virus check on attachments, 98% data backup and 96% work with password protected access systems. The critical areas, however, are in the details: 21% of Wi-Fi access is, in fact, not protected, only 26% of organizations use passwords selected according to security principles, 19% back up once a month if all goes well and only 13% do so also on pcs and mobile devices.

Finally, respecting security requirements is often a regulatory constraint, primarily the Law on privacy and the DPS, the Security Planning Document designed in accordance with the rules provided by the Authority for the protection of personal data.

On these fronts Lombard SMEs are „compliant" but only at surface level: even though 99% have implemented the minimum security measures, only 58% have extended the measures to all PCs and servers in the company, 48% do not update the DPS annually and only 39% regularly update their programmes and operating systems. Finally, 86% have absolutely no idea of the indirect costs caused by a hypothetical cyber attack and a subsequent data loss, and a stunning 88% do not have an inventory of sensitive or valuable information inside the company itself.

Despite everything, a positive fact emerges: only 4% of the sample claim to have suffered data loss in the last 3 years. Having said that, the adoption of digital signatures, in line with deadlines imposed by law, which is increasing, even if 52% of companies have passed this to their accountants, 80% of companies have an ad hoc profile that is responsible □ort he IT system and security procedures. Very often (in 85% of cases), however, this is entrusted to an external consultant and there is a lack of training and assessment of knowledge of security policies related to internal personnel: 65% do not impose assessment tests, 50% do not undertake periodical monitoring.

Please note that the Lombardy Region is one of the most important industrial areas of excellence in Italy.

11.4) Resume

The analysis conducted shows that a profound change is underway. New opportunities, unfortunately, are seen only by a very small part of the Italian economy and businesses. The result is that actors of the production system resorting to information security are still patchy and mainly undertaken by large companies and an objectively modest number as regards SMEs.

It is, therefore, a strategic objective to promote and diffuse the culture of information security for a safer and more knowledgeable use of technologies and the web in Italian SMEs.

This objective implies the need to encourage the spread of a "mindset" on Innovation Technology Security, as a means to preserve the company's business, supporting SMEs to identify e-security solutions that are both adequate and economically sustainable.

There is also a need to bridge the mismatch between supply and demand for training programmes, tailored to organizational, size and cultural characteristics of small businesses, filling an "open" space with the development and provision of training products/programmes that provide adequate depth and systemic vision of information security, and at the same time, provide the key elements of knowledge to guide the small business owner to introduce and manage proper data and business information security policies.

11.5) List of References

AICA. http://www.aicanet.it/certificazioni/eucip

Confindustria. http://www.confindustriasi.it/index.php?cont=login

Clusit. http://www.clusit.it/newsletter_30_06_07.pdf

EconomiaFinanza: http://www.economiafinanza.net/istat-in-italia-e-boom-di-micro-imprese

ICT SECURITY, CRESCE LA CONSAPEVOLEZZA IN AZIENDA. http://searchsecurity.techtarget.it/articoli/0,1254,18_ART_103067,00.html

"RAPPORTO TRA LE PICCOLE E MEDIE IMPRESE E LE TECNOLOGIE DI COMUNICAZIONE E INFORMAZIONE (ICT)-RELATIONSHIP BETWEEN SMALL AND MEDIUM SIZED ENTERPRISES AND ICT": http://arxiv.org/ftp/arxiv/papers/1001/1001.1232.pdf

http://www.compliancenet.it/content/sicurezza-informatica-nelle-piccole-e-micro-imprese-intervista-claudio-telmon

http://www.tecnologieinformatiche.com/dps.html

http://www.eucip.it/proposta-di-confindustria-per-adozione-di-eucip.

http://www.mondodigitale.net/Rivista/08_numero_3/Rub.%20Piva%20%20p.%2059-65.pdf)

http://mastersicurezza.uniroma1.it/

PMI Finance. http://www.pmifinance.it/show9cde.html?page=18380

SECURITY MANAGEMENT. http://searchsecurity.techtarget.it/articoli/0,1254,18_ART_104000,00.html

http://www.symantec.com/it/it

http://www.tecnologieinformatiche.com/dps.html

11.5.1) Sources of Law

Decree Law 30th June 2003, n. 196 "Code on protection of personal data", published in the Gazzetta Ufficiale No. 174 of 29th July, 2003 - Ordinary Supplement No. 123 and available on the website of the "Chamber of Deputies" in the special section on laws/proxies at the following internet address: http://www.camera.it/parlam/leggi/deleghe/testi/03196dl.htm

Decree Law 29th November 2008, n. 185: http://www.tesoro.it/documenti/open.asp?idd=20301)